JOURNAL OF NUMBER THEORY 38, 300–322 (1991)

Tours ramifiées infinies de corps de classes

MARC PERRET

Équipe C.N.R.S. "Arithmétique et Théorie de l'Information," C.I.R.M., Luminy Case 916, 13288 Marseille Cedex 9, France

Communicated by M. Waldschmidt

Received November 6, 1989; revised June 6, 1990

The number $A(q)$ is the upper limit of the maximum number of points of a curve defined over $\mathbf{F}_q$, divided by the genus. A lower bound was established by Serre, using unramified Hilbert class field towers. In this paper, the author gives a conditional criterion of infinitude of ramified class field towers, and applies this result in order to obtain some better lower bounds for $A(q)$. Moreover, the author obtains some slightly weaker unconditional results.

INTRODUCTION

Soit q une puissance d'un nombre premier p et $\mathbf{F}_q$ le corps fini à q éléments. On désigne par $N(g, q)$ le nombre maximum de points rationnels sur $\mathbf{F}_q$ d'une courbe algébrique lisse irréductible de genre g définie sur $\mathbf{F}_q$. Weil a montré dans [16] que

$$N(g, q) \leqslant q + 1 + 2g\sqrt{q}.$$

Cette majoration n'est pas optimale, sauf pour les petites valeurs de g. Afin d'étudier $N(g, q)$ pour les grandes valeurs de g, on pose

$$A(q) = \limsup_{n \to \infty} \frac{N(g, q)}{g}.$$

L'inégalité de Weil montre que $A(q) \leqslant 2\sqrt{q}$. Drinfeld et Vladut ont montré (cf. [2], en utilisant des formules explicites—discrètes—de Weil) que $A(q) \leqslant \sqrt{q} - 1$. D'autre part, Ihara, ainsi que Tsfasman, Vladut, et Zink, ont montré (dans [4, 15], en utilisant des courbes de Shimura) que $A(q^2) = q - 1$. Enfin, Serre a montré (non publié) l'existence d'une constante $c > 0$ telle que, pour tout q, on ait $A(q) > c \log q$. Nous reprenons ici la méthode de Serre pour donner, pour certaines valeurs de q, une meilleure minoration de $A(q)$; la méthode repose sur la construction de

0022-314X/91 $3.00

tours infinies de corps de classes de Hilbert. En généralisant ce procédé à des tours ramifiées de corps de classes, on peut, modulo une conjecture portant sur un critère de non finitude de telles tours, montrer l'existence pour tout nombre premier p d'une constante $c(p)$ telle que, si q est une puissance p, on ait

$$A(q) \geqslant c(p)(\sqrt{q}-1).$$

On montre aussi une minoration non conditionnelle, c'est-à-dire indépendante de toute conjecture: si ℓ est un nombre premier, et si $q \equiv 1$ modulo ℓ, alors

$$A(q^\ell) > \frac{\sqrt{\ell(q-1)}-2\ell}{\ell-1}.$$

La méthode est la suivante: on assimile une courbe algébrique lisse définie sur $\mathbf{F}_q$ à son corps de fonctions, qui est une extension de degré de transcendance 1 de $\mathbf{F}_q$ (c'est-à-dire un corps global de caractéristique p). Un point rationnel sur $\mathbf{F}_q$ de la courbe correspond à une place de degré 1 de son corps de fonctions, et le genre de la courbe est le genre de ce corps. Afin de minorer $A(q)$, il faut donc trouver une suite infinie de corps globaux de caractéristique p ayant asymptotiquement beaucoup de places de degré 1 par rapport au genre. Pour cela, on se donne un tel corps k, un ensemble fini non vide S de places de k, un module $\mathfrak{m}$ sur k, étranger à S, ainsi qu'un nombre premier ℓ. On construit alors une ℓ-tour de corps de classes $(k_n, S_n, \mathfrak{m}_n, \ell)$, et on cherche un critère de non finitude de cette ℓ-tour; un tel critère sera conjecturé dans le cas général, et démontré dans le cas où $\mathfrak{m}=0$, c'est-à-dire dans le cas où la tour considérée est la ℓ-tour de corps de classes de Hilbert de k. Il faut ensuite exhiber explicitement un triplet $(k, S, \mathfrak{m})$ répondant à ce critère, pour lequel on sache évaluer le genre et le nombre de places de degré 1. La minoration de $A(q)$ s'en suit aisément.

On construira au §I la tour $(k_n, S_n, \mathfrak{m}_n, \ell)$ pour un corps global de caractéristique quelconque, et on bornera le degré du discriminant de k_n/k_0 par une expression linéaire en le degré $[k_n : k_0]$ (Théorème 1). Au §II, on conjecturera un critère de non-finitude de la ℓ-tour $(k_n, S_n, \mathfrak{m}_n, \ell)$ (Conjecture 1), ainsi qu'une condition entraînant cette conjecture, la condition étant vérifiée si $\mathfrak{m}=0$ (Théorème 2). Le §III est consacré aux minorations de $A(q)$ que l'on peut établir en admettant la Conjecture 1 pour les corps globaux de caractéristique finie. Ces minorations reposent sur les extensions d'Artin–Schreier de $\mathbf{F}_q(T)$; les résultats sur ces extensions qui nous seront utiles sont rappelés dans la section III, 1. On obtiendra 2 minorations de $A(q)$ (Théorèmes 3 et 4), qui impliquent le résultat plus agréable $A(q) \geqslant c(p)(\sqrt{q}-1)$ (Corollaire 1). Lorsque la conjecture 1 est

démontrée, c'est-à-dire pour les tours non ramifiées, on peut tout de même donner, du moins pour certaines valeurs de q, des minorations de $A(q)$ meilleures que celle de Serre (la "minoration non conditionnelle"); c'est l'objet du §IV. Enfin on donnera au §V des applications de ces résultats à la Théorie des Codes Correcteurs d'Erreurs, puis à la Théorie des Réseaux (empilements de sphères).

