ACTA ARITHMETICA
118.2 (2005)

Classes modulo les puissances dans l'anneau des S-entiers d'un corps de fonctions

par

Mireille Car (Marseille)

Soit un entier $l \geq 2$. Pour tout nombre premier p congru à 1 modulo l, soit $n_l(p)$ le plus petit entier qui *n'est* pas une puissance l-ième modulo p et soit $r_l(p)$ le plus petit nombre *premier qui est* puissance l-ième modulo p. Il est conjecturé que pour tout nombre réel $\varepsilon > 0$,

$$(\mathrm{C}_l) \qquad n_l(p) \ll p^{\varepsilon},$$

la constante impliquée par le symbole $\ll$ dépendant de l et de ε. Des majorations de $n_l(p)$ ont été établies en direction de cette conjecture [10], [15], [18]. Généralisant un résultat de Vinogradov [20], Elliott [8] a montré que $r_l(p) \ll p^{(l-1)/4+\varepsilon}$. La majoration $n_2(p) \ll \log(p)^2$ a été établie par Ankeny sous hypothèse de Riemann [1], la méthode utilisée pouvant conduire à la majoration $n_l(p) \ll \log(p)^2$. Cette dernière majoration n'est pas loin d'être optimale puisque la minoration $n_l(p) \gg \log(p)$ a lieu pour une infinité de nombres premiers p [7]. Le cas $l = 2$ mis à part, 1 et un entier non puissance l-ième modulo p ne suffisent pas à représenter toutes les classes du groupe quotient $(\mathbb{Z}/p\mathbb{Z})^*/((\mathbb{Z}/p\mathbb{Z})^*)^l$, ce qui conduit à définir d'autres bornes. Pour tout entier k, soit $H_l(k)$ le plus petit entier strictement positif tel que les entiers de l'intervalle $[1, H_l(k)]$ représentent toutes les classes du groupe quotient $(\mathbb{Z}/k\mathbb{Z})^*/((\mathbb{Z}/k\mathbb{Z})^*)^l$. Des majorations établies dans [16] on peut déduire que pour tout réel $\varepsilon > 0$, $H_l(k) \ll k^{3/8+\varepsilon}$. Un problème voisin a été étudié dans le cas $l = 2$ par A. Zaharescu [22]. Le nombre $h_2(k)$ étant défini comme le plus petit entier positif tel que les entiers de l'intervalle $[-h_2(k), h_2(k)]$ représentent toutes les classes du groupe quotient $(\mathbb{Z}/k\mathbb{Z})^*/((\mathbb{Z}/k\mathbb{Z})^*)^2$, A. Zaharescu a démontré que pour tout nombre réel $\varepsilon > 0$,

$$h_2(k) \ll k^{1/4+\varepsilon}.$$

2000 *Mathematics Subject Classification*: 11T06, 11T55.

Dans ce même article, il conjecturait aussi que pour tout nombre réel $\varepsilon > 0$,

$$h_2(k) \ll k^{\varepsilon}. \tag{C$'_2$}$$

Dans [3] une version polynomiale de la conjecture (C$'_2$) a été établie, cette conjecture étant un corollaire au théorème suivant.

THÉORÈME. *Soit q une puissance d'un nombre premier impair et soit $H \in \mathbb{F}_q[T]$ de degré $\deg H \geq 2$. Alors, pour tout entier*

$$j \geq \left(2\log(2)\,\frac{4q-1}{q-1} + \frac{2q}{e(q-1)\log(q)} + \frac{1}{e}\left(1 - \frac{2\log(2)}{\log(q)}\right)\right)\frac{\deg H}{\log(\deg H)}$$

pour tout polynôme A premier à H, il existe un polynôme irréductible unitaire P de degré j tel que AP soit un carré modulo H.

En d'autres termes, il existe un entier $R(H) \ll \deg H/\log(\deg H)$ tel que pour tout entier $j \geq R(H)$, les polynômes *irréductibles unitaires* de degré j représentent toutes les classes du groupe $(\mathbb{F}_q[T]/(H))^*/((\mathbb{F}_q[T]/(H))^*)^2$, (H) désignant l'idéal principal engendré par H.

Dans ce qui suit nous proposons une généralisation de ce résultat. Cette généralisation se fait dans deux directions. D'une part, on remplace l'étude modulo les carrés par l'étude modulo les puissances l-ièmes pour un entier l premier à la caractéristique du corps $\mathbb{F}_q$. D'autre part, on remplace l'anneau $\mathbb{F}_q[T]$ par l'anneau des S-entiers d'un corps de fonctions dont le corps des constantes est le corps $\mathbb{F}_q$. On s'intéresse toujours aux restes modulo un idéal *non nécessairement premier*. Une version polynomiale de la conjecture (C$_l$) sera donc un corollaire immédiat des résultats établis dans ce qui suit.

Soient K un corps de fonctions de corps des constantes k, corps fini à q éléments. Soient S un ensemble fini non vide de places de K et O_S l'anneau des S-entiers de K. Si P est un idéal premier de O_S, soit f_P le degré de P, c'est-à-dire le degré de l'extension de $\mathbb{F}_q$ par le corps O_S/P. On étend la notion de degré à tous les idéaux non nuls de O_S en posant pour un idéal H non nul,

$$f_H = \sum_P v_P(H) f_P,$$

la somme étant étendue aux idéaux premiers de O_S divisant H, $v_P(H)$ désignant l'exposant de P dans la factorisation de H en produit d'idéaux premiers. Le degré d'un élément non nul y de O_S est le degré de l'idéal principal de O_S engendré par y. Le degré d'un élément $y \in O_S$ dépend de l'ensemble S. Nous le noterons $\deg_S(y)$. La formule du produit montre que pour tout $y \in O_S$, $\deg_S(y)$ est divisible par le nombre $\operatorname{pgcd}\{f_v\,;\ v \in S\}$. Soit $l \geq 2$ un entier premier à la caractéristique du corps k. Soit H un idéal de O_S différent de $\{0\}$ et de O_S. On désigne par $N_l(S;H)$ le plus petit entier j_0 possédant la propriété suivante: pour tout entier $j \geq j_0$ divisible par $\operatorname{pgcd}\{f_v\,;\ v \in S\}$, pour tout $a \in O_S$ premier à l'idéal H, il existe $y \in O_S$

premier à H, de degré j tel que ay soit puissance l-ième modulo l'idéal H. Dans ce travail nous montrons qu'un tel entier existe et nous en donnons une majoration. Cette majoration est une conséquence de la majoration du nombre $R_l(S;H)$ qui désigne le plus petit entier j_0 possédant la propriété suivante: pour tout entier $j \geq j_0$ divisible par $\operatorname{pgcd}\{f_v;\ v \in S\}$, pour tout $a \in O_S$ premier à l'idéal H, il existe $y \in O_S$ de degré j, *engendrant un idéal premier*, premier à l'idéal H et tel que ay soit puissance l-ième modulo l'idéal H. De façon évidente,

$$N_l(S;H) \leq R_l(S;H).$$

Une majoration de $R_l(S;H)$ donnera une majoration de $N_l(S;H)$. Nous démontrerons que

$$R_l(S;H) \ll f_H/\log(f_H),$$

la constante contenue dans le symbole $\ll$ ne dépendant que de K, S et l.

Les anneaux de S-entiers d'un corps de fonctions de corps des constantes $\mathbb{F}_q$ peuvent être vus comme les analogues des anneaux d'entiers de corps de nombres. Le résultat établi ici n'a pas d'analogue connu dans le cadre des corps de nombres. Soit A un anneau d'entiers algébriques. Soit I un idéal non nul de A différent de l'idéal unité. On pourrait définir le nombre $H_l(\mathsf{A},I)$, resp. $R_l(\mathsf{A},I)$, comme étant le plus entier positif tel que les entiers de A de norme $\leq H_l(\mathsf{A},I)$, resp. les entiers premiers de A de norme $\leq R_l(\mathsf{A},I)$, représentent toutes les classes du groupe multiplicatif $(\mathsf{A}/I)^*/((\mathsf{A}/I)^*)^l$. Aucune majoration des nombres $H_l(\mathsf{A},I)$ ou $R_l(\mathsf{A},I)$ ne semble connue dans le cas général. Les seuls résultats connus concernent le cas d'un idéal premier P tel que $N(P) \equiv 1 \bmod l$. Pour un tel idéal, soit $n_l(\mathsf{A},P)$ la plus petite norme d'un entier de A qui n'est pas une puissance l-ième modulo P. La majoration $n_l(\mathsf{A},P) \ll N(P)^{1/2v+\varepsilon}$ a été établie par Friedlander [9], $v = v(l)$ désignant l'unique solution de l'équation $\varrho(u) = 1/l$, ϱ étant la fonction de Dickman [5].

Nous nous placerons d'abord dans le cas où l'ensemble S est réduit à un seul élément. La majoration dépend d'un théorème effectif de répartition des éléments premiers dans l'anneau O_S. Bien que la majoration des nombres $R_l(S;H)$ dans le cas général n'utilise le "théorème des éléments premiers" effectif que dans le cas où S contient une seule place, il nous a semblé intéressant de donner la preuve du "théorème des éléments premiers" dans le cas général, car la démonstration n'en est pas plus difficile. Dans ce travail, nous établirons d'abord le

THÉORÈME 1. *Si* $\mathbf{m} = (m_v)_{v\in S}$ *est une suite d'entiers rationnels telle que*

$$\|\mathbf{m}\| = -\sum_{v\in S} f_v m_v > 0,$$

soit $p_{\mathbf{m}}$ le nombre d'idéaux premiers principaux de O_S engendrés par un élément π tel que $(v(\pi))_{v\in S} = \mathbf{m}$. Alors, on a

$$p_{\mathbf{m}} = \frac{q^{\|\mathbf{m}\|}}{h\|\mathbf{m}\|} + O(q^{\|\mathbf{m}\|/2}),$$

les constantes impliquées par le symbole O ne dépendant que de K.

En fait, une version effective plus précise de ce théorème sera donnée par le théorème III.13.

Nous majorerons ensuite les nombres $R_l(S;H)$ en accordant une attention plus particulière au cas où l'idéal H est premier. Notons g le genre de K et notons h le nombre de classes de diviseurs de degré 0 de K. Nous démontrerons le

THÉORÈME 2. *Soit H un idéal non nul de O_S de degré $f_H > 1$ et soient*

$$a(H) = l^{\omega(H)}\left\{2g-2+d_S+\frac{q}{q-1}\right\} + (l-1)f_H l^{\omega(H)-1} + \frac{\varepsilon(S)}{h},$$

$$b(H) = 2gl^{\omega(H)}\frac{q^{1/2}}{q^{1/2}-1}, \qquad c(H) = (1-\varepsilon(S))l^{\omega(H)},$$

où $d_S = \min\{f_v\,;\, v\in S\}$, $\varepsilon(S) = 1$ si $d_S = 1$, $\varepsilon(S) = 0$ si $d_S \neq 1$, où $\omega(H)$ désigne le nombre d'idéaux premiers distincts divisant l'idéal H. Soit un entier

$$j \geq 1 + \max\Bigg(\max\{f_v\,;\, v\in S\}, 2\Bigg[\log_q\Bigg(h\Bigg\{a(H) + \frac{b(H)}{\sqrt{ha(H)}} + \frac{2c(H)\log(ha(H))}{\log(q)ha(H)} + \frac{l}{h(l-1)}\Bigg\}\Bigg)\Bigg]\Bigg).$$

Alors, si j est divisible par $\operatorname{pgcd}\{f_v\,;\, v\in S\}$, pour tout $a\in O_S$ premier à l'idéal H, il existe $y\in O_S$ de degré j, engendrant un idéal premier, premier à H tel que ay soit puissance l-ième modulo l'idéal H.

Dans le cas où l'idéal H est premier, nous établirons le

THÉORÈME 3. *Pour tout idéal premier P de O_S de degré f_P assez grand, on a*

$$R_l(S;P) \leq 1 + 2\Bigg[\log_q\Bigg(h\Bigg\{(l-1)f_P + l\Bigg\{2g-2+d_S+\frac{q}{q-1}+\frac{2(1-\varepsilon(S))}{e\log(q)}\Bigg\} + \frac{\varepsilon(S)}{h} + \frac{2gl\sqrt{q}}{(\sqrt{q}-1)\sqrt{h(l-1)}}\Bigg\}\Bigg)\Bigg],$$

les nombres d_S et $\varepsilon(S)$ étant ceux définis au théorème 2.

Précisons maintenant l'organisation de ce travail. Dans une première partie, nous fixons les notations. Dans une deuxième partie, nous définissons un

symbole à valeurs dans le groupe des racines l-èmes de l'unité complexes, symbole analogue au symbole d'Eisenstein et établissons les propriétés de ce symbole utiles à notre travail. La troisième partie est consacrée à la démonstration du "théorème des éléments premiers" pour l'anneau O_S ainsi qu'à une majoration de somme de caractères liés au symbole d'Eisenstein précédemment introduit. La majoration des nombres $R_l(S;H)$ et $N_l(S;H)$ sera établie dans la quatrième partie de ce travail. Les majorations obtenues dans le cas général sont évidemment valables quand l'anneau O_S est l'anneau $k[T]$. Par exemple, le théorème 2 nous donne que pour tout polynôme unitaire $H \in k[T]$,

$$R_l(H) \leq 1 + 2\left[\log_q\left((l-1)f_H l^{\omega(H)-1} + \frac{1}{q-1}\, l^{\omega(H)} + \frac{2l-1}{l-1}\right)\right],$$

où $R_l(H) = R_l(\{\infty\};(H))$, ∞ désignant la place à l'infini du corps $k(T)$. Toutefois, des calculs directs donnent des résultats plus précis dans le cas rationnel. Nous indiquerons dans une dernière partie les résultats effectifs pouvant être obtenus dans le cas rationnel.

I. Notations et rappels. Rappelons que le genre de K est noté g et que h désigne le nombre de classes de diviseurs de degré 0 de K.