Cet article a été en partie annoncé par une note aux Comptes Rendus de l'Académie des Sciences de Paris ([9]).

I. La tour ramifiée de corps de classes

1. *Le corps de classes de rayon*

Soit k un corps global de caractéristique quelconque. On se donne un ensemble fini R de places de k, et pour toute place $\mathfrak{p}$ de R, un entier $m_\mathfrak{p} > 0$; on dispose ainsi d'un module $\mathfrak{m}$ porté par R

$$\mathfrak{m} = \sum_{\mathfrak{p} \in R} m_\mathfrak{p} \mathfrak{p}.$$

Posons

$$W_\mathfrak{m} = k^* \times \prod_{\mathfrak{p} \in R} U_\mathfrak{p}^{m_\mathfrak{p}} \times \prod_{\mathfrak{p} \notin R} U_\mathfrak{p}.$$

Le groupe $W_\mathfrak{m}$ est un sous groupe ouvert d'indice fini du groupe $\mathbf{J}_k$ des idèles de k (cf. [6, 8]). Il définit donc par la Théorie du corps de classes une extension abélienne $k_\mathfrak{m}$ de k, qui n'est ramifiée qu'en les places $\mathfrak{p} \in R$; $k_\mathfrak{m}$ est appelé le corps de classes de rayon $\mathfrak{m}$ de k. Par exemple, si R est vide, alors $\mathfrak{m} = 0$, et k_0 n'est autre que le corps de classes de Hilbert de k.

Soit L une extension abélienne de k. Puisque

$$k^{ab} = \varinjlim_{\mathfrak{m}} k_\mathfrak{m},$$

il existe un plus petit module $\mathfrak{f}$, tel que $L \subset k_\mathfrak{f}$. Ce module $\mathfrak{f}$ est appelé le conducteur de L/k (voir [6, 8]). Le conducteur de L/k divise $\mathfrak{m}$ si et seulement si $k \subset L \subset k_\mathfrak{m}$.

2. *Discriminant d'une extension de conducteur divisant* $\mathfrak{m}$

Si L/K est une extension abélienne, et si $\mathfrak{p}$ est une place de K, on note $\mathfrak{P}$ une place quelconque de L divisant $\mathfrak{p}$. Dans ce paragraphe, on utilisera librement les résultats de [1], ainsi que ceux de [13].

PROPOSITION 1. *Soit L/k une extension abélienne et $\mathfrak{m} = \sum_{\mathfrak{p} \in R} m_{\mathfrak{p}} \mathfrak{p}$ un module sur k. Alors le conducteur de L/k divise $\mathfrak{m}$ si et seulement si les groupes de ramification $\mathrm{Gal}(L_{\mathfrak{P}}/k_{\mathfrak{p}})^{m_{\mathfrak{p}}}$ sont triviaux pour toute place $\mathfrak{p}$ de k.*

Remarque. Si $m_{\mathfrak{p}} = 0$, le groupe de ramification $\mathrm{Gal}(L_{\mathfrak{P}}/k_{\mathfrak{p}})^0$ n'est autre que le groupe d'inertie $D_{\mathfrak{P}}$ de L/K en $\mathfrak{P}$. Celui-ci est trivial si et seulement si la place $\mathfrak{P}$ est non ramifiée dans l'extension L/K.

Preuve. Soient $\mathfrak{p}$ une place de k, et $\psi_{\mathfrak{p}}$ l'application locale de réciprocité de $L_{\mathfrak{P}}/k_{\mathfrak{p}}$; notons $\mathfrak{f}$ le conducteur de L/K. Puisque

$$k_{\mathfrak{p}} \subset L_{\mathfrak{P}} \subset k_{\mathfrak{f},\mathfrak{p}}$$

on a

$$N_{k_{\mathfrak{f},\mathfrak{p}}/k_{\mathfrak{p}}}(k^*_{\mathfrak{f},\mathfrak{p}}) \subset N_{L_{\mathfrak{P}}/k_{\mathfrak{p}}}(L^*_{\mathfrak{P}}) = \mathrm{Ker}(\psi_{\mathfrak{p}}).$$

Mais (cf. [6]),

$$U^{(i)}_{\mathfrak{p}} \subset N_{L_{\mathfrak{P}}/k_{\mathfrak{p}}}(L^*_{\mathfrak{P}}) \Leftrightarrow U^{(i)}_{\mathfrak{p}} \subset k^* N_{L/k}(\mathbf{J}_L),$$

où $U^{(i)}_{\mathfrak{p}}$ désigne le groupe des i-unités de $k_{\mathfrak{p}}$: $U^{(i)}_{\mathfrak{p}} = \{x \in k_{\mathfrak{p}},\ v_{\mathfrak{p}}(x-1) \geqslant i\}$ (on a noté $v_{\mathfrak{p}}$ la valuation de $k_{\mathfrak{p}}$ associée à $\mathfrak{p}$).

Ainsi, $U^{(m_{\mathfrak{p}})}_{\mathfrak{p}} \subset \mathrm{Ker}(\psi_{\mathfrak{p}})$. Comme de plus $\psi_{\mathfrak{p}}(U^{(m_{\mathfrak{p}})}_{\mathfrak{p}}) = G^{m_{\mathfrak{p}}}$, ces derniers groupes sont nuls pour toute place $\mathfrak{p}$ de k si et seulement si $\mathfrak{f}$ divise $\mathfrak{m}$. ∎

PROPOSITION 2. *Soit $\mathfrak{m} = \sum_{\mathfrak{p} \in R} m_{\mathfrak{p}} \mathfrak{p}$ un module sur k, et L/k une extension abélienne de conducteur divisant $\mathfrak{m}$. Alors le discriminant $\mathfrak{d}(L/k)$ de L/k divise $\prod_{\mathfrak{p} \in R} \mathfrak{p}^{m_{\mathfrak{p}}([L_{\mathfrak{P}}/k_{\mathfrak{p}}]-1)}$.*

Preuve. Le problème est local, puisque

$$\mathfrak{d}(L/k) = \prod_{\mathfrak{p} \in R} \mathfrak{d}(L_{\mathfrak{P}}/k_{\mathfrak{p}}).$$

Soit donc $\mathfrak{p}$ une place de R et $G = \mathrm{Gal}(L_{\mathfrak{P}}/k_{\mathfrak{p}})$. La Führerdiskriminantenproduktformuln affirme que

$$\mathfrak{d}(L_{\mathfrak{P}}/k_{\mathfrak{p}}) = \prod_{\chi \in X_{\mathrm{irr}}(G)} \mathfrak{f}(\chi),$$

où $X_{\mathrm{irr}}(G)$ est l'ensemble des caractères irréductibles de G, et où $\mathfrak{f}(\chi)$ désigne le conducteur de χ. Notons que, G étant abélien, $X_{\mathrm{irr}}(G)$ est l'ensemble des caractères de degré 1 de G, et qu'il y a $\mathrm{Card}\, G = [L_{\mathfrak{P}}/k_{\mathfrak{p}}]$ tels caractères. Si χ est trivial, alors $\mathfrak{f}(\chi) = (1)$. Soit χ un caractère non trivial de G, de degré 1, et $\mathrm{Ker}(\chi)$ son noyau. Il lui correspond par la Théorie de Galois une extension intermédiaire $L_{\mathfrak{P},\chi}/k_{\mathfrak{p}}$, de groupe de

Galois $G/\mathrm{Ker}(\chi)$. Puisque $L_{\mathfrak{P},\chi}/k_{\mathfrak{p}}$ est cyclique, son conducteur $\mathfrak{f}(\chi)$ est donné par

$$\mathfrak{f}(\chi)=\mathfrak{p}^{f(\chi)},$$

avec $f(\chi)=c+1$, c étant l'unique entier tel que les groupes de ramification supérieurs satisfassent $G^{c+1}=\{1\}$, et $G^{c}\neq\{1\}$ (c'est le dernier saut de la filtration de G formée des groupes de ramification supérieurs $\{G^{v}\}_{v\geqslant -1}$). Cet entier $c+1$ est inférieur ou égal à $m_{\mathfrak{p}}$ d'après la proposition 1. ∎

3. *Construction de la tour de corps de classes*

On se place dans la situation du paragraphe 1, et on se donne de plus un ensemble fini non vide S de places de k, contenant les places archimédiennes si k est de caractéristique nulle, disjoint de R, ainsi qu'un nombre premier ℓ.

On note k_a la plus grande extension abélienne de k, d'exposant 1 ou ℓ, où les places de S se décomposent totalement, et de conducteur divisant $\mathfrak{m}$. On pose alors S_a (resp. R_a) l'ensemble des places de k_a au-dessus de S (resp. R), et $\mathfrak{m}_a=\sum_{\mathfrak{p}\in R}\sum_{\mathfrak{P}\mid\mathfrak{p}} m_{\mathfrak{p}}\mathfrak{P}=\sum_{\mathfrak{P}\in R_a} m_{\mathfrak{P}}\mathfrak{P}$, avec $m_{\mathfrak{P}}=m_{\mathfrak{p}}$ si $\mathfrak{P}\mid\mathfrak{p}$.

En itérant cette construction, on obtient:

— une suite d'extensions

$$k_0=k,$$
$$k_n=(k_{n-1})_a \qquad \text{pour} \quad n\geqslant 1;$$

— pour chaque corps k_n, deux ensembles finis disjoints de places

$$S_0=S, \qquad R_0=R,$$
$$S_n=(S_{n-1})_a, \qquad R_n=(R_{n-1})_a \qquad \text{pour} \quad n\geqslant 1;$$

— un module porté par R_n

$$\mathfrak{m}_0=\mathfrak{m},$$
$$\mathfrak{m}_n=(\mathfrak{m}_{n-1})_a \qquad \text{pour} \quad n\geqslant 1.$$

Remarque. Si k est de caractéristique finie p, si $\ell=p$, et si $\mathfrak{m}=0$ ou bien $\mathfrak{m}=\mathfrak{p}$ pour une place $\mathfrak{p}$ de k, alors $k_a=k$. En effet, supposons que $\mathfrak{m}=\mathfrak{p}$. L'indice de $\mathrm{Gal}(k_{a,\mathfrak{P}}/k_{\mathfrak{p}})^1$ dans le groupe d'inertie $\mathrm{Gal}(k_{a,\mathfrak{P}}/k_{\mathfrak{p}})^0$, (qui est un p-groupe), est premier à p; ces groupes sont donc égaux, et la nullité de $\mathrm{Gal}(k_{a,\mathfrak{P}}/k_{\mathfrak{p}})^1$ implique la nullité de $\mathrm{Gal}(k_{a,\mathfrak{P}}/k_{\mathfrak{p}})^0$, ce qui revient au choix $\mathfrak{m}=0$. Dans ce cas, k_a/k est une p-extension non ramifiée, ce qui

n'est possible que si $k_a = k$. En effet, si $k_a \neq k$, il existe une extension d'Artin–Shreier K intermédiaire entre k et k_a, nécessairement ramifiée (cf. [7]).