Soit V l'ensemble des places de K. On identifiera une place à la valuation normalisée qui lui est associée. Pour toute place $v \in V$, on note respectivement K_v, K_v^*, U_v le complété du corps K en v, le groupe multiplicatif du corps K_v, le groupe des unités de l'anneau de valuation de K_v, on note f_v le degré résiduel de v, et, pour tout entier rationnel $j > 0$, on note $U_v^{(j)}$ le sous-groupe des éléments $u \in U_v$ tels que $v(u-1) \geq j$.

Soit $\mathsf{D} = \mathsf{D}(K)$ le groupe des diviseurs de K. Si $D \in \mathsf{D}(K)$ est le diviseur

$$D = \sum_{v \in V} a_v v,$$

son degré est le nombre

$$\mathfrak{f}_D = \sum_{v \in V} a_v f_v.$$

Posons pour $v \in V$,

$$v(D) = a_v.$$

Si tous les coefficients $v(D)$ sont positifs ou nuls, le diviseur D est dit effectif. Soit $\mathsf{D}_+(K)$ l'ensemble des diviseurs effectifs de K.

Soit $J(K)$ le groupe des idèles de K. L'application diagonale $\Delta : K^* \to J(K)$ définie par $\Delta(a) = (z_v)$ où $z_v = a$ pour tout $v \in V$ est un morphisme injectif. Il existe un morphisme surjectif Div de $J(K)$ dans $\mathsf{D}(K)$. Il est

défini par

$$\mathrm{Div}((z_v)) = \sum_{v\in V} v(z_v)v. \tag{I.1}$$

Comme (z_v) est un idèle, les nombres $v(z_v)$ sont tous nuls à l'exception d'un nombre fini d'entre eux, et, dans l'égalité ci-dessus, le terme de droite est bien un diviseur.

Soit ζ_K la fonction zêta du corps K. Elle est définie sur le disque ouvert $D_{1/q}$ par

$$\zeta_K(u) = \prod_{v\in V} (1-u^{f_v})^{-1}, \tag{I.2}$$

où D_r désigne pour tout réel $r>0$, l'ensemble des nombres complexes z tels que $|z|<r$.

Notre preuve utilisera certaines propriétés de ζ_K que nous rappelons ici, [21]. Pour $u\in D_{1/q}$,

$$\zeta_K(u) = \frac{P_K(u)}{(1-u)(1-qu)}, \tag{I.3}$$

où P_K est un polynôme de degré $2g$.

De plus, si $g>0$, il existe des entiers algébriques $\varrho_1,\dots,\varrho_{2g}$ tels que

$$P_K(u) = \prod_{i=1}^{2g}(1-\varrho_i u), \qquad |\varrho_i| = q^{1/2}. \tag{I.4}$$

II. Symbole d'Eisenstein. Si ce qui suit est bien connu lorsque l divise $q-1$ [17, chap. 3], il n'en est pas de même lorsque cette hypothèse n'est pas vérifiée. Nous proposons ici la construction d'un symbole valable pour tout entier l premier à la caractéristique de k.

Pour tout entier $n\geq 1$, soit $l_n = \mathrm{pgcd}(l, q^n-1)$. Dans un corps à q^n éléments, toute puissance l_n-ième est une puissance l-ième et il y a donc exactement l_n racines l-ièmes de l'unité dans un tel corps. Pour tout idéal premier P de l'anneau O_S on choisit une fois pour toutes un caractère χ_P d'ordre l_{f_P} du groupe multiplicatif du corps fini quotient $F_P = O_S/P$. Posons, pour alléger les notations, $l_{f_P} = l_P$. Désignons par σ_P l'homomorphisme surjectif canonique de O_S sur F_P.

On définit pour tout $\xi\in O_S$ le symbole $\left(\frac{\xi}{P}\right)$ par

$$\left(\frac{\xi}{P}\right) = \begin{cases} \chi_P(\sigma_P(\xi)) & \text{si } \xi \text{ est premier à } P,\\ 0 & \text{sinon.}\end{cases} \tag{II.1}$$

La proposition suivante donne les principales propriétés de ce symbole.

PROPOSITION II.1. *Soit P un idéal premier de O_S. Soient ξ et η des éléments de O_S. Alors*,

$$\xi \equiv \eta \bmod P \;\Rightarrow\; \left(\frac{\xi}{P}\right) = \left(\frac{\eta}{P}\right), \tag{II.2}$$

$$\left(\frac{\xi\eta}{P}\right) = \left(\frac{\xi}{P}\right)\left(\frac{\eta}{P}\right). \tag{II.3}$$

Si de plus ξ est premier à P, alors,

$$\sum_{j=0}^{l_P-1} \left(\frac{\xi}{P}\right)^j = \begin{cases} l_P & \text{si } \xi \text{ est puissance } l\text{-ième modulo } P, \\ 0 & \text{sinon.} \end{cases} \tag{II.4}$$

Preuve. Les deux premières assertions sont des conséquences immédiates de la définition du symbole. Soit $\eta \in O_S$ premier à P et soit $\xi \in O_S$ congru à η^l modulo P. Alors, d'après (II.2) et (II.3), $\left(\frac{\xi}{P}\right) = \left(\frac{\eta}{P}\right)^l = 1$, d'où,

$$\sum_{j=0}^{l_P-1} \left(\frac{\xi}{P}\right)^j = l_P.$$

Réciproquement, si $\xi \in O_S$ n'est pas puissance l-ième modulo P, $\sigma_P(\xi)$ n'est pas puissance l_P-ième dans le groupe multiplicatif F_P^*. Le caractère χ_P ayant été choisi d'ordre l_P, $\chi_P(\sigma_P(\xi)) \neq 1$ et $\left(\frac{\xi}{P}\right)$ est une racine l_P-ième de l'unité différente de 1, d'où,

$$\sum_{j=0}^{l_P-1} \left(\frac{\xi}{P}\right)^j = 0.$$

L'égalité (II.4) montre que la somme $1 + \left(\frac{\xi}{P}\right) + \cdots + \left(\frac{\xi}{P}\right)^{l_P-1}$ ne dépend pas du choix du caractère χ_P.

On étend le symbole précédemment défini à tout couple (H, α) où H est un idéal de O_S et α un élément de O_S en posant

$$\left(\frac{\alpha}{H}\right) = \prod_{\substack{P \in \mathbf{P} \\ P \mid H}} \left(\frac{\alpha}{P}\right)^{v_P(H)}, \tag{II.5}$$

où $\mathbf{P}$ est l'ensemble des idéaux premiers de O_S et, par abus de notation, $v_P(H)$ désigne l'exacte puissance de P divisant l'idéal H. La proposition suivante résume les propriétés de ce symbole.

PROPOSITION II.2. *Soient H et I des idéaux de O_S et soient ξ et η des éléments de O_S. Alors*,

$$\xi \equiv \eta \bmod H \;\Rightarrow\; \left(\frac{\xi}{H}\right) = \left(\frac{\eta}{H}\right), \tag{II.6}$$

$$\left(\frac{\xi\eta}{H}\right) = \left(\frac{\xi}{H}\right)\left(\frac{\eta}{H}\right), \tag{II.7}$$

$$\left(\frac{\xi}{H}\right)^{l} = 1, \tag{II.8}$$

$$\left(\frac{\xi}{HI}\right) = \left(\frac{\xi}{H}\right)\left(\frac{\xi}{I}\right). \tag{II.9}$$

III. Éléments premiers et idéaux premiers de l'anneau O_S. On suppose dans cette section que l'ensemble S a $s+1$ éléments, s étant un entier positif ou nul.

Notons $\mathbf{P}$ l'ensemble des idéaux premiers de O_S et Π l'ensemble des éléments premiers de O_S. Pour tout entier $n \geq 1$, soient p_n le nombre d'idéaux premiers degré n de O_S, $\operatorname{pr} p_n$ le nombre d'idéaux principaux premiers degré n de O_S. De façon évidente, $\operatorname{pr} p_n = 0$ si n n'est pas divisible par $\operatorname{pgcd}\{f_v\,;\, v \in S\}$. Si $\mathbf{m} = (m_v)_{v\in S}$ est un $(s+1)$-uple d'entiers rationnels, soit $\|\mathbf{m}\|$ l'entier défini par la relation

$$-\|\mathbf{m}\| = \sum_{v\in S} f_v m_v. \tag{III.1}$$

Si x est un élément non nul de K, soit $\mathbf{v}(x) = (v(x))_{v\in S}$.

Soit $\mathbf{m} = (m_v)_{v\in S}$ un $(s+1)$-uple d'entiers rationnels tel que $\|\mathbf{m}\| \geq 0$. L'ensemble $X_{\mathbf{m}}$ des $x \in O_S$ tels que $\mathbf{v}(x) = \mathbf{m}$ est fini. Soit $\Pi_{\mathbf{m}}$ l'ensemble des éléments de $X_{\mathbf{m}}$ engendrant un idéal premier de O_S. En d'autres termes, $\Pi_{\mathbf{m}} = \Pi \cap X_{\mathbf{m}}$. Soit $\pi_{\mathbf{m}}$ le nombre d'éléments de $\Pi_{\mathbf{m}}$. Soit aussi $\operatorname{pr} P_{\mathbf{m}}$, resp. $\operatorname{pr} p_{\mathbf{m}}$, l'ensemble des idéaux premiers principaux de O_S engendrés par un élément π tels que $\mathbf{v}(\pi) = \mathbf{m}$, resp. le nombre d'idéaux premiers principaux engendrés par un élément π de O_S tel que $\mathbf{v}(\pi) = \mathbf{m}$.

Des éléments $\pi \in O_S$ et $\theta \in O_S$ engendrent le même idéal et vérifient $\mathbf{v}(\pi) = \mathbf{v}(\theta)$ si et seulement si π/θ est une unité absolue, c'est-à-dire un élément non nul du corps k. On a donc pour tout $(s+1)$-uple d'entiers rationnels $\mathbf{m}$,

$$\pi_{\mathbf{m}} = (q-1)\operatorname{pr} p_{\mathbf{m}}. \tag{III.2}$$

Nous nous intéressons dans cette section à la distribution des idéaux et des éléments premiers. En ce qui concerne ces derniers, compte tenu de (III.2), celà revient à s'intéresser à la distribution des idéaux principaux premiers. L'estimation

$$np_n = q^n + O(q^{\theta n}), \qquad 0 < \theta < 1,$$

a été établie par Artin [2] lorsque K est une extension quadratique de $\mathbb{F}_p(T)$ où p est un nombre premier. Bien que dans le cas général l'estimation

$$np_n = q^n + O(q^{n/2})$$

semble bien connue, nous n'avons pas pu nous référer à des articles donnant des bornes explicites utiles dans la suite de notre travail. Les seules références trouvées étaient des articles [11], [12] ne donnant pas de résultats effectifs, l'un d'entre eux étant écrit en japonais. Une preuve de ce théorème est donnée dans [17, chap. 5] sans toutefois fournir de constantes effectives. Aussi avons nous pris le risque de redémontrer au théorème III.13 un résultat connu.

Notons ∞ l'une des places de S et posons $\mathsf{A} = O_{\{\infty\}}$. Remarquons ici que le groupe des éléments inversibles de l'anneau A est égal au groupe multiplicatif du corps k. Ultérieurement, nous choisirons la place ∞ dans S de façon à minimiser le degré résiduel f_∞ . Comme il a été dit dans l'introduction, il nous a paru intéressant de donner un théorème de répartition des éléments premiers dans le cas général de l'anneau O_S. Pour ce faire, au lieu de démontrer directement le théorème donnant la distribution des éléments premiers de l'anneau A, nous démontrons à la proposition III.2 un résultat un peu plus général dont un corollaire donne la distribution des idéaux principaux premiers dans A. Ce résultat plus général nous permettra d'obtenir un théorème de distribution des idéaux premiers principaux dans l'anneau O_S quand l'ensemble S n'est pas réduit à un seul élément. Enfin, nous avons aussi placé dans cette section une majoration relative à des symboles de puissance car la preuve de cette majoration utilise des techniques semblables à celles utilisées dans le reste de la section.

Tout d'abord, donnons un théorème effectif de répartion des idéaux premiers dans le cas général.

THÉORÈME III.1. *Pour tout entier $n \geq 1$, on a*

$$\text{(III.3)}\qquad q^n - q^{n/2}\left(2g + \frac{q}{q-1}\right) + \frac{q}{q-1} - 2g\,\frac{q^{1/2+n/4}-1}{q^{1/2}-1} - \delta(n) + \sum_{\substack{v\in S\\ f_v\mid n}} f_v\left(\delta\left(\frac{n}{f_v}\right) - 1\right) \leq np_n \leq q^n + 2gq^{n/2} + 1 - \sum_{\substack{v\in S\\ f_v\mid n}} f_v,$$

$\delta(n)$ désignant le nombre de diviseurs de n différents de n.