PROPOSITION 3. *Pour tout entier $n \geqslant 1$, l'extension k_n/k_0 est galoisienne.*

Preuve. Elle se fait par récurrence sur $n \in \mathbf{N}^*$. Pour $n = 1$, c'est trivial puisque k_1/k_0 est abélienne. Supposons que k_{n-1}/k_0 soit galoisienne. L'extension k_n/k_0 est alors séparable puisque k_{n-1}/k_0 et k_n/k_{n-1} le sont (la première est galoisienne par hypothèse de récurrence, et la seconde est abélienne par construction).

Pour montrer que k_n/k_0 est normale, soit k_0^{ac} une clôture algébrique de k_0, contenant k_n, et

$$\sigma : k_n \to k_0^{ac}$$

un k_0 plongement de k_n dans k_0^{ac}; il s'agit de montrer que $\sigma(k_n) = k_n$.

Le morphisme σ induit par restriction un k_0 plongement de k_{n-1} dans k_0^{ac}; l'extension k_{n-1}/k_0 étant supposée normale par hypothèse de récurrence, on a donc $\sigma(k_{n-1}) = k_{n-1}$. On est donc en présence d'une extension $\sigma(k_n)/k_{n-1}$, qui est abélienne, d'exposant 1 ou ℓ, où les places de S_{n-1} se décomposent totalement, et de conducteur divisant $\mathfrak{m}_{n-1}$. Il s'en suit par maximalité de k_n vis-à-vis de ces propriétés que $\sigma(k_n) \subset k_n$, ce qui prouve la Proposition 3. ∎

On peut donc poser

$$G_n = \mathrm{Gal}(k_n/k) \qquad \text{pour} \quad n \geqslant 1,$$

$$k_\infty = \bigcup_{n \geqslant 0} k_n,$$

$$G = \mathrm{Gal}(k_\infty/k) = \varprojlim_n G_n.$$

G_1 est un groupe de type $(\ell, ..., \ell)$, les G_n, $n \geqslant 1$, sont des ℓ-groupes, et G est un pro-ℓ-groupe. De plus, $G_1 = G^{\mathrm{ab}}/(G^{\mathrm{ab}})^\ell$, puisque k_1 est la plus grande extension abélienne de k, contenue dans k_∞, d'exposant 1 ou ℓ.

Remarque. Étudions les groupes $\mathrm{Gal}(k_{n+1}/k_n)$. Soit $n \in \mathbf{N}^*$. La plus grande extension abélienne de k_n, où les places de S_n se décomposent totalement, et de conducteur divisant $\mathfrak{m}$, est le corps de classes $\tilde{k}_n$ du groupe de norme (cf. [6])

$$P_n = \prod_{\mathfrak{p} \in S_n} k_{n,\mathfrak{p}}^* \times \prod_{\mathfrak{p} \in R_n} U_{n,\mathfrak{p}}^{m_\mathfrak{p}} \times \prod_{\mathfrak{p} \notin S_n \cup R_n} U_{n,\mathfrak{p}}.$$

Soit $\mathrm{Im}\, P_n$ l'image de P_n dans le groupe des classes d'idèles C_n de k_n. Puisque k_{n+1} est la plus grande extension abélienne d'exposant divisant ℓ de k_n, on peut écrire

$$\mathrm{Gal}(k_{n+1}/k_n) = G(\tilde{k}_n/k_n)/(G(\tilde{k}_n/k_n))^{\ell},$$

c'est-à-dire

$$\mathrm{Gal}(k_{n+1}/k_n) = (C_n/\mathrm{Im}\, P_n)/(C_n/\mathrm{Im}\, P_n)^{\ell}.$$

On en déduit immédiatement que l'extension k_∞/k est finie si et seulement si il existe $n \in \mathbf{N}^*$, tel que le groupe $(C_n/\mathrm{Im}\, P_n)$ soit d'ordre premier à ℓ.

4. *Le discriminant de k_n/k_0*

On suppose maintenant que pour tout $n \in \mathbf{N}^*$, les places de R_n sont totalement ramifiées dans k_{n+1}. On se propose alors de majorer le degré du discriminant de k_n/k_0. Les résultats qui suivent sont classiques; rappelons tout d'abord que si $K \subset L \subset M$ est une tour de corps, alors:

— Le discriminant relatif $\mathfrak{d}(M/K)$ est donné par

$$\mathfrak{d}(M/K) = N_{L/K}(\mathfrak{d}(M/L)) \cdot (\mathfrak{d}(L/K))^{[M:L]};$$

— Si $v_\mathfrak{p}$ est la valuation associée à la place $\mathfrak{p}$ de K, le degré du discriminant de L/K est défini par

$$\deg \mathfrak{d}(L/K) = \sum_{\mathfrak{p}} v_\mathfrak{p}(\mathfrak{d}(L/K)) \cdot \deg \mathfrak{p};$$

— Si $\mathfrak{p}$ est une place de K, en notant $\mathfrak{P}$ les places de L divisant $\mathfrak{p}$,

$$v_\mathfrak{p}(N_{L/K}(\mathfrak{d}(M/L)) = \sum_{\mathfrak{P}\mid\mathfrak{p}} f(\mathfrak{P}/\mathfrak{p})\, v_\mathfrak{P}(\mathfrak{d}(M/L)),$$

où le degré résiduel $f(\mathfrak{P}/\mathfrak{p})$ est le degré de l'extension $\bar{L}_\mathfrak{P}/\bar{K}_\mathfrak{p}$ des corps résiduels.

Nous sommes alors en mesure de prouver le Théorème suivant:

THÉORÈME 1. *Si, pour tout n, les places de R_n se ramifient totalement dans k_{n+1}, alors*

$$\deg \mathfrak{d}(k_n/k_0) \leqslant ([k_n : k_0] - 1) \deg \mathfrak{m}.$$

Remarque. Ce Théorème est bon car en général, on ne peut majorer le degré du discriminant que par un terme de l'ordre de $[k_n : k_0] \log [k_n : k_0]$.

Preuve. Puisque les ramifications sont totales, les degrés résiduels en les places ramifiées valent 1, et pour chaque place $\mathfrak{p}$ de R_{i-1}, il n'y a qu'une seule place $\mathfrak{P}$ de k_i au-dessus de $\mathfrak{p}$. Les rappels ci-dessus permettent d'écrire

$$\deg \mathfrak{d}(k_i/k_0) = [k_i: k_{i-1}] \deg \mathfrak{d}(k_{i-1}/k_0) + \sum_{\mathfrak{p} \in R_{i-1}} v_{\mathfrak{p}}(\mathfrak{d}(k_i: k_{i-1})) \deg v_{\mathfrak{p}}.$$

D'après la Proposition 2,

$$v_{\mathfrak{p}}(\mathfrak{d}(k_i: k_{i-1})) \leqslant m_{\mathfrak{p}}([k_i: k_{i-1}] - 1),$$

d'où, puisque $\deg \mathfrak{m} = \sum_{\mathfrak{p} \in R_0} m_{\mathfrak{p}} \deg v_{\mathfrak{p}}$,

$$\deg \mathfrak{d}(k_i/k_0) + \deg \mathfrak{m} \leqslant [k_i: k_{i-1}](\deg \mathfrak{d}(k_{i-1}/k_0) + \deg \mathfrak{m}).$$

En sommant ces inégalités pour $1 \leqslant i \leqslant n$, on obtient le résultat annoncé. ∎

Voici un cas particulier qui nous sera utile, pour lequel l'hypothèse du Théorème 1 est vérifiée:

PROPOSITION 4. *Si R_0 est réduit à une unique place et si $\ell = p$ est la caractéristique de k_0, alors pour tout $n \geqslant 0$, R_n est réduit à une unique place, et les ramifications sont totales.*

Preuve. L'extension k_1/k_0 étant d'exposant p, c'est une extension d'Artin-Schreier, ramifiée en une unique place; la ramification est donc totale (voir [7]). R_1 est donc réduit à une unique place, et la Proposition en découle par récurrence. ∎

II. CRITÈRE DE NON-FINITUDE

1. *Générateurs et relations dans un p-groupe*

a. *Le Théorème de Golod et Shafarevich*

Pour plus de détails sur cette partie, voir [12]. Soit G un groupe noté multiplicativement, et p un nombre premier. On note G^{ab} l'abélianisé de G, et $G/p = G^{\mathrm{ab}}/(G^{\mathrm{ab}})^p$ le plus grand quotient abélien de G d'exposant 1 ou p. Ainsi, G/p est un $\mathbf{F}_p$ espace vectoriel; on pose

$$d_p(G) = \dim_{\mathbf{F}_p} G/p = \dim_{\mathbf{F}_p} G^{\mathrm{ab}}/(G^{\mathrm{ab}})^p.$$

Le nombre $d_p(G)$ peut être fini ou infini, c'est le p-rang de G. Si ℓ est un nombre premier, et si G est un pro-ℓ-groupe, alors $d_p(G) = 0$ pour $p \neq \ell$, et on pose $d(G) = d_\ell(G)$ si aucune confusion n'est possible. Dans ce cas, $d(G)$ est le nombre minimum de générateurs de G. Puisque $G/\ell = H^1(G, \mathbf{F}_\ell)$, et puisque $H^1(G, \mathbf{F}_\ell)$ et $H_1(G, \mathbf{F}_\ell)$ ont même $\mathbf{F}_\ell$-rang, on peut écrire

$$d(G) = \dim_{\mathbf{F}_\ell} H^1(G, \mathbf{F}_\ell) = \dim_{\mathbf{F}_\ell} H_1(G, \mathbf{F}_\ell).$$

De même, si G est un pro-ℓ-groupe, le nombre minimum $r(G)$ de relations entre $d(G)$ générateurs de G définissant G comme pro-ℓ-groupe peut être obtenu par la formule

$$r(G) = \dim_{\mathbf{F}_\ell} H^2(G, \mathbf{F}_\ell) = \dim_{\mathbf{F}_\ell} H_2(G, \mathbf{F}_\ell).$$

Dans le cas où G est fini, c'est-à-dire si G est un ℓ-groupe, on dispose de minorations de $r(G)$ en fonction de $d(G)$: Golod et Shafarevich ont montré dans [3] que si G est fini, et si $d(G) \geqslant 1$, alors

$$r(G) > (d(G) - 1)^2/4.$$

Nous utiliserons dans la suite une amélioration de ce résultat, due à Gaschütz et Vinberg, dont on trouvera la preuve dans [1].