Preuve. Soit pour $z \in D_{1/q}$,

$$\text{(1)}\qquad f(z) = \zeta_K(z)\prod_{v\in S}(1 - z^{f_v}).$$

Alors avec (I.2),

$$f(z) = \prod_{P\in\mathbf{P}} (1 - z^{f_P})^{-1}, \tag{2}$$

puis avec (I.3),

$$f(z) = \frac{P_K(z)}{(1-z)(1-qz)} \prod_{v\in S} (1 - z^{f_v}),$$

d'où, avec (I.4),

$$f(z) = \Big\{ \prod_{v\in S} (1 - z^{f_v}) \Big\} (1-z)^{-1}(1-qz)^{-1} \prod_{i=1}^{2g} (1 - \varrho_i z), \tag{3}$$

avec $|\varrho_i| = q^{1/2}$, le dernier produit étant pris égal à 1 si $g = 0$. On calcule $zf'(z)/f(z)$ à l'aide des relations (2) et (3) ci-dessus et on identifie les coefficients de z^n dans les deux expressions obtenues. Il vient

$$\sum_{j|n} jp_j = q^n + 1 - \sum_{\substack{v\in S \\ f_v|n}} f_v - \sum_{i=1}^{2g} \varrho_i^n,$$

d'où

$$q^n + 1 - 2gq^{n/2} - \sum_{\substack{v\in S \\ f_v|n}} f_v \le \sum_{j|n} jp_j \le q^n + 1 + 2gq^{n/2} - \sum_{\substack{v\in S \\ f_v|n}} f_v. \tag{4}$$

On en déduit la majoration

$$np_n \le q^n + 2gq^{n/2} + 1 - \sum_{\substack{v\in S \\ f_v|n}} f_v. \tag{5}$$

Avec (5), il vient

$$\begin{aligned} \sum_{\substack{j|n \\ j\ne n}} jp_j &\le \sum_{\substack{j|n \\ j\ne n}} \Big(q^j + 2gq^{j/2} + 1 - \sum_{\substack{v\in S \\ f_v|j}} f_v \Big) \\ &\le \frac{q^{1+n/2}-1}{q-1} + 2g\,\frac{q^{1/2+n/4}-1}{q^{1/2}-1} + \delta(n) - \sum_{\substack{v\in S \\ f_v|n}} f_v \delta\Big(\frac{n}{f_v}\Big), \end{aligned}$$

$\delta(j)$ désignant le nombre de diviseurs de j différents de j. Compte tenu de (4), on en déduit la minoration

$$\begin{aligned} np_n \ge\ & q^n + 1 - 2gq^{n/2} \\ & - \sum_{\substack{v\in S \\ f_v|n}} f_v - \delta(n) + \sum_{\substack{v\in S \\ f_v|n}} f_v \delta\Big(\frac{n}{f_v}\Big) - \frac{q^{1+n/2}-1}{q-1} - 2g\,\frac{q^{1/2+n/4}-1}{q^{1/2}-1}. \end{aligned}$$

Ultérieurement, nous utiliserons la majoration

$$\text{(III.4)}\quad \sum_{\substack{j|n\\ j\neq n}} jp_j \leq \frac{q^{1+n/2}-1}{q-1} + 2g\,\frac{q^{1/2+n/4}-1}{q^{1/2}-1} + \delta(n) - \sum_{\substack{v\in S\\ f_v|n}} f_v\delta\left(\frac{n}{f_v}\right)$$

établie au cours de la démonstration précédente.

On remarque que si $g=0$ et si S est réduit à une seule place de degré 1, le théorème III.1 donne le résultat bien connu sur le nombre de polynômes irréductibles unitaires de degré n, [13].

Corollaire III.2. *Sous les mêmes hypothèses, pour tout entier* $n\geq 1$,

$$\text{(III.5)}\quad \sum_{j=1}^{n} p_j \leq \frac{3}{2(q-1)}\,\frac{q^{n+1}}{n} + 2g\max\left(3, \frac{2q^{1/2}}{q^{1/2}-1}\right)\frac{q^{n/2}}{n} + \log(n) + 1.$$

Preuve. D'après (III.3),

$$\sum_{i=1}^{n} p_i \leq \sum_{i=1}^{n} \frac{q^i}{i} + 2g\sum_{i=1}^{n}\frac{q^{i/2}}{i} + \sum_{i=1}^{n}\frac{1}{i}.$$

Trivialement,

$$\sum_{i=1}^{n}\frac{1}{i} \leq 1+\log(n).$$

D'après [6, lemme I.24],

$$\sum_{i=1}^{n}\frac{q^i}{i} \leq \frac{3q}{2(q-1)}\,\frac{q^n}{n}.$$

Par une méthode semblable à celle utilisée pour obtenir la majoration ci-dessus, on obtient la majoration

$$\sum_{i=1}^{n}\frac{q^{i/2}}{i} \leq \max\left(3, \frac{2q^{1/2}}{q^{1/2}-1}\right)\frac{q^{n/2}}{n}.$$

Le corollaire se déduit de ces trois majorations.

Proposition III.3. *Soit* H *un idéal de* O_S *tel que* $f_H \geq q^2$. *Alors*,

$$\text{(III.6)}\qquad \omega(H) \leq C(K)\,\frac{f_H}{\log_q(f_H)},$$

avec

$$\text{(III.7)}\quad C(K) = \left(1 + \frac{3q}{q-1} + 4g\max\left(\frac{3}{q}, \frac{2}{q-q^{1/2}}\right) + \frac{2\log(2)}{q^2} + \frac{2}{q^2}\right).$$

Preuve. Par une démonstration analogue à celle de la proposition I.2 de [3] on obtient la majoration

$$\omega(H) - \frac{f_H}{\log_q(f_H)} \leq \sum_{\substack{P\in\mathbf{P}\\ f_P\leq\log_q(f_H)}} 1. \tag{1}$$

Posons $n = [\log_q(f_H)]$. Le théorème précédent nous donne

$$\omega(H) - \frac{f_H}{\log_q(f_H)} \leq \frac{3q}{2(q-1)}\,\frac{q^n}{n} + 2g\max\left(3, \frac{2q^{1/2}}{q^{1/2}-1}\right)\frac{q^{n/2}}{n} + \log(n) + 1,$$

d'où

$$\begin{aligned}\omega(H) &\leq \left(1+\frac{3q}{q-1}\right)\frac{f_H}{\log_q(f_H)} + 4g\max\left(3, \frac{2q^{1/2}}{q^{1/2}-1}\right)\frac{\sqrt{f_H}}{\log_q(f_H)}\\ &\quad + \log(\log_q(f_H)) + 1\\ &\leq \left(1+\frac{3q}{q-1} + 4g\max\left(\frac{3}{q}, \frac{2}{q-q^{1/2}}\right) + \frac{2\log(2)}{q^2} + \frac{2}{q^2}\right)\frac{f_H}{\log_q(f_H)}.\end{aligned}$$

Nous supposons maintenant que S est réduit à la place ∞ notée aussi v_∞ et donc que $\mathsf{A} = O_S$. Posons, pour tout entier $n \geq 1$,

$$\Delta_n = \sum_{\substack{j|n\\ j\neq n}} jp_j. \tag{III.8}$$

Introduisons des définitions et notations relatives à l'anneau A. L'ensemble V des places de K est réunion de la place ∞ et des places P-adiques associées aux idéaux premiers P de A. Afin d'alléger les notations on pose $f_{v_\infty} = f_\infty$, $K_{v_\infty} = K_\infty$, $U^{(k)}_{v_\infty} = U^{(k)}_\infty$ et $f_{v_P} = f_P$, $K_{v_P} = K_P$, $U^{(k)}_{v_P} = U^{(k)}_P$ si P est un idéal premier de A. On note aussi $\mathbf{I} = \mathbf{I}(\mathsf{A})$ l'ensemble des idéaux entiers non nuls de A, $\mathbf{FI} = \mathbf{FI}(\mathsf{A})$ le groupe des idéaux fractionnaires de A dans K, $\mathrm{pr} = \mathrm{pr}(\mathsf{A})$ le groupe des idéaux principaux fractionnaires de A dans K, $\mathcal{C}\ell = \mathcal{C}\ell(\mathsf{A})$ le groupe des classes d'idéaux de A. On rappelle que $\mathbf{P} = \mathbf{P}(\mathsf{A})$ désigne l'ensemble des idéaux premiers de A. Si $a \in K$, l'idéal principal $\mathsf{A}a$ sera aussi noté (a). Soit $H \in \mathbf{I}$. On dira que l'idéal fractionnaire $J \in \mathbf{FI}(\mathsf{A})$ est *premier* à H si $v_P(J) = 0$ pour tout idéal premier P divisant H. On note $\mathbf{FI}_H$ l'ensemble des $Y \in \mathbf{FI}$ premiers à H. De même, $\mathbf{I}_H$, resp. $\mathbf{P}_H$, pr_H désignera l'ensemble des idéaux premiers à H appartenant à l'ensemble $\mathbf{I}$, resp. $\mathbf{P}$, pr.

On note Ξ le groupe des caractères de $\mathcal{C}\ell$. Par abus de notations, si $\chi \in \Xi$ et si $Y \in \mathbf{FI}$, on note encore $\chi(Y)$ le nombre $\chi(\overline{Y})$ où $\overline{Y}$ est la classe de l'idéal Y dans le groupe des classes d'idéaux $\mathcal{C}\ell$. Soit $H \in \mathbf{I}(\mathsf{A})$. On dit que le diviseur $D \in \mathsf{D}(K)$ est premier à H si $v_P(D) = 0$ pour tout idéal premier P divisant H. Notons D_H l'ensemble des $Y \in \mathsf{D}$ premiers à H. Il

existe un morphisme surjectif Id de $\mathsf{D}(K)$ sur le groupe $\mathbf{FI}(\mathsf{A})$ des idéaux fractionnaires de A. Il est défini par

$$\mathrm{Id}\Big(\sum_{v\in V} a_v v\Big) = \prod_{P\in\mathbf{P}} P^{a_{v_P}}. \tag{III.9}$$

De plus, $\mathbf{I}$ est l'image de $\mathsf{D}_+(K)$ par Id.

Soit h_∞ le nombre de classes d'idéaux de l'anneau A, c'est-à-dire l'ordre du groupe $\mathcal{C}\ell$. On a

$$h_\infty = hf_\infty. \tag{III.10}$$

Une preuve de cette égalité est donnée dans [13].

Le groupe $\mathbf{FI}(\mathsf{A})$ étant libre, il en est de même du sous-groupe pr$\mathbf{FI}(\mathsf{A})$ formé par les idéaux principaux fractionnaires de A. Soit B une base de ce groupe libre. Pour tout idéal $B \in \mathsf{B}$, soit $b_B \in K$ un générateur de B choisi une fois pour toutes. Alors, le sous-groupe H de K^* engendré par $\{b_B\,;\, B \in \mathsf{B}\}$ est isomorphe au groupe pr$\mathbf{FI}(\mathsf{A})$. Soit $M = H \cap \mathsf{A}$. L'ensemble M est un semi-groupe multiplicatif tel que tout idéal principal de A est engendré par un et un seul élément de M.

Dans le cas rationnel, on peut prendre pour B l'ensemble des polynômes irréductibles unitaires et pour M l'ensemble des polynômes unitaires. Aussi, par analogie, les éléments du semi-groupe M seront appelés les éléments *unitaires*.

Le corollaire 5 au théorème 2 de [21, chap. VII] donne l'existence d'un diviseur

$$\mathcal{A}_1 = \sum_{v\in V} a_v v$$

de degré 1 tel que $a_\infty = 0$. Choisissons un tel diviseur et posons

$$I_1 = \mathrm{Id}(\mathcal{A}_1). \tag{III.11}$$

On a donc

$$f_{I_1} = 1. \tag{III.12}$$

Remarques III.4. (i) *Soit $a \in \mathsf{A}$. Alors,*

$$\deg_{\{\infty\}}(a) = -f_\infty v_\infty(a). \tag{III.13}$$

(ii) *Le morphisme $X \mapsto f_X$ de $\mathbf{FI}(\mathsf{A})$ dans $\mathbb{Z}$ est surjectif.*

(iii) *Soient I et J des idéaux fractionnaires de A dans K appartenant à la même classe Γ. Alors,*

$$f_I \equiv f_J \bmod f_\infty. \tag{III.14}$$

Il existe donc un morphisme surjectif $\Gamma \mapsto \varphi_\Gamma$ du groupe $\mathcal{C}\ell(\mathsf{A})$ sur le groupe $\mathbb{Z}/\mathbb{Z}f_\infty$ tel que

$$\varphi_\Gamma = f_H \quad \textit{pour tout } H \in \Gamma. \tag{III.15}$$

Preuve. La formule du produit (cf. [4, chap. I]) donne (III.13). Soit d l'entier positif engendrant dans $\mathbb{Z}$ l'idéal $\operatorname{Im} f$. Alors d divise $f_{I_1} = 1$. Le (iii) est alors immédiat.

Le noyau de φ jouera un rôle important dans ce qui suit.

PROPOSITION III.5. *Soit $\chi \in \Xi$. Alors, la série*

$$L(\chi, u) = \sum_{Y \in \mathbf{I}} \chi(Y) u^{f_Y} \tag{III.16}$$

est absolument convergente dans le disque $D_{1/q}$ et pour $u \in D_{1/q}$,

$$L(\chi, u) = \prod_{P \in \mathbf{P}} (1 - \chi(P) u^{f_P})^{-1}. \tag{III.17}$$

Si χ est trivial sur $\operatorname{Ker} \varphi$,

$$L(\chi, u) = \zeta_K(\chi(I_1)u)(1 - u^{f_\infty}). \tag{III.18}$$

Si χ n'est pas trivial sur $\operatorname{Ker} \varphi$, *$g \geq 1$, $L(\chi, u)$ est un polynôme de degré $2g - 2 + f_\infty$ et*

$$L(\chi, u) = \prod_{i=1}^{2g-2+f_\infty} (1 - \omega_i u), \tag{III.19}$$

avec $|\omega_i| = q^{1/2}$ pour $1 \leq i \leq 2g-2$ et $|\omega_i| = 1$ pour $2g-1 \leq i \leq 2g-2+f_\infty$.