PROPOSITION 5. *Si G est un ℓ-groupe fini, et si $d(G) \geqslant 1$, alors $r(G) > d(G)^2/4$.*

Remarque. Pour tout nombre premier ℓ, et pour tout entier $d \geqslant 1$, on sait construire un ℓ-groupe fini ayant d générateurs et $d(d-1)/2$ relations.

b. *Le ℓ-rang d'un sous groupe et d'un quotient*

PROPOSITION 6. *Soit $A \longrightarrow B \xrightarrow{f} C$ une suite exacte de groupes abéliens. L'inégalité*

$$d_\ell(B) \leqslant d_\ell(A) + d_\ell(C)$$

est vraie dans les deux cas suivants:

(1) *f est surjective*;

(2) *C est un groupe abélien de type fini.*

Preuve. Le premier cas est connu: c'est la suite inflation–restriction; le morphisme $B \xrightarrow{f} \operatorname{Im} f$ étant le surjectif, le second cas se ramène au premier puisque $d_\ell(\operatorname{Im} f) \leqslant d_\ell(C)$. Pour voir ce dernier point, soit G un groupe abélien de type fini, et H un sous groupe de G; il s'agit de montrer que $d_\ell(H) \leqslant d_\ell(G)$. Il existe un morphisme surjectif

$$\mathbf{Z}^d \xrightarrow{\phi} G/\ell \longrightarrow 1,$$

avec $d_\ell(G) = d_\ell(G/\ell) = d$. Ainsi, $\phi^{-1}(H/\ell)$ est un sous $\mathbf{Z}$-module de $\mathbf{Z}^d$, qui est donc un $\mathbf{Z}$-module de rang fini $d' \leqslant d$. On déduit alors du morphisme surjectif

$$\phi^{-1}(H/\ell) = \mathbf{Z}^{d'} \xrightarrow{\phi} H/\ell \longrightarrow 1$$

que $d_\ell(H/\ell) \leqslant d_\ell(G/\ell)$. ∎

2. *Le critère de non finitude*

Soit $(k_n, S_n, \mathfrak{m}_n, \ell)$ la ℓ-tour de corps de classes ramifiée construite en I, §3. On note

$$d = d_\ell(G)\ (= d_\ell(G_1) \text{ puisque } G_1 \text{ est l'abélianisé de } G),$$

$$r = r_\ell(G).$$

Conjecture 1. Si $d + \#S \leqslant d^2/4$, alors l'extension k_∞/k est infinie.

Supposons que k_∞/k soit finie. D'après la remarque de I, §3, cela signifie qu'il existe $n \in \mathbf{N}^*$ tel que le groupe $F = (C_n/\mathrm{Im}\ P_n)$ (où C_n est le groupe des classes d'idèles de k_n, et où P_n a été défini en I, §3) soit d'ordre premier à ℓ.

LEMME 1. *Soit n l'entier défini ci-dessus. Pour tout $q \in \mathbf{Z}$, on a des isomorphismes de groupes*

$$\hat{H}^q(G, \mathrm{Im}\ P_n) \approx \hat{H}^{q-2}(G, \mathbf{Z}).$$

Preuve. Puisque G est un ℓ-groupe et F est d'ordre premier à ℓ, les groupes $\hat{H}^q(G, F)$ sont triviaux pour tout q. La suite exacte courte

$$1 \to \mathrm{Im}\ P_n \to C_n \to F \to 1$$

induit donc des isomorphismes $\hat{H}^q(G, \mathrm{Im}\ P_n) \approx \hat{H}^q(G, C_n)$. Mais le cup-produit par un générateur de $\hat{H}^2(G, C_n)$ donne des isomorphismes $\hat{H}^q(G, C_n) \approx \hat{H}^{q-2}(G, \mathbf{Z})$; voir par exemple [1, 6, 8, ou 13]. ∎

Soit $E_n = E_{S_n}(m_n)$ le groupe des S_n unités de k_n congrues à 1 mod* $\mathfrak{m}_n$, c'est-à-dire l'ensemble des éléments $x \in k_n$, tels que $v_\mathfrak{p}(x) = 0$ pour $\mathfrak{p} \notin S_n$, et $v_\mathfrak{p}(x-1) \geqslant m_\mathfrak{p}$ pour $\mathfrak{p} \in R_n$.

LEMME 2. *$\hat{H}^0(G, E_n)$ est un groupe abélien de type fini, et $d_\ell(\hat{H}^0(G, E_n)) \leqslant \#S$.*

Preuve. Par définition, $\hat{H}^0(G, E_n) = (E_n)^G / N_{k_n/k_0}(E_n)$. Il est facile de voir que $(E_n)^G = E_{S_0}(\mathfrak{m}')$, avec $\mathfrak{m}' = \sum_{\mathfrak{p} \in R_0} \lceil m_\mathfrak{p}/[k_n : k_0] \rceil \mathfrak{p}$ ($\lceil x \rceil$ désignant la partie entière par excès du nombre réel x, c'est-à-dire le plus petit entier $n \geqslant x$). Le groupe $(E_n)^G$ est un sous groupe de E_{S_0}, qui est, par le théorème des unités de Dirichlet (cf. [17]), un groupe abélien de type fini de rang inférieur ou égal à $\#S$. Le groupe abélien $(E_n)^G$ est donc de type fini, de ℓ-rang inférieur ou égal à $\#S$ par la Proposition 6. Il en est de même pour $\hat{H}^0(G, E_n)$ en tant que quotient de $(E_n)^G$. ∎

Remarque. La preuve ci-dessus montre en fait que $d_\ell(\hat{H}^0(G, E_n)) \leqslant \#S - \delta$, avec $\delta = 0$ si E_n contient le groupe des racines ℓ-ièmes de l'unité, et $\delta = -1$ sinon (si $\ell = p = \mathrm{char}(k)$, alors $\delta = -1$). Par conséquent, on peut formuler la Conjecture suivante: si $d + \#S - \delta \leqslant d^2/4$, alors l'extension k_∞/k est infinie.