Preuve. La convergence absolue se déduit de celle de la fonction ζ_K. Soit ω le caractère du groupe $\mathsf{D}(K)$ défini par la relation

$$\omega = \chi \circ \operatorname{Id}. \tag{1}$$

Alors, ω est trivial sur le groupe $\operatorname{Div} \circ \Delta(K^*)$ des diviseurs principaux. Soit L_ω la fonction L associée à ω. Si $u \in D_{1/q}$,

$$L_\omega(u) = \prod_{v \in V(K)} (1 - \omega(v) u^{f_v})^{-1} = \sum_{Y \in \mathsf{D}_+(K)} \omega(Y) u^{f_Y}.$$

Le produit, resp. la série, ci-dessus est absolument convergent dans le disque $D_{1/q}$. Comme $\operatorname{Ker} \operatorname{Id}$ est le sous-groupe de $\mathsf{D}(K)$ engendré par v_∞,

$$(1 - u^{f_\infty}) L_\omega(u) = \prod_{P \in \mathbf{P}} (1 - \chi(P) u^{f_P})^{-1},$$

et

$$L(\chi, u) = (1 - u^{f_\infty}) L_\omega(u). \tag{2}$$

1° On suppose que χ est trivial sur le sous-groupe $\operatorname{Ker} \varphi$. Alors ω est trivial sur le sous-groupe $\mathsf{D}_0(K)$ formé par les diviseurs de degré 0 et, d'après [4, chap. III],

$$L_\omega(u) = \zeta_K(\omega(\mathcal{A}_1)u).$$

Avec (1) et (III.12),

$$L_\omega(u) = \zeta_K(\chi(I_1)u), \tag{3}$$

et (III.18) est donnée par (2).

2° On suppose que χ n'est pas trivial sur le sous-groupe $\operatorname{Ker}\varphi$. Il existe donc un idéal H de A tel que $f_H \equiv 0 \bmod f_\infty$ et $\chi(H) \neq 1$. Considérons le diviseur

$$\mathcal{Y} = -\frac{f_H}{f_\infty}\, v_\infty + \sum_{\substack{P\in\mathbf{P}\\ P|H}} v_P(H) v_P.$$

D'après (I.1) puis (III.9), $\mathfrak{f}_\mathcal{Y} = 0$, $\omega(\mathcal{Y}) \neq 1$. D'après [4, chap. III], $g \geq 1$ et L_ω est un polynôme de degré $2g-2$. Si $g = 1$, $L_\omega(u) = 1$ et (III.19) se déduit de (2). On suppose $g > 1$. D'après [21, chap. 7], il existe des entiers algébriques $\omega_1, \ldots, \omega_{2g-2}$ tels que

$$L_\omega(u) = \prod_{i=1}^{2g-2} (1 - \omega_i u), \qquad |\omega_i| = q^{1/2}.$$

On conclut avec (2).

Dans la suite de ce travail nous n'utiliserons qu'une version plus faible de la proposition suivante. Il nous suffirait en fait de remplacer dans le résultat ci-dessous, la condition (III.22) par la condition plus forte:

$$\text{Pour tout } x \in K, \quad x \equiv 1 \bmod H \;\Rightarrow\; \Psi((x)) = 1. \tag{III.22$'$}$$

La version donnée plus forte donnée ci-dessous pourra être utilisée pour traiter d'autres problèmes.

Proposition III.6. *Soient $\chi \in \Xi$ et $H \in \mathbf{I}$. Soit Ψ un morphisme du groupe $\mathbf{FI}_H(\mathsf{A})$ dans le groupe μ_m des racines m-ièmes de l'unité. Alors, la série*

$$\Lambda(\chi\Psi, u) = \sum_{Y\in\mathbf{I}_H} \chi(Y)\Psi(Y) u^{f_Y} \tag{III.20}$$

est absolument convergente dans le disque $D_{1/q}$ et pour $u \in D_{1/q}$,

$$\Lambda(\chi\Psi, u) = \prod_{P\in\mathbf{P}_H} (1 - \chi(P)\Psi(P) u^{f_P})^{-1}. \tag{III.21}$$

De plus, si Ψ n'est pas trivial sur le groupe des idéaux principaux et vérifie la condition :

$$\text{Pour tout } x \in K, \quad x \in U_\infty^{(1)} \text{ et } x \equiv 1 \bmod H \;\Rightarrow\; \Psi((x)) = 1, \tag{III.22}$$

alors $f_H \geq 1$, $\Lambda(\chi\Psi, u)$ est un polynôme de degré $d(\chi\Psi) \leq 2g - 2 + f_\infty + f_H$

et

$$\Lambda(\chi\Psi,u)=\prod_{i=1}^{d(\chi\Psi)}(1-\varrho_i u), \tag{III.23}$$

avec $|\varrho_i|\in\{q^{1/2},1\}$.

Preuve. (I) La convergence absolue de la série $\Lambda(\chi\Psi,u)$ se déduit de celle du produit

$$g(u)=\prod_{P\in\mathbf{P}}(1-u^{f_P})^{-1},$$

intervenant dans la preuve du théorème III.1. Pour $u\in D_{1/q}$, $\Lambda(\chi\Psi,u)$ se développe en produit eulérien absolument convergent

$$\Lambda(\chi\Psi,u)=\prod_{P\in\mathbf{P}_H}(1-\chi(P)\Psi(P)u^{f_P})^{-1}. \tag{1}$$

(II) Soit $\Sigma=\{v_P\,;\,P\in\mathbf{P},\,P\,|\,H\}\cup\{v_\infty\}$ et soit G_Σ le sous-groupe de $J(K)$ formé par les idèles (z_v) tels que $z_v=1$ pour tout $v\in\Sigma$. Pour tout idéal premier P divisant H, soit

$$T_{v_P}=U_P^{(V_P(H))},$$

et soit

$$T_{v_\infty}=U_\infty^{(1)}.$$

Soit $z\in K^*$ tel que $z\in T_v$ pour tout $v\in\Sigma$. Alors $z\equiv 1 \bmod H$. Puisque Ψ vérifie la condition (III.22) et que $\mathrm{Id}\circ\mathrm{Div}(\Delta(z))$ est l'idéal principal $\mathsf{A}z$,

$$(\chi\Psi)\circ\mathrm{Id}\circ\mathrm{Div}(\Delta(z))=1=\prod_{v\in\Sigma}\psi_v(z),$$

où, pour tout $v\in\Sigma$, ψ_v est le morphisme trivial de T_v dans le groupe μ_l. D'après [21, chap. 7], le morphisme $(\chi\Psi)\circ\mathrm{Id}\circ\mathrm{Div}$ du groupe G_Σ dans le groupe μ_m peut être étendu de façon unique en un quasi-caractère ω de $J(K)$ trivial sur $\Delta(K^*)$. Ce quasi-caractère est non ramifié en toute place $v\notin\Sigma$. De plus, pour tout $v\in\Sigma$, ω induit le morphisme trivial sur T_v. Soit L_ω la fonction L associée à ω. Alors, si $u\in D_{1/q}$,

$$L_\omega(u)=\prod_{v\in V_\omega}(1-\omega\circ j_v(\Pi_v)u^{f_v})^{-1},$$

où V_ω est l'ensemble des places $v\in V(K)$ pour lesquelles le caractère $\omega_v=\omega\circ j_v$ est non ramifié, où pour $v\in V(K)$, Π_v est une uniformisante de K_v. Soit $P\in\mathbf{P}$ premier à H. Soient $a\in K_P^*$ et $z=j_{v_P}(a)$. Alors,

$$(\mathrm{Id}\circ\mathrm{Div})(z)=\mathrm{Id}(v_P(a)v_P)=P^{v_P(a)},\qquad \omega(j_{v_P}(a))=\chi(P^{v_P(a)})\Psi(P^{v_P(a)}).$$

Prenons pour a une uniformisante Π_P de O_{v_P}. Il vient

$$\omega(j_{v_P}(\Pi_P))=\chi(P)\Psi(P). \tag{2}$$

Par suite, avec (1) et (2),

$$\Lambda(\chi\Psi,u)=L_\omega(u)\prod_{v\in\Sigma_\omega}(1-\omega\circ j_v(\Pi_v)u^{f_v}), \tag{3}$$

où Σ_ω est l'ensemble des places $v\in\Sigma$ où $\omega_v=\omega\circ j_v$ est non ramifié.

On suppose Ψ non trivial sur le groupe des idéaux principaux. Tout d'abord, compte tenu de la condition (III.22), l'idéal H n'est pas l'idéal unité et $f_H>0$. Comme Ψ n'est pas trivial sur l'ensemble des idéaux premiers, l'ensemble $V(K)-V_\omega(K)$ n'est pas vide et ω n'est pas un caractère principal. D'après [21, chap. 7] et [21, Appendix V.5], $L_\omega(u)$ est un polynôme de degré

$$\deg L_\omega(u)=2g-2+\sum_{\substack{v\in\Sigma\\ v\notin\Sigma_\omega}}f_v \tag{4}$$

dont les racines sont de module $q^{1/2}$. D'après (3), $\Lambda(\chi\Psi,u)$ est un polynôme pouvant s'écrire comme produit

$$\Lambda(\chi\Psi,u)=\prod_{i=1}^{d}(1-\varrho_i u), \tag{5}$$

avec

$$|\varrho_i|\in\{1,q^{1/2}\},\qquad d=\deg\Lambda(\chi\Psi,u)=2g-2+\sum_{v\in\Sigma}f_v\le 2g-2+f_\infty+f_H.$$

Proposition III.7. *Soient $\chi\in\Xi$, $H\in\mathbf{I}$ et $A\in\mathbf{I}$ un idéal premier à H. Soit Ψ un morphisme du groupe $\mathbf{FI}_H(A)$ dans le groupe μ_m vérifiant la condition* (III.22)*. Pour tout entier positif n, soit*

$$b(\chi,H,A,\Psi,n)=\sum_{\substack{P\in\mathbf{P}_{AH}\\ f_P=n}}\chi(P)\Psi(P). \tag{III.24}$$

Si l'une des deux conditions suivantes est vérifiée :

(I) *Il existe $x\in M$ tel que $\Psi((x))\neq 1$,*

(II) *$H=1$, Ψ est trivial sur le groupe $\mathbf{FI}(\mathsf{A})$ et χ n'est pas trivial sur le sous-groupe* $\operatorname{Ker}\varphi$,

alors, pour tout $n\ge 1$,

$$|nb(\chi,H,A,\Psi,n)|\le(2g-2+f_\infty+f_H)q^{n/2}+\omega(A)+\Delta_n, \tag{III.25}$$

où Δ_n est défini par (III.8).

Preuve. Posons pour $u\in D_{1/q}$,

$$f(u)=\prod_{P\in\mathbf{P}_{AH}}(1-\chi(P)\Psi(P)u^{f_P})^{-1}. \tag{1}$$

Soit $d = d(\chi\Psi)$ défini par la proposition précédente dans l'hypothèse (I) et $d = d(\chi\Psi) = 2g-2+f_\infty$ dans l'hypothèse (II). D'après les deux propositions précédentes, il existe des entiers algébriques $\varrho_1, \dots, \varrho_d$ de module $\leq q^{1/2}$ tels que pour $z \in D_{1/q}$,

$$f(u) = \Big\{ \prod_{\substack{P\in\mathbf{P}\\ P|A}} (1-\chi(P)\Psi(P)u^{f_P})\Big\}\Big\{ \prod_{i=1}^{d}(1-\varrho_i u)\Big\}. \tag{2}$$

On calcule $uf'(u)/f(u)$ à l'aide des deux expressions ci-dessus et on identifie les coefficients de u^n dans les deux expressions. Il vient

$$\sum_{\substack{P\in\mathbf{P}_{AH}\\ jf_P=n}} f_P(\chi(P)\Psi(P))^j = -\sum_{i=1}^{d}\varrho_i^n - \sum_{\substack{P\in\mathbf{P}\\ P|A}} (\chi(P)\Psi(P))^n,$$

d'où

$$nb(\chi,H,A,\Psi,n) = -\sum_{i=1}^{d}\varrho_i^n - \sum_{\substack{P\in\mathbf{P}\\ P|A}} (\chi(P)\Psi(P))^n - \sum_{\substack{P\in\mathbf{P}_H\\ jf_P=n,\, j\neq 1}} f_P(\chi(P)\Psi(P))^j.$$

Par suite,

$$|nb(\chi,H,A,\Psi,n)| \leq d(\chi\Psi)q^{n/2} + \omega(A) + \sum_{\substack{P\in\mathbf{P}\\ f_P|n,\, f_P\neq n}} f_P.$$

Avec la notation (III.8),

$$|nb(\chi,H,A,\Psi,n)| \leq d(\chi\Psi)q^{n/2} + \omega(A) + \Delta_n.$$

Corollaire III.8. *Soient $H \in \mathbf{I}$ et Ψ un morphisme du groupe $\mathbf{FI}_H(\mathsf{A})$ dans le groupe μ_m des racines m-ièmes de l'unité, non-trivial sur le sous-groupe des idéaux principaux et vérifiant la condition* (III.22). *Pour tout entier $n > 0$, soit*

$$t(\Psi,H,n) = \sum_{\substack{P\in\mathbf{P}\cap\mathrm{pr}\\ (P,H)=1,\, f_P=n}} \Psi(P). \tag{III.26}$$

Alors,

$$|nt(\Psi,H,n)| \leq (2g-2+f_\infty+f_H)q^{n/2} + \Delta_n. \tag{III.27}$$

Preuve. Si n n'est pas divisible par f_∞, la somme définissant $t(\Psi,H,n)$ porte sur l'ensemble vide et $t(\Psi,H,n) = 0$. On suppose n divisible par f_∞. Par orthogonalité,

$$\#(\Xi)t(\Psi,H,n) = \sum_{\chi\in\Xi} b(\chi,H,(1),\Psi,n),$$

$b(\chi,H,(1),\Psi,n)$ étant défini par (III.24). On conclut avec (III.25).

PROPOSITION III.9. *Soient $\chi \in \Xi$ trivial sur le sous-groupe* $\operatorname{Ker}\varphi$ *et H un idéal de* A. *Pour tout entier positif n, soit*

$$a(\chi, H, n) = \sum_{\substack{P \in \mathbf{P}_H \\ f_P = n}} \chi(P). \tag{III.28}$$

Alors, pour tout entier $n \geq 1$ congru à $-f_H$ modulo f_∞,

$$|n\chi(H)a(\chi, H, n) - q^n| \leq 2gq^{n/2} + 2 + \omega(H) + \Delta_n. \tag{III.29}$$

De plus,

$$|na(\chi, (1), n) - q^n| \leq 2gq^{n/2} + \Delta_n. \tag{III.30}$$

Preuve. Considérons la fonction $L(\chi, \cdot)$ définie à la proposition III.5. D'après (III.17), (III.18), suivis de (I.2), (I.3) et (I.5), pour $u \in D_{1/q}$,

$$\prod_{P \in \mathbf{P}_H} (1 - \chi(P)u^{f_P})^{-1} = (1 - u^{f_\infty})(1 - \chi(I_1)u)^{-1}(1 - q\chi(I_1)u)^{-1} \times \Big\{ \prod_{i=1}^{2g} (1 - \varrho_i \chi(I_1)u) \Big\} \Big\{ \prod_{\substack{P \in \mathbf{P} \\ P|H}} (1 - \chi(P)u^{f_P}) \Big\},$$

où, pour $i = 1, \ldots, 2g$, $|\varrho_i| = q^{1/2}$. En procédant comme à la proposition précédente, on obtient

$$\sum_{\substack{P \in \mathbf{P}_H \\ jf_P = n}} f_P(\chi(P))^j = -\sum_{i=1}^{2g} \varrho_i^n \chi(I_1)^n - \varepsilon(f_\infty, n) + \chi(I_1)^n + \chi(I_1)^n q^n - \sum_{\substack{P \in \mathbf{P} \\ P|H \\ jf_P = n}} (\chi(P))^n,$$

où $\varepsilon(f_\infty, n) = 1$ ou 0 suivant que f_∞ divise ou ne divise pas n.

Supposons $n + f_H \equiv 0 \bmod f_\infty$. D'après (III.12), $f_{I_1} = 1$ d'où $f_H + nf_{I_1} \equiv 0 \bmod f_\infty$. Comme χ est trivial sur $\operatorname{Ker}\varphi$,

$$\chi(H)(\chi(I_1))^n = 1,$$

d'où

$$\chi(H) \sum_{\substack{P \in \mathbf{P}_H \\ jf_P = n}} f_P(\chi(P))^j = q^n + 1 - \sum_{i=1}^{2g} \varrho_i^n - \chi(H)\varepsilon(f_\infty, n) - \chi(H) \sum_{\substack{P \in \mathbf{P} \\ P|H \\ jf_P = n}} (\chi(P))^j,$$

et

$$n\chi(H)\sum_{\substack{P\in\mathbf{P}_H\\ f_P=n}}\chi(P)=q^n+1-\sum_{i=1}^{2g}\varrho_i^n-\chi(H)\varepsilon(f_\infty,n)$$
$$-\chi(H)\Big(\sum_{\substack{P\in\mathbf{P}\\ P|H\\ jf_P=n}}(\chi(P))^j+\sum_{\substack{P\in\mathbf{P}_H\\ jf_P=n\\ j\neq1}}f_P(\chi(P))^j\Big),$$

d'où la majoration (III.29). Si $H=(1)$, $n\equiv 0 \bmod f_\infty$, $1-\chi(H)\varepsilon(f_\infty,n)=0$, d'où (III.30).

Proposition III.10. *Soit H un idéal de A. Soit un entier $n\geq 1$ tel que $f_H+n\equiv 0 \bmod f_\infty$. Alors,*

$$\Big|hn\sum_{\substack{P\in\mathbf{P}_H\\ f_P=n\\ PH\in\mathrm{pr}}}1-q^n\Big| \leq h(2gq^{n/2}+\omega(H)+\Delta_n)+(h-1)(f_\infty-2)q^{n/2}+\varrho(H), \tag{III.31}$$

où

$$\varrho(H)=\begin{cases}0 & \text{si } H=(1),\\ 2 & \text{si } H\neq(1).\end{cases} \tag{III.32}$$

Preuve. On suppose $H\neq(1)$. Pour tout entier $n>0$, soit

$$x_n=\sum_{\substack{Y\in\mathbf{P}_H\\ f_Y=n\\ YH\in\mathrm{pr}}}1. \tag{1}$$

Par orthogonalité,

$$h_\infty x_n=\sum_{\chi\in\Xi}\chi(H)u(\chi,n), \tag{2}$$

où, pour tout entier $j>0$,

$$u(\chi,j)=\sum_{\substack{Y\in\mathbf{P}_H\\ f_Y=j}}\chi(Y). \tag{3}$$

La somme $u(\chi,j)$ est la somme $b(\chi,(1),H,\Psi,j)$ définie par (III.24) où l'on prend pour Ψ le morphisme trivial. Soit Ξ_1 le sous-groupe de Ξ formé par les caractères triviaux sur $\operatorname{Ker}\varphi$. Ce sous-groupe est d'ordre f_∞, d'où, avec (III.25),

$$\Big|n\sum_{\substack{\chi\in\Xi\\ \chi\notin\Xi_1}}u(\chi,n)\Big|\leq(h_\infty-f_\infty)((2g-2+f_\infty)q^{n/2}+\omega(H)+\Delta_n). \tag{4}$$

Soit $\chi \in \Xi_1$. Alors $u(\chi, j)$ est la somme $a(\chi, H, j)$ définie par (III.28). D'après (III.29),

$$\left| n \sum_{\chi \in \Xi_1} u(\chi, n) - f_\infty q^n \right| \leq f_\infty (2gq^{n/2} + 2 + \omega(H) + \Delta_n). \tag{5}$$

Avec (2), (4) et (5), il vient

$$|nh_\infty x_n - f_\infty q^n| \leq h_\infty (2gq^{n/2} + \omega(H) + \Delta_n) + (h_\infty - f_\infty)(f_\infty - 2)q^{n/2} + 2f_\infty,$$

d'où, avec (III.11),

$$|nhx_n - q^n| \leq h(2gq^{n/2} + \omega(H) + \Delta_n) + (h-1)(f_\infty - 2)q^{n/2} + 2.$$

Ceci achève la démonstration lorsque $H \neq (1)$. On procède de même si $H = (1)$. D'après (III.30), dans la majoration (5), on peut remplacer $2 + \omega(H)$ par 0, d'où la majoration annoncée.

THÉORÈME III.11. *Pour tout entier n non nul et divisible par f_∞ on a*

$$\left| n \operatorname{pr} p_n - \frac{q^n}{h} \right| \leq 2gq^{n/2} + \Delta_n + \left(1 - \frac{1}{h}\right)(f_\infty - 2)q^{n/2}. \tag{III.33}$$

Preuve. Il suffit d'appliquer (III.31) dans le cas où $H = (1)$.

Avant de revenir au cas général pour donner la preuve du "théorème des éléments premiers", restons encore dans le cas particulier de l'anneau $\mathsf{A} = O_{\{\infty\}}$ pour majorer une somme de symboles d'Eisenstein.

PROPOSITION III.12. *Soit H un idéal de A différent de A et possédant un facteur premier P tel que $v_P(H) \leq l_P - 1$. Alors, pour tout entier $n \geq 1$,*

$$n \left| \sum_{\substack{\pi \in \Pi \\ (\pi, H) = 1 \\ \deg_{\{\infty\}}(\pi) = n}} \left(\frac{\pi}{H}\right) \right| \leq (q-1)((2g - 2 + f_\infty + f_{F(H)})q^{n/2} + \Delta_n), \tag{III.34}$$

$F(H)$ désignant le produit des facteurs premiers distincts de H.

Preuve. Pour chaque idéal $P \in \operatorname{pr} \mathbf{P}$, il existe un unique élément unitaire $\beta_P \in M$ tel que $P = \mathsf{A}\beta_P$. Comme k^* est le groupe des unités de A, tout autre générateur de P est de la forme $y\beta_P$, $y \in k^*$. Par suite,

$$\begin{aligned} \sum_{\substack{\pi \in \Pi \\ (\pi, H) = 1 \\ \deg_{\{\infty\}}(\pi) = n}} \left(\frac{\pi}{H}\right) &= \sum_{\substack{\pi \in \Pi \cap M \\ (\pi, H) = 1 \\ \deg_{\{\infty\}}(\pi) = n}} \sum_{y \in k^*} \left(\frac{y\pi}{H}\right), \\ \sum_{\substack{\pi \in \Pi \\ (\pi, H) = 1 \\ \deg_{\{\infty\}}(\pi) = n}} \left(\frac{\pi}{H}\right) &= \sum_{\substack{\pi \in \Pi \cap M \\ (\pi, H) = 1 \\ \deg_{\{\infty\}}(\pi) = n}} \left(\frac{\pi}{H}\right) \sum_{y \in k^*} \left(\frac{y}{H}\right). \end{aligned} \tag{1}$$

Supposons que l'application $y \mapsto \left(\frac{y}{H}\right)$ ne soit pas triviale sur le groupe k^*. Par orthogonalité,

$$\sum_{y \in k^*} \left(\frac{y}{H}\right) = 0$$

et (III.34) est trivialement vérifiée.

Supposons maintenant que l'application $y \mapsto \left(\frac{y}{H}\right)$ soit triviale sur le groupe k^*. On peut alors définir un morphisme Ψ' du semi-groupe $\mathrm{pr}_H(\mathsf{A})$ dans le groupe μ_l par $\Psi'(Y) = \left(\frac{y}{H}\right)$ si $y \in \mathsf{A}$ engendre l'idéal principal Y. Ce morphisme admet une unique extension Ψ'' au groupe $\mathrm{pr}\,\mathbf{FI}_H(\mathsf{A})$, $\mathrm{pr}\,\mathbf{FI}_H(\mathsf{A})$ étant le groupe des idéaux principaux fractionnaires de A dans K premiers à H. Comme le groupe $\mathrm{pr}\,\mathbf{FI}_H(\mathsf{A})$ est d'indice fini dans le groupe $\mathbf{FI}_H(\mathsf{A})$, le morphisme Ψ'' admet une extension Ψ au groupe $\mathbf{FI}_H(\mathsf{A})$. Cette extension est à valeurs dans un groupe μ_m de racines m-ièmes de l'unité, m étant un multiple de l. L'égalité (1) peut donc s'écrire

$$\sum_{\substack{\pi \in \Pi,\,(\pi,H)=1 \\ \deg_{\{\infty\}}(\pi)=n}} \left(\frac{\pi}{H}\right) = (q-1) \sum_{\substack{P \in \mathrm{pr} \cap \mathbf{P}_H \\ f_P = n}} \Psi(P). \tag{2}$$

Posons

$$H = P_1^{m_1} \cdots P_r^{m_r} \tag{3}$$

où $P_1, \ldots, P_r$ sont des idéaux premiers deux à deux distincts et $m_1, \ldots, m_r$ des entiers strictement positifs. Supposons pour fixer les idées que

$$0 < m_r < l_{P_r}. \tag{4}$$

Posons aussi

$$F = P_1 \cdots P_r. \tag{5}$$

Soient ω_{P_r} un générateur du groupe multiplicatif du corps A/P_r et $\xi_r \in \mathsf{A}$ tel que

$$\sigma_{P_r}(\xi_r) = \omega_{P_r}. \tag{6}$$

σ_{P_r} ayant été défini au paragraphe II. D'après le théorème des restes chinois, il existe $\xi \in \mathsf{A}$ tel que

$$\xi \equiv 1 \bmod P_i, \quad 1 \leq i \leq r-1, \quad \xi \equiv \xi_r \bmod P_r. \tag{7}$$

Avec (II.8) et (II.9), puis (II.1) et (II.6),

$$\left(\frac{\xi}{H}\right) = \left(\frac{\xi_r}{P_r}\right)^{m_r} = \chi_{P_r}(\omega_{P_r})^{m_r},$$

où χ_{P_r} est le caractère d'ordre exactement l_{P_r} précédemment choisi. On a donc $(\xi/H) \neq 1$ et l'application $\eta \mapsto (\eta/H)$ n'est pas triviale sur A.

L'homomorphisme Ψ n'est pas trivial sur l'ensemble des idéaux principaux. D'autre part, d'après (II.8) et (II.9), si $\xi \in \mathsf{A}$ est congru à 1 modulo F,

$$\left(\frac{\xi}{H}\right) = \left(\frac{1}{H}\right) = 1 \quad \text{et} \quad \Psi((\xi)) = 1.$$

Le morphisme Ψ vérifie la condition (III.22). En fait il vérifie la condition plus forte (III.22′). Avec (2),

$$\sum_{\substack{\pi\in\Pi\\(\pi,H)=1\\ \deg_{\{\infty\}}(\pi)=n}} \left(\frac{\pi}{H}\right) = (q-1) \sum_{\substack{P\in\mathbf{P}\cap\mathrm{pr}\\(P,H)=1\\ f_P=n}} \Psi(P) = (q-1)t(\Psi,F,n),$$

$t(\Psi,F,n)$ étant défini par (III.26). On conclut avec (III.27).

Revenons au cas général pour démontrer le "théorème des éléments premiers". Le cas où S est réduit a un seul élément ayant été traité, nous supposerons que S a $s+1 \geq 2$ éléments. Soit

$$d_S = \min\{f_v\,;\, v \in S\}.$$

Soit $\infty = v_\infty$ une place de S telle que $f_\infty = d_S$. Considérons l'anneau $\mathsf{A} = O_{\{\infty\}}$. Soit $S' = S - \{\infty\}$. Pour $v \in S'$, soit P_v l'idéal premier de A associé à la place v et soit h_v l'ordre de la classe de l'idéal P_v dans le groupe $\mathcal{C}\ell(\mathsf{A})$ des classes d'idéaux de A. Pour $v \in S'$, l'idéal $P_v^{h_v}$ est principal engendré par un élément unitaire γ_v. On note ici que cet élément γ_v est inversible dans l'anneau O_S. On a dans l'anneau A,

$$P_v^{h_v} = (\gamma_v) = \mathsf{A}\gamma_v \quad \text{pour tout } v \in S'. \tag{III.35}$$

Le "théorème des éléments premiers" pour l'anneau O_S peut s'énoncer de la façon suivante.