La suite exacte courte

$$1 \longrightarrow E_n \longrightarrow P_n \xrightarrow{\pi} \mathrm{Im}\, P_n \longrightarrow 1$$

induit la suite exacte

$$\hat{H}^{-1}(G, P_n) \xrightarrow{\pi} \hat{H}^{-1}(G, \mathrm{Im}\, P_n) \xrightarrow{\delta} \hat{H}^0(G, E_n),$$

d'où la suite exacte

$$1 \longrightarrow \hat{H}^{-1}(G, P_n)/\mathrm{Ker}\, \pi \xrightarrow{\pi} \hat{H}^{-1}(G, \mathrm{Im}\, P_n) \xrightarrow{\delta} \mathrm{Im}\, \delta \longrightarrow 1.$$

Ainsi, $\mathrm{Im}\, \delta \approx \hat{H}^{-1}(G, \mathrm{Im}\, P_n)/[\hat{H}^{-1}(G, P_n)/\mathrm{Ker}\, \pi]$, d'où la relation

$$d_\ell(\mathrm{Im}\, \delta) \leqslant d_\ell(\hat{H}^{-1}(G, \mathrm{Im}\, P_n)) = d_\ell(\hat{H}^{-3}(G, \mathbf{Z}))$$

d'après le Lemme 1.

Conjecture 1'. Si $k_\infty = k_n$, alors

$$d_\ell(\hat{H}^{-3}(G, \mathbf{Z})) = d_\ell(\mathrm{Im}\, \delta).$$

THÉORÈME 2. (i) *La Conjecture* 1' *implique la Conjecture* 1.

(ii) *Si* R_0 *est vide, alors la Conjecture* 1' *est vraie.*

Preuve. (i) Si $k_\infty = k_n$, et si $d_\ell(\hat{H}^{-3}(G, \mathbf{Z})) = d_\ell(\mathrm{Im}\, \delta)$, alors d'après le Lemme 2 et le fait que $d_\ell(\hat{H}^{-3}(G, \mathbf{Z})) = r - d$ (voir [5]), on a: $r \leqslant d + \#S$, et donc, d'après le Théorème de Gaschütz et Vinberg, $d + \#S \geqslant r \geqslant d^2/4$. Cela prouve la première partie du Théorème 2.

(ii) La suite exacte courte

$$1 \to E_n \to P_n \to \mathrm{Im}\, P_n \to 1$$

induit la suite exacte

$$\hat{H}^{-1}(G, P_n) \longrightarrow \hat{H}^{-1}(G, \mathrm{Im}\, P_n) \xrightarrow{\delta} \hat{H}^0(G, E_n) \longrightarrow \hat{H}^0(G, P_n).$$

D'après le Lemme 1, $\hat{H}^{-1}(G, \mathrm{Im}\, P_n) \approx \hat{H}_2(G, \mathbf{Z})$. Les places $\mathfrak{p} \in S_n$ étant totalement décomposées le G-module $\prod_{\mathfrak{p} \in S_n} k_{n,\mathfrak{p}}^*$ est induit, donc cohomologiquement trivial. De même, les places $\mathfrak{p} \notin S_n \cup R_n$ étant non ramifiées (cf. [1] ou [13]), $\prod_{\mathfrak{p} \notin S_n \cup R_n} U_{n,\mathfrak{p}}$ est cohomologiquement trivial.

Ainsi, $\hat{H}^q(G, P_n) \approx \hat{H}^q(G, \prod_{\mathfrak{p} \in R_n} U_{n,\mathfrak{p}}^{m_\mathfrak{p}}) = 1$ si R est vide. Dans ce cas, la suite exacte ci-dessus montre que $\hat{H}_2(G, \mathbf{Z}) \approx \hat{H}^0(G, E_n)$, d'où la seconde partie du Théorème 2. ∎

III. Minoration de $A(q)$ sous la Conjecture 1

1. *Extensions d'Artin–Schreier de* $\mathbf{F}_q(T)$

Pour un exposé complet de ce qui suit, voir [7]. Soient q une puissance d'un nombre premier p, k_0 une extension finie de $\mathbf{F}_q(T)$ et f un élément de k_0, tel que $f \neq h^p - h$ pour tout $h \in k_0$. On considère l'équation d'Artin–Schreier

$$Y^p - Y = f(T),$$

qui définit une extension $k = k_0(y)$ de k_0, cyclique, de degré p.

Si u est une place de k_0, et si O_u est l'anneau des fonctions régulières en u, on définit

$$v_u(f) = 0 \qquad \text{si} \quad f \in \mathsf{O}_u,$$
$$v_u(f) = \text{ordre du pôle de } f \text{ en } u \qquad \text{si} \quad f \notin \mathsf{O}_u,$$

et

$$v_u^*(f) = \operatorname{Min}\{v_u(f - g^p + g),\ g \in k_0\}.$$

Le nombre $v_u^*(f)$ est l'ordre réduit de f en u, et peut être calculé par l'algorithme d'Artin. Nous allons énoncer les résultats sur ces extensions dont nous aurons besoin. On note $U^*(f)$ l'ensemble des places u de k_0, pour lesquelles $v_u^*(f) > 0$. Si u est une place de k, et si $f = h + g^p - g$ avec $h \in \mathsf{O}_u$, on note $\operatorname{Tr}_u^*(f) = \operatorname{Tr}_{k_0(u)/\mathbf{F}_p}(h(u))$.

Proposition 7. *Avec les notations précédentes, l'extension k/k_0 est cyclique de degré p. Les places de k_0 ramifiées dans k sont celles de $U^*(f)$; en chacune de ces places, la ramification est totale et sauvage. Soit $u \notin U^*(f)$. Si $\operatorname{Tr}_u^*(f) \neq 0$, la place u a un degré résiduel égal à p. Si $\operatorname{Tr}_u^*(f) = 0$, la place u se décompose totalement dans k; c'est le cas en particulier si u est un zéro de f. Si g_0 est le genre de k_0, le genre g de k est donné par la formule*

$$2g - 2 = p(2g_0 - 2) + (p-1) \sum_{u \in U^*(f)} (v_u^*(f) + 1) \deg u.$$

2. *Construction d'un triplet* $(K, S, \mathfrak{m})$.