THÉORÈME III.13. *Soit* $\mathbf{n} = (n_v)_{v\in S}$ *un* $(s+1)$*-uple d'entiers rationnels tel que* $\|\mathbf{n}\| > 0$. *Alors, on a*

$$\left|\|\mathbf{n}\|p_{\mathbf{n}} - \frac{q^{\|\mathbf{n}\|}}{h}\right| \tag{III.36}$$
$$\leq q^{\|\mathbf{n}\|/2}\left(2g + \frac{q}{q-1} + \left(1-\frac{1}{h}\right)(d_S-2)\right) + 2g\,\frac{q^{\|\mathbf{n}\|/4+1/2}}{q^{1/2}-1} + s + \delta(\|\mathbf{n}\|) + \frac{2}{h},$$

$\delta(\|\mathbf{n}\|)$ *étant le nombre de diviseurs de* $\|\mathbf{n}\|$ *différents de* $\|\mathbf{n}\|$.

Preuve. Pour $v \in S'$, soient m_v et r_v définis par les relations

$$n_v = h_v m_v + r_v, \quad 0 \leq r_v < h_v. \tag{1}$$

Pour $a \in K$, soit $a' = a\prod_{v\in S'} \gamma_v^{-m_v}$. L'application $a \mapsto a'$ est bijective. De plus, les idéaux $O_S a$ et $O_S a'$ sont égaux. En appliquant la formule du

produit aux éléments unitaires γ_v, on obtient que $a \in X_{\mathbf{n}}$ si et seulement si les trois conditions suivantes sont vérifiées :

(i) $a' \in \mathsf{A}$,
(ii) $v(a') = r_v$ pour tout $v \in S'$,
(iii) $f_\infty v_\infty(a') = f_\infty n_\infty + \sum_{v\in S'} f_v m_v h_v$.

Pour tout $a \in X_{\mathbf{n}}$, l'idéal $O_S a = O_S a'$ est un idéal premier de O_S si et seulement si l'idéal $P = a' \prod_{v\in S'} P_v^{-r_v}$ est un idéal premier de l'anneau A. Cet idéal est de degré

$$f_P = -f_\infty v_\infty(a') - \sum_{v\in S'} f_v r_v,$$

soit compte tenu de (iii) et (1),

$$f_P = -f_\infty n_\infty - \sum_{v\in S'} f_v(m_v h_v + r_v) = -f_\infty n_\infty - \sum_{v\in S'} f_v n_v = \|\mathbf{n}\|.$$

Posons

$$H = \prod_{v\in S'} P_v^{r_v}. \tag{2}$$

Le nombre $p_{\mathbf{n}}$ est donc égal au nombre d'idéaux premiers P de l'anneau A tels que

(i) PH est principal,
(ii) $(P, H) = 1$,
(iii) $f_P = \|\mathbf{n}\|$.

Les calculs précédents montrent que $\|\mathbf{n}\| + f_H$ est congru à 0 modulo f_∞. La proposition III.10 jointe à (III.8) et (III.4) nous donne

$$\begin{aligned}|h\|\mathbf{n}\|p_{\mathbf{n}} - q^{\|\mathbf{n}\|}| \le hq^{\|\mathbf{n}\|/2}\left(2g + \frac{q}{q-1} + \left(1 - \frac{1}{h}\right)(f_\infty - 2)\right)\\ + 2g\,\frac{q^{1/2+n/4}}{q^{1/2}-1} + s + \delta(\|\mathbf{n}\|) + 2,\end{aligned}$$

ce qui donne la majoration annoncée.

IV. Démonstration des théorèmes 2 et 3. Rappelons que A désigne l'anneau $O_{\{\infty\}}$. Soit H un idéal de A différent de A.

Introduisons quelques notations supplémentaires. Soit $\alpha \in \mathsf{A}$ premier à H et n un entier strictement positif. On désigne par $\tau(H, n)$ le nombre d'éléments $\pi \in \Pi_n$ tels que l'idéal $\mathsf{A}\pi$ divise H et par $\lambda(H, \alpha, n)$ le nombre d'éléments $\pi \in \Pi_n$ premiers à H tels que $\alpha\pi$ soit puissance l-ième modulo H.

Ces nombres sont nuls si n n'est pas divisible par f_∞. On pose aussi

$$\Phi(H) = \prod_{P\in\mathbf{P},\, P|H} l_P, \tag{IV.1}$$

$$\Psi(H) = \sum_{D\in\mathbf{I},\, D|H} f_D \Phi^-(D), \tag{IV.2}$$

où

$$\Phi^-(Y) = \prod_{P\in\mathbf{P},\, P|Y} (l_P - 1). \tag{IV.3}$$

On a alors la

PROPOSITION IV.1. *Soient H un idéal de A différent de A et un entier $n > 0$ divisible par f_∞. Pour tout $\alpha \in \mathsf{A}$ premier à H on a*

$$\begin{aligned}\left|\frac{n\Phi(H)\lambda(H,\alpha,n)}{q-1} - \frac{q^n}{h}\right| &\le \frac{n\tau(H,n)\Phi(H)}{(q-1)(l,q^{n-1}-1)} + \Delta_n\Phi(H)\\ &\quad + q^{n/2}\left(\Phi(H)(2g-2+f_\infty) + \Psi(H) + \frac{2-f_\infty}{h}\right).\end{aligned} \tag{IV.4}$$

Preuve. Soient J un idéal et

$$H = F(J) = \prod_{P\in\mathbf{P},\, P|J} P.$$

Soit $\xi \in \mathsf{A}$. Alors ξ est premier à J si et seulement si il est premier à H. Soit $\xi \in \mathsf{A}$ premier à H. Si ξ est puissance l-ième modulo J, ξ est puissance l-ième modulo H. Réciproquement, si ξ est puissance l-ième modulo H, ξ est puissance l-ième modulo tous les facteurs premiers de J. D'après le lemme de Hensel et le théorème des restes chinois, ξ est puissance l-ième modulo J. Par suite,

$$\lambda(J,\alpha,n) = \lambda(H,\alpha,n).$$

De façon évidente,

$$\tau(H,n) = \tau(J,n), \quad \Phi(H) = \Phi(J), \quad \Psi(H) \le \Psi(J).$$

Il suffit donc d'établir la proposition dans le cas où l'idéal H est sans facteur carré, ce que nous supposerons désormais.

Posons, pour tout idéal Y,

$$Y^* = \prod_{P\in\mathbf{P},\, P|Y} P^{l_P-1}. \tag{1}$$

Remarquons, pour une utilisation future, que le nombre $\Phi(Y)$ défini par (IV.1) est égal au nombre d'idéaux divisant l'idéal Y^*. Soit $\xi \in \mathsf{A}$ premier

à H. On a vu que $\alpha\xi$ est puissance l-ième modulo H si et seulement si pour tout idéal premier P divisant H, $\alpha\xi$ est puissance l-ième modulo P.

D'après la proposition II.1,

$$\lambda(H,a,n)=\sum_{\substack{\pi\in\Pi_n\\(\pi,H)=1}}\prod_{\substack{P\in\mathbf{P}\\P|H}}\left\{\frac{1+\left(\frac{a\pi}{P}\right)+\left(\frac{a\pi}{P}\right)^2+\cdots+\left(\frac{a\pi}{P}\right)^{l_P-1}}{l_P}\right\},$$

d'où, avec (II.8) et (IV.1),

$$\Phi(H)\lambda(H,\alpha,n)=\sum_{\substack{\pi\in\Pi_n\\(\pi,H)=1}}\prod_{\substack{P\in\mathbf{P}\\P|H}}\left\{1+\left(\frac{\alpha\pi}{P}\right)+\left(\frac{\alpha\pi}{P^2}\right)+\cdots+\left(\frac{\alpha\pi}{P^{l_P-1}}\right)\right\}.$$

En développant le produit intérieur, on obtient avec la notation (1),

$$\Phi(H)\lambda(H,\alpha,n)=\sum_{\substack{\pi\in\Pi_n\\(\pi,H)=1}}\sum_{\substack{D\in\mathbf{I}\\D|H^*}}\left(\frac{\alpha\pi}{D}\right).$$

Après inversion de l'ordre des sommations, il vient

$$\Phi(H)\lambda(H,\alpha,n)=\pi_n-\tau(H,n)+\sum_{\substack{D\in\mathbf{I}\\D|H^*,\,D\neq(1)}}\left(\frac{\alpha}{D}\right)\sum_{\substack{\pi\in\Pi_n\\(\pi,H)=1}}\left(\frac{\pi}{D}\right),$$

d'où

$$\Phi(H)\lambda(H,\alpha,n)=\pi_n-\tau(H,n)+\Sigma_n-\Theta_n,$$

avec

$$\Sigma_n=\sum_{\substack{D\in\mathbf{I}\\D|H^*,\,D\neq(1)}}\left(\frac{\alpha}{D}\right)\sum_{\substack{\pi\in\Pi_n\\(\pi,D)=1}}\left(\frac{\pi}{D}\right), \tag{3}$$

$$\Theta_n=\sum_{\substack{D\in\mathbf{I}\\D|H^*,\,D\neq(1)}}\left(\frac{\alpha}{D}\right)\sum_{\substack{\pi\in\Pi_n\\(\pi,D)=1,\,(\pi)|H}}\left(\frac{\pi}{D}\right). \tag{4}$$

Si H n'admet pas de diviseur premier principal de degré n, $\Theta_n=0$. Sinon,

$$|\Theta_n|\le\sum_{\substack{D\in\mathbf{I}\\D|H^*\\D\neq(1)}}\sum_{\substack{\pi\in\Pi_n\\(\pi,D)=1\\(\pi)|H}}1=\sum_{\substack{\pi\in\Pi_n\\(\pi)|H}}\sum_{\substack{D\in\mathbf{I}\\D|(H/(\pi))^*\\D\neq(1)}}1,$$

d'où, avec (IV.2),

$$|\Theta_n|\le\sum_{\substack{\pi\in\Pi_n\\(\pi)|H}}(\Phi(H/(\pi))-1).$$

Soit $\pi \in \Pi_n$ tel que $(\pi)|H$. D'après (IV.1),

$$\Phi(H/(\pi)) = \Big\{ \prod_{\substack{P\in\mathbf{P}\\ P|H}} l_P \Big\} l_{(\pi)}^{-1} = \Phi(H)/l_{(\pi)} = \Phi(H)(l, q^{n-1}-1)^{-1},$$

d'où la majoration,

$$|\Theta_n| \le \tau(H,n)(\Phi(H)(l,q^{n-1}-1)^{-1}-1). \tag{5}$$

On note que (5) reste valable si $\tau(H,n)=0$. Avec (2) et (5) il vient

$$|\Phi(H)\lambda(H,\alpha,n) - \pi_n| \le |\Sigma_n| + \frac{\tau(H,n)\Phi(H)}{(l,q^{n-1}-1)}. \tag{6}$$

D'après la proposition III.12,

$$n|\Sigma_n| \le (q-1) \sum_{\substack{D\in\mathbf{I}\\ D|H^*,\, D\neq(1)}} \{(2g-2+f_\infty+f_{F(D)})q^{n/2} + \Delta_n\},$$

d'où, avec (1) et (IV.1),

$$n|\Sigma_n| \le (q-1)\Big\{(\Phi(H)-1)((2g-2+f_\infty)q^{n/2}+\Delta_n) + q^{n/2} \sum_{\substack{D\in\mathbf{I}\\ D|H^*,\, D\neq(1)}} f_{F(D)}\Big\}.$$

Comme H est sans facteur carré, compte tenu de (1),

$$\sum_{\substack{D\in\mathbf{I}\\ D|H^*,\, D\neq(1)}} f_{F(D)} = \sum_{\substack{D\in\mathbf{I}\\ D|H}} f_D \sum_{\substack{Y\in\mathbf{I}\\ Y|H^*,\, Y\neq(1)\\ F(Y)=D}} 1,$$

d'où, avec (IV.2), (1) et (IV.3),

$$\sum_{\substack{D\in\mathbf{I}\\ D|H^*,\, D\neq(1)}} f_{F(D)} = \sum_{\substack{D\in\mathbf{I}\\ D|H}} f_D \Phi^-(D) = \Psi(H).$$

On en déduit que

$$n|\Sigma_n| \le (q-1)\{(\Phi(H)-1)((2g-2+f_\infty)q^{n/2}+\Delta_n) + q^{n/2}\Psi(H)\}, \tag{7}$$

avec (III.2) et (III.33),

$$\left|\frac{n\pi_n}{q-1} - \frac{q^n}{h}\right| \le 2gq^{n/2} + \Delta_n + \left(1-\frac{1}{h}\right)(f_\infty - 2)q^{n/2}.$$

On a le résultat annoncé avec (6), (7), (IV.1) et (IV.4).

Lemme IV.2. *On a*

$$\sum_{\substack{D\in\mathbf{I}\\ D|H}} f_D(l-1)^{\omega(D)} = (l-1)f_H l^{\omega(H)-1}. \tag{IV.5}$$

Preuve. Le lemme est évident si $\omega(H) = 0$ ou 1. Supposons que $\omega(H) = r \geq 2$. Posons

$$H = \prod_{i=1}^{r} P_i,$$

où $P_1, \ldots, P_r$ sont des idéaux premiers 2 à 2 distincts, ainsi que $f_i = f_{P_i}$ pour tout i. Alors,

$$\begin{aligned}
\sum_{\substack{D \in \mathbf{I} \\ D|H}} f_D (l-1)^{\omega(D)-1} &= \sum_{s=1}^{r} \sum_{\substack{\{1,\ldots,r\} \supset E \\ \#E=s}} \sum_{i \in E} f_i (l-1)^{s-1} \\
&= \sum_{i=1}^{r} f_i \sum_{s=1}^{r} \sum_{\substack{\{1,\ldots,r\} \supset E \\ \#E=s \\ i \in E}} (l-1)^{s-1} \\
&= \sum_{i=1}^{r} f_i \sum_{t=0}^{r-1} \sum_{\substack{\{1,\ldots,r\} \supset F \\ \#F=t \\ i \notin F}} (l-1)^{t} \\
&= \sum_{i=1}^{r} f_i (1+l-1)^{r-1} = l^{r-1} f_H.
\end{aligned}$$

Théorème IV.3. *Soit H un idéal de $\mathsf{A} = O_{\{\infty\}}$ tel que $f_H > 1$. Alors,*

$$\begin{aligned}
&\text{(IV.6)} \quad R_l(\{\infty\}; H) \\
&\leq 1 + 2\left[\log_q \left(h \left\{ a(H) + \frac{b(H)}{\sqrt{ha(H)}} + \frac{2c(H)\log(ha(H))}{\log(q) ha(H)} + \frac{l}{h(l-1)} \right\} \right) \right],
\end{aligned}$$

avec

$$\text{(IV.7)} \quad a(H) = \frac{\varepsilon(f_\infty)}{h} + l^{\omega(H)} \left\{ 2g - 2 + f_\infty + \frac{q}{q-1} \right\} + (l-1) f_H l^{\omega(H)-1},$$

$$\text{(IV.8)} \quad b(H) = 2g l^{\omega(H)} \frac{q^{1/2}}{q^{1/2}-1},$$

$$\text{(IV.9)} \quad c(H) = (1 - \varepsilon(f_\infty)) l^{\omega(H)},$$

où

$$\text{(IV.10)} \quad \varepsilon(j) = \begin{cases} 1 & \text{si } j = 1, \\ 0 & \text{sinon.} \end{cases}$$

Preuve. Soit n un entier divisible par f_∞. D'après (IV.1),

$$\text{(1)} \quad \Phi(H) \leq l^{\omega(H)}.$$

D'après (IV.3), pour tout idéal Y,

$$\Phi^-(Y) \leq (l-1)^{\omega(Y)},$$

d'où, avec (IV.2) puis (IV.5),

$$\Psi(H) \leq \sum_{\substack{D\in\mathbf{I}\\ D|H}} f_D(l-1)^{\omega(D)} = (l-1)f_H l^{\omega(H)-1}. \tag{2}$$

Soit $\alpha \in \mathsf{A}$ premier à H. Compte tenu de (1) et (2), la relation (IV.4) jointe à la majoration triviale

$$n\tau(H,n) \leq (q-1)f_H$$

nous donne

$$\begin{aligned}\frac{nq^{-n/2}\Phi(H)\lambda(H,\alpha,n)}{q-1} \geq \frac{q^{n/2}}{h} - l^{\omega(H)}\Delta_n q^{-n/2} - (l-1)f_H l^{\omega(H)-1}\\ - l^{\omega(H)}(2g-2+f_\infty) - f_H l^{\omega(H)}q^{-n/2} + \frac{f_\infty - 2}{h}.\end{aligned}$$

Avec (III.8) et (III.4), il vient

$$\Delta_n \leq \frac{q^{1+n/2}-1}{q-1} + 2g\,\frac{q^{1/2+n/4}-1}{q^{1/2}-1} + \delta(n) - f_\infty\delta(n/f_\infty).$$

On a donc

$$\begin{aligned}&\frac{nq^{-n/2}\Phi(H)\lambda(H,\alpha,n)}{q-1}\\ &\geq \frac{q^{n/2}}{h} + \frac{f_\infty-2}{h} - (l-1)f_H l^{\omega(H)-1}\\ &- l^{\omega(H)}\left\{2g-2+f_\infty+\frac{q}{q-1}+2g\,\frac{q^{1/2-n/4}}{q^{1/2}-1} + (\delta(n)-f_\infty\delta(n/f_\infty))q^{-n/2}\right\}\\ &- f_H l^{\omega(H)}q^{-n/2}.\end{aligned}$$

Lorsque $f_\infty \neq 1$, on majore trivialement $\delta(n) - \delta(n/f_\infty)$ par n. On pose

$$\varepsilon(j) = \begin{cases} 1 & \text{si } j = 1,\\ 0 & \text{sinon,}\end{cases} \tag{3}$$

$$a = \frac{\varepsilon(f_\infty)}{h} + l^{\omega(H)}\left\{2g-2+f_\infty+\frac{q}{q-1}\right\} + (l-1)f_H l^{\omega(H)-1}, \tag{4}$$

$$b = 2gl^{\omega(H)}\frac{q^{1/2}}{q^{1/2}-1}, \tag{5}$$

$$c = (1-\varepsilon(f_\infty))l^{\omega(H)}. \tag{6}$$

Si n est divisible par f_∞ et tel que

$$\frac{q^{n/2}}{h} > a + bq^{-n/4} + cnq^{-n/2} + f_H l^{\omega(H)} q^{-n/2}, \tag{7}$$

alors

$$\frac{nq^{-n/2}\Phi(H)\lambda(H,\alpha,n)}{q-1} > 0.$$

Soit maintenant un entier n tel que

$$\frac{q^{n/2}}{h} \geq a + \frac{b}{\sqrt{ha}} + \frac{2c\log(ha)}{\log(q)ha} + \frac{l}{h(l-1)}. \tag{8}$$

Les minorations $q^{n/2} > ha$, $a \geq l^{\omega(H)} + (l-1)f_H l^{\omega(H)-1}$ nous donnent les majorations :

$$f_H l^{\omega(H)} q^{-n/2} < \frac{l}{h(l-1)}, \tag{9}$$

$$bq^{-n/4} < \frac{b}{\sqrt{ha}}. \tag{10}$$

Supposons $f_\infty \neq 1$. Alors,

$$ha \geq a \geq \frac{q}{q-1}\, l^{\omega(H)} + (l-1)f_H l^{\omega(H)-1}.$$

La condition $f_H > 1$ nous donne

$$ha \geq \frac{2q}{q-1} + 2 > e = \exp(1).$$

Donc,

$$cnq^{-n/2} \leq \frac{2c\log(ha)}{\log(q)ha}. \tag{11}$$

D'après (3) et (6), si $f_\infty = 1$, $c = 0$ et (11) reste valable. Par suite, tout entier n vérifiant (8) vérifie aussi (7). On a donc

$$R_l(\{\infty\}; H) \leq n, \tag{12}$$

pour tout entier n divisible par f_∞ et vérifiant (8). Ceci prouve le résultat annoncé.

THÉORÈME IV.4. *Soit P un idéal premier de $O_{\{\infty\}}$. Alors,*

$$\begin{aligned} &R_l(\{\infty\}; P) \\ &\leq 1 + 2\left[\log_q\left(h\left\{(l-1)f_P + l\left\{2g - 2 + f_\infty + \frac{q}{q-1} + \frac{2(2-\varepsilon(f_\infty))}{e\log(q)}\right\}\right.\right. \\ &\quad \left.\left. + \frac{\varepsilon(f_\infty)}{h} + \frac{2gl\sqrt{q}}{(\sqrt{q}-1)\sqrt{h(l-1)}}\right\}\right)\right]. \end{aligned} \tag{IV.11}$$

De plus, si f_P est assez grand,

$$\text{(IV.12)}\qquad R_l(\{\infty\};P)$$
$$\le 1+2\left[\log_q\left(h\left\{(l-1)f_P+l\left\{2g-2+f_\infty+\frac{q}{q-1}+\frac{2(1-\varepsilon(f_\infty))}{e\log(q)}\right\}\right.\right.$$
$$\left.\left.+\frac{\varepsilon(f_\infty)}{h}+\frac{2gl\sqrt{q}}{(\sqrt{q}-1)\sqrt{h(l-1)}}\right\}\right)\right].$$

Preuve. Soit un entier $n \ge 1$ divisible par f_∞. Avec (IV.4), (IV.1), (IV.2), (IV.3) et la notation (IV.10),

$$\frac{nl_P\lambda(P,\alpha,n)}{q-1}\ge\frac{q^n}{h}-\frac{n\tau(P,n)l}{q-1}-l\Delta_n$$
$$-q^{n/2}\left((l-1)f_P+l(2g-2+f_\infty)-\frac{\varepsilon(f_\infty)}{h}\right).$$

On majore $\tau(P,n)$ par $q-1$. Comme ci-dessus, avec (III.8), (III.4) et (IV.10), il vient

$$\frac{nl_P\lambda(P,\alpha,n)q^{-n/2}}{q-1}$$
$$\ge\frac{q^{n/2}}{h}-(l-1)f_P$$
$$-l\left\{2g-2+f_\infty+\frac{q}{q-1}+2g\,\frac{q^{1/2-n/4}}{q^{1/2}-1}+(2-\varepsilon(f_\infty))nq^{-n/2}\right\}-\frac{\varepsilon(f_\infty)}{h}$$
$$\ge\frac{q^{n/2}}{h}-(l-1)f_P$$
$$-l\left\{2g-2+f_\infty+\frac{q}{q-1}+\frac{2(2-\varepsilon(f_\infty))}{e\log(q)}+2g\,\frac{q^{1/2-n/4}}{q^{1/2}-1}\right\}-\frac{\varepsilon(f_\infty)}{h}$$

et $\lambda(P,\alpha,n)>0$ pour tout entier n divisible par f_∞ et tel que

$$\text{(1)}\qquad\frac{q^{n/2}}{h}>(l-1)f_P+l\left\{2g-2+f_\infty+\frac{q}{q-1}+\frac{2(2-\varepsilon(f_\infty))}{e\log(q)}\right\}$$
$$+\frac{\varepsilon(f_\infty)}{h}+\frac{2gl\sqrt{q}}{(\sqrt{q}-1)\sqrt{h(l-1)}}.$$

Si P n'est pas principal, ou si P est principal et si $n\ne f_P$, $\tau(P,n)=0$, et

$$\frac{nl_P\lambda(P,\alpha,n)q^{-n/2}}{q-1}\ge\frac{q^{n/2}}{h}-l\Delta_nq^{-n/2}-(l-1)f_P-l(2g-2+f_\infty)-\frac{\varepsilon(f_\infty)}{h}.$$

Par suite, $\lambda(P,\alpha,n)>0$ pour tout entier $n\neq f_P$, divisible par f_∞ et tel que

$$\frac{q^{n/2}}{h}>(l-1)f_P+l\left\{2g-2+f_\infty+\frac{q}{q-1}\right\}+\frac{2(1-\varepsilon(f_\infty))}{e\log(q)}+\frac{\varepsilon(f_\infty)}{h}+\frac{2gl\sqrt{q}}{(\sqrt{q}-1)\sqrt{h(l-1)}}. \tag{2}$$

On a donc $R_l(\{\infty\};P)\leq n$ pour tout entier $n\neq f_P$ divisible par f_∞ et vérifiant (2). Si l'idéal P est tel que

$$q^{f_P/2}>h\left\{(l-1)f_P+l\left\{2g-2+f_\infty+\frac{q}{q-1}\right\}+\frac{2(1-\varepsilon(f_\infty))}{e\log(q)}+\frac{\varepsilon(f_\infty)}{h}+\frac{2gl\sqrt{q}}{(\sqrt{q}-1)\sqrt{h(l-1)}}\right\},$$

il existe $n<f_P$ divisible par f_∞ et vérifiant (2), d'où la deuxième partie du théorème.

Nous revenons au cas général. Le cas où S est réduit à une seule place venant d'être traité, nous supposerons ici que S a $s+1\geq 2$ éléments. Nous utiliserons les notations introduites à la fin de la section III, en particulier la notation (III.36). Posons

$$D_S=\max\{f_v\,;\,v\in S\}. \tag{IV.13}$$

Théorème IV.5. *Soit $\mathcal{H}$ un idéal non nul de O_S différent de O_S. Alors,*

$$R_l(S;\mathcal{H})\leq 1+\max\left(D_S,2\left[\log_q\left(h\left\{a(\mathcal{H})+\frac{b(\mathcal{H})}{\sqrt{ha(\mathcal{H})}}+\frac{2c(\mathcal{H})\log(ha(\mathcal{H}))}{\log(q)ha(\mathcal{H})}+\frac{l}{h(l-1)}\right\}\right)\right]\right), \tag{IV.14}$$

avec

$$a(\mathcal{H})=\frac{\varepsilon(d_S)}{h}+l^{\omega(\mathcal{H})}\left\{2g-2+d_S+\frac{q}{q-1}\right\}+(l-1)f_Hl^{\omega(\mathcal{H})-1}, \tag{IV.15}$$

$$b(\mathcal{H})=2gl^{\omega(\mathcal{H})}\frac{q^{1/2}}{q^{1/2}-1}, \tag{IV.16}$$

$$c(\mathcal{H})=(1-\varepsilon(d_S))l^{\omega(\mathcal{H})}. \tag{IV.17}$$

Preuve. Notons ∞ une place de S telle que $f_\infty=d_S=\min\{f_v\,;\,v\in S\}$. Soit $\mathsf{A}=O_{\{\infty\}}$. Pour $v\in S'$, soit P_v l'idéal premier de A associé à la place v et soit h_v l'ordre de la classe de l'idéal P_v dans le groupe $\mathcal{C}\ell(\mathsf{A})$ des classes d'idéaux de A. A la fin de la troisième section, on a vu que pour tout $v\in S'$, il existe un élément unitaire γ_v tel que

$$P_v^{h_v}=(\gamma_v)=\mathsf{A}\gamma_v. \tag{III.35}$$

Cet élément γ_v est inversible dans l'anneau O_S.

Soit $\mathcal{H}$ un idéal non nul de O_S différent de O_S. Alors, $H = \mathcal{H} \cap \mathsf{A}$ est un idéal non nul de A, différent de A et premier au produit $\prod_{v \in S'} P_v$. Soit $n \geq R_l(\{\infty\}; H)$ un entier congru à 0 modulo f_∞. Soit $\alpha \in O_S$ premier à $\mathcal{H}$. Pour $v \in S'$, soient m_v et r_v définis par les relations

$$v(\alpha) = lh_v m_v + r_v, \quad 0 \leq r_v < lh_v. \tag{1}$$

Soit

$$\theta(\alpha) = \prod_{v \in S'} \gamma_v^{-m_v}. \tag{2}$$

Alors, $\alpha\theta(\alpha)^l$ est un élément de l'anneau $\mathsf{A} = O_{\{\infty\}}$, premier à l'idéal H. D'après la définition des nombres $R_l(\{\infty\}; H)$, il existe $p \in \mathsf{A}$ engendrant un idéal premier, premier à l'idéal H, tel que $\deg_{\{\infty\}}(p) = n$ et tel que $p\alpha\theta(\alpha)^l$ soit puissance l-ième modulo l'idéal H. Par suite, il existe $y \in \mathsf{A}$ tel que $(p\alpha\theta(\alpha)^l - y^l) \in H$, d'où $(p\alpha\theta(\alpha)^l - y^l) \in \mathcal{H}$. Comme $\theta(\alpha)$ est une unité de O_S, $(p\alpha - (y/\theta(\alpha))^l) \in \mathcal{H}$, avec $(y/\theta(\alpha)) \in O_S$. Dans l'anneau O_S, $p\alpha$ est puissance l-ième modulo l'idéal $\mathcal{H}$. Comme p engendre un idéal premier dans A, si $\mathsf{A}p \notin \{P_v\,;\, v \in S'\}$, p engendre aussi un idéal premier dans O_S. Celà est en particulier réalisé si $n > f_v$ pour tout $v \in S'$. Par suite,

$$R_l(S; \mathcal{H}) \leq \max(1 + \max\{f_v\,;\ v \in S'\}, R_l(\{\infty\}; H)). \tag{3}$$

On applique la majoration (IV.6) en remarquant que $\omega(H) = \omega(\mathcal{H})$ et que $f_{\mathcal{H}} = f_{\mathcal{H} \cap \mathsf{A}}$.

Corollaire IV.6. *Soit $\mathcal{H}$ un idéal de O_S différent de O_S et tel que $f_{\mathcal{H}} \geq q^2$. Alors, on a*

$$R_l(S; \mathcal{H}) \ll \frac{f_{\mathcal{H}}}{\log(f_{\mathcal{H}})}, \tag{IV.18}$$

la constante contenue dans le symbole $\ll$ ne dépendant que de K, S et l.

Preuve. Avec (IV.14) et (III.6).

Théorème IV.7. *Soit $\mathcal{P}$ un idéal premier de O_S. Alors,*

$$R_l(S; \mathcal{P}) \leq 1 + \max\Bigg(D_S, 2\Bigg[\log_q\Bigg(h\Bigg\{(l-1)f_{\mathcal{P}} + l\Bigg(2g-2+d_S+\frac{q}{q-1}+\frac{2(2-\varepsilon(d_S))}{e\log(q)}\Bigg)+\frac{\varepsilon(d_S)}{h}+\frac{2gl\sqrt{q}}{(\sqrt{q}-1)\sqrt{h(l-1)}}\Bigg\}\Bigg)\Bigg]\Bigg). \tag{IV.19}$$

De plus, si $f_{\mathcal{P}}$ est assez grand,

$$R_l(S; \mathcal{P}) \leq 1 + 2\Bigg[\log_q\Bigg(h\Bigg\{(l-1)f_{\mathcal{P}} + l\Bigg(2g-2+d_S+\frac{q}{q-1}+\frac{2(1-\varepsilon(d_S))}{e\log(q)}\Bigg)+\frac{\varepsilon(d_S)}{h}+\frac{2gl\sqrt{q}}{(\sqrt{q}-1)\sqrt{h(l-1)}}\Bigg\}\Bigg)\Bigg]. \tag{IV.20}$$

Preuve. On reprend la preuve du théorème IV.5 en remplaçant l'idéal $\mathcal{H}$ par un idéal premier $\mathcal{P}$. L'idéal $P = \mathcal{P} \cap \mathsf{A}$ est premier dans A. On applique alors le théorème IV.4.

V. Le cas polynomial. On désigne maintenant par A l'anneau $k[T]$ des polynômes à coefficients dans le corps k. L'anneau A est l'anneau O_S lorsque S est réduit à la place infinie associée la valuation $(1/T)$-adique. Dans ce cas, $f_\infty = 1$ et $g = 0$.

Pour tout polynôme $H \in \mathsf{A}$ non constant on désigne par $r_l(H)$ le plus petit entier n tel que pour tout polynôme $A \in \mathsf{A}$ premier à H, il existe $Q \in \mathsf{A}$, polynôme irréductible de degré n, premier à H, tel que AQ soit puissance l-ième modulo H.

Les théorèmes IV.3 et IV.4 deviennent les théorèmes V.1 et V.2 qui suivent. On notera la forme plus précise du théorème V.2.

THÉORÈME V.1. *Soit H un polynôme différent de* 1. *Alors*,

$$r_l(H) \le 1 + 2\left[\log_q\left((l-1)l^{\omega(H)-1}\deg H + \frac{l^{\omega(H)}}{q-1} + \frac{2l-1}{l-1}\right)\right]. \tag{V.1}$$

THÉORÈME V.2. *Soit $P \in \mathsf{A}$ un polynôme irréductible. Alors*,

$$r_l(P) \le 1 + 2\left[\log_q\left((l-1)\deg P + \frac{2l}{e\log(q)} + \frac{l}{q-1} + 1\right)\right]. \tag{V.2}$$

Si de plus,

$$q^{\deg P} > q\left((l-1)\deg P + \frac{l}{q-1} + 1\right)^2, \tag{V.3}$$

alors,

$$r_l(P) \le 1 + 2\left[\log_q\left((l-1)\deg P + \frac{l}{q-1} + 1\right)\right]. \tag{V.4}$$

En outre, *si*

$$q > \left(\frac{(2q-1)l}{q-1} - 1\right)^2, \tag{V.5}$$

la relation (V.4) *est vérifiée pour tout polynôme irréductible P de degré* $\deg P \ge 2$.

Preuve. La relation (V.2) est la simple écriture de (IV.8) dans le cas polynomial. On suppose $n < \deg P$. Dans ce cas, la proposition IV.1 nous donne $\tau(P, n) = 0$ et

$$\frac{nl_P\lambda((P), A, n)q^{-n/2}}{q-1} \ge q^{n/2} - \left(\frac{l}{q-1} + 1 + (l-1)\deg P\right). \tag{1}$$

On a $\lambda((P), A, n) > 0$ pour tout entier n tel que

$$q^{n/2} > \frac{l}{q-1} + 1 + (l-1)\deg P. \tag{2}$$

On a donc $r_l(P) \leq n$ pour tout entier n tel que

$$1 \leq n < \deg P \quad \text{et} \quad q^{n/2} > \frac{l}{q-1} + 1 + (l-1)\deg P.$$

Ces deux dernières conditions peuvent être réalisées simultanément si

$$q^{\deg P} > q\left((l-1)\deg P + \frac{l}{q-1} + 1\right)^2, \tag{3}$$

d'où

$$r_l(P) \leq 1 + 2\left[\log_q\left((l-1)\deg P + \frac{l}{q-1} + 1\right)\right]$$

pour tout polynôme irréductible P dont le degré vérifie la condition (3). Si $q > \left(\frac{(2q-1)l}{q-1} - 1\right)^2$, (3) est réalisée dès que $\deg P \geq 2$. La minoration ci-dessus est réalisée dès que $q \geq (2l-1)^2 + 2$. D'où, les deux dernières parties de la proposition.

Remarque V.3. *Soit P un polynôme irréductible de degré* 1. *Alors*, $r_l(P) = 1$.

Preuve. Pour tout polynôme A premier à P, il existe un polynôme unitaire Q de degré 1, inverse de A modulo P. Comme AQ est congru à 1 modulo P, AQ est une puissance l-ième modulo P. Ce polynôme Q est irréductible.

Notons que la majoration (V.1) donne pour $l = 2$:

$$r_2(H) \leq 1 + 2\left[\log_q\left(2^{\omega(H)-1}\deg H + \frac{2^{\omega(H)}}{q-1} + 3\right)\right].$$

Rappelons que $r_2(H)$ est le plus petit entier n tel que pour tout polynôme $B \in \mathsf{A}$ premier à H, il existe $Q \in \mathsf{A}$, polynôme irréductible de degré n, premier à H, tel que BQ soit carré modulo H. Rappelons aussi que d'après [3, corollaire II.3],

$$R_2(H) \leq 1 + 2\left[\log_q\left(2^{\omega(H)-1}\deg H + \frac{2^{\omega(H)}}{q-1} + 2\right)\right],$$

où $R_2(H)$ est le plus petit entier n tel que pour tout polynôme $B \in \mathsf{A}$ premier à H, il existe $Q \in \mathsf{A}$, polynôme irréductible *unitaire* de degré n, premier à H, tel que BQ soit carré modulo H.

Si l'on suppose que l divise $q-1$, hypothèse réalisée quand $l = 2$, alors pour tout entier $n > 0$, $(l, q^{n-1} - 1) = l$ et $(l, q^{n-1} - 1)^{-1}$ peut être majoré

par $1/l$ au lieu d'être majoré trivialement par 1, ce qui dans le cas général conduit à remplacer la majoration (IV.6) par la majoration

$$R_l(\{\infty\};H) \le 1 + 2\left[\log_q\left(h\left\{a(H) + \frac{b(H)}{\sqrt{ha(H)}} + \frac{2c(H)\log(ha(H))}{\log(q)ha(H)} + \frac{1}{h(l-1)}\right\}\right)\right],$$

ce qui donne dans le cas polynomial,

$$r_l(H) \le 1 + 2\left[\log_q\left((l-1)l^{\omega(H)-1}\deg H + \frac{l^{\omega(H)}}{q-1} + \frac{l}{l-1}\right)\right].$$

On obtient alors, pour $l = 2$, la même majoration que celle obtenue pour le nombre $R_2(H)$ dans [3]. Il est naturel de s'intéresser à une généralisation des nombres $R_2(H)$. Si $H \in \mathsf{A}$ est un polynôme non constant, on désigne par $R_l(H)$ le plus petit entier n, s'il existe, tel que pour tout polynôme $B \in \mathsf{A}$ premier à H, il existe $Q \in \mathsf{A}$, polynôme irréductible *unitaire* de degré n, premier à H, tel que BQ soit puissance l-ième modulo H. On pourrait penser adapter au cas général la méthode utilisée dans [3] pour majorer $R_2(H)$. Une telle tentative échoue. Une analyse rapide de la preuve donnée dans [3] explique cet échec. La preuve donnée dans [3] utilise deux propriétés. L'une de ces propriétés est la loi de réciprocité quadratique qui se généralise en une loi de réciprocité l-ième lorsque l divise $q-1$ [17, Théorème 3.3]. La deuxième propriété, utilisée de façon implicite, est l'unicité du caractère quadratique du groupe multiplicatif d'un corps fini. Cette dernière propriété est propre aux caractères d'ordre 2 et ne se généralise pas aux caractères d'ordre $l > 2$.

Références

[1] N. C. Ankeny, *The least quadratic non residue*, Ann. of Math. (2) 55 (1952), 65–72.

[2] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen*, Math. Z. 19 (1924), 153–246.

[3] M. Car, *Résidus quadratiques dans* $\mathbb{F}_q[T]$, Acta Arith. 104 (2002), 137–153.

[4] M. Deuring, *Lectures on the Theory of Algebraic Functions of One Variable*, Lecture Notes in Math. 314, Springer, 1973.

[5] K. Dickman, *On the frequency of numbers containing prime factors of a certain relative magnitude*, Ark. Mat. Astr. Fys. 22 (1930), 1–14.

[6] G. Effinger and D. R. Hayes, *Additive Number Theory of Polynomials Over a Finite Field*, Oxford Math. Monogr., 1991.

[7] P. D. T. A. Elliott, *The distribution of power residues and certain related results*, Acta Arith. 17 (1970), 141–159.

[8] —, *The least prime k-th power residue*, J. London Math. Soc. (2) 3 (1971), 205–210.

[9] J. B. Friedlander, *On the least kth power non-residue in an algebraic number field*, Proc. London Math. Soc (3) 26 (1973), 19–34.

[10] J. Jordan, *The distribution of kth power non-residues*, Duke Math. J. 37 (1970), 333–340.
[11] Y. Koshiba, *A number theoretic property of algebraic function fields*, Sci. Rep. Kagoshima Univ. 23 (1974), 1–5 (in Japanese).
[12] —, *An arithmetic property of algebraic function fields*, ibid. 25 (1976), 27–29.
[13] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge Univ. Press, 1997.
[14] R. E. Mac Rae, *On unique factorization in certain rings of algebraic functions*, J. Algebra 17 (1971), 243–261.
[15] T. Nagell, *The least positive nth non-power-residue*, Norsk. Mat. Tidsskr. 34 (1952), 13 (in Norwegian).
[16] K. Norton, *Upper bounds for k-th power cosets representatives modulo n*, Acta Arith. 15 (1969), 161–179.
[17] M. Rosen, *Number Theory in Function Fields*, Grad. Texts in Math. 210, Springer, 2002.
[18] T. Skolem, *Existence of an nth non-power-residue mod p less than* $\sqrt{p}$, Norsk. Mat. Tidsskr. 33 (1951), 123–126 (in Norwegian).
[19] S. A. Stepanov, *Arithmetic of Algebraic Curves*, Monogr. Contemp. Math., Consultants Bureau, New York, 1994.
[20] I. M. Vinogradov, *On the bound of the least non residue of nth powers*, Trans. Amer. Math. Soc. 28 (1927), 218–226.
[21] A. Weil, *Basic Number Theory*, 3rd ed., Grundlehren Math. Wiss. 144, Springer, 1974.
[22] A. Zaharescu, *Small values of* $n^2\alpha \pmod 1$, Invent. Math. 121 (1995), 379–388.

Université Aix-Marseille III
L.A.T.P., U.M.R. 6632
Bâtiment Henri Poincaré
Faculté des Sciences de St-Jérôme
Av. Escadrille Normandie-Niemen
13397 Marseille Cedex 20, France
E-mail: mireille.car@univ.u-3mrs.fr

Reçu le 29.6.2004 (4794)