Soient A, B deux parties disjointes de $\mathbf{F}_q$, $\#A = a \geqslant 2$, $\#B = b \geqslant p$; on suppose que b est une puissance de p. On pose $k_0 = \mathbf{F}_q(T)$, et on considère les extensions $K = k_0(y)$, où

$$y^p - y = \prod_{\beta \in B} (T-b)\left(\sum_{\alpha \in A} \frac{1}{(T-\alpha)^b}\right),$$

et $K_\alpha = K(y_\alpha)$ pour $\alpha \in A$, où

$$y_\alpha^p - y_\alpha = \prod_{\beta \in B} (T-\beta)\left(\frac{1}{(T-\alpha)^b} + \sum_{\alpha' \neq \alpha} \frac{1}{(T-\alpha')^{b/p}}\right).$$

On pose

$$S_0 = S = \{\text{places de } K \text{ au-dessus de } (T-\beta),\ \beta \in B\},$$

$$R_0 = R = \left\{\text{la place de } K \text{ au-dessus de } \frac{1}{T}\right\} = \{\mathfrak{p}_\infty\},$$

$$\mathfrak{m}_0 = \mathfrak{m} = 2\mathfrak{p}_\infty,$$

de sorte que $\#S = p\,\#B = pb$ et $\#R = 1$ (la place à l'infini $1/T$ de k_0 se ramifiant dans K, elle se remonte en une unique place $\mathfrak{p}_\infty$ de K, de degré 1), et on considère la p-tour de corps $(K_n, S_n, \mathfrak{m}_{n,p})$ au-dessus de $(K, S, \mathfrak{m})$.

Énonçons tout d'abord un lemme.

LEMME 3. *Soit K/k une extension abélienne; supposons qu'il existe n extensions intermédiaires $k_1, \ldots, k_n$ cycliques de degré p, aucune n'étant contenue dans le compositum des $n-1$ autres; alors $d_p(\mathrm{Gal}(K/k)) \geqslant n$.*

Preuve. Puisque les extensions $k_1, \ldots, k_n$ sont telles qu'aucune n'est dans le compositum des $n-1$ autres, le p-groupe abélien $\mathrm{Gal}(K/k)$ contient au moins n sous groupes isomorphes à $\mathbf{Z}/p\mathbf{Z}$; il a donc au moins n facteurs cycliques distincts, et s'écrit donc sous la forme

$$\mathrm{Gal}(K/k) = W \times \mathbf{Z}/p^{c_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{c_n}\mathbf{Z},$$

où W est un p-groupe, et $d_p(\mathrm{Gal}(K/k)) = n + d_p(W) \geqslant n$. ∎

PROPOSITION 8. $d_p(\mathrm{Gal}(K_1/K)) \geqslant a - 1$.

Preuve. En vertu du lemme 3, il suffit de prouver que les K_α, lorsque α décrit A sauf un élément, sont des extensions cycliques de degré p, où les

places au-dessus de $(T-\beta)$, $\beta \in B$, se décomposent totalement, de conducteur divisant $\mathfrak{m}$, et que K_α n'est pas contenue dans le compositum $\prod_{\alpha' \in A, \alpha' \neq \alpha} K_{\alpha'}$. Seules les deux dernières assertions ne sont pas triviales.

On peut écrire $K_\alpha = K(z_\alpha)$, avec $z_\alpha = y - y_\alpha$, satisfaisant

$$z_\alpha^p - z_\alpha = \prod_{\beta \in B} (T-\beta)\left(\sum_{\alpha' \neq \alpha} \frac{1}{(T-\alpha')^b} - \frac{1}{(T-\alpha')^{b/p}}\right) = f_\alpha(T).$$

Posons

$$\phi_\alpha = \sum_{\alpha' \neq \alpha} \frac{1}{(T-\alpha')^{b/p}} \quad \text{et} \quad h = \prod_{\beta \in B} (T-\beta).$$

Le membre de droite de l'équation précédente s'écrit

$$f_\alpha = h(\phi_\alpha^p - \phi_\alpha).$$

Le polynôme h n'ayant pas de pôle aux places distinctes de l'infini, la relation ci-dessus montre que l'ordre réduit de f en les places de K divisant $(T-\alpha')$ est nul; ces places ne se ramifient donc pas dans K_α; il n'y a donc ramification qu'en la place à l'infini $\mathfrak{p}_\infty$ de K. De plus, le conducteur des extensions K_α/K est $\mathfrak{f}(K_\alpha/K) = v_\infty^*(f_\alpha) + 1 = 2$ (voir [7]), ce qui prouve la première assertion à démontrer.

La dernière assertion découle du fait que les places de K au-dessus de $(T-\alpha)$ se décomposent totalement dans K_α par la Proposition 7 puisque $\mathrm{Tr}^*_{(T-\alpha)}(f_\alpha) = 0$, et sont inertes dans $K_{\alpha'}$ si $\alpha' \neq \alpha$ puisque $\mathrm{Tr}^*_{(T-\alpha)}(f_{\alpha'}) \neq 0$. ∎

Il nous reste à calculer le genre de K.

PROPOSITION 9. *Soit g_0 le genre de K. Si b est de la forme $b = p^n$, $n \geqslant 1$, alors*

$$g_0 - 1 = a(p-1) - p.$$

Preuve. Appliquons la proposition 7 avec $k_0 = \mathbf{F}_q(T)$ et $k = K$. Les seules places de k_0, ramifiées dans K, sont les places $u_\alpha = (T-\alpha)$, $\alpha \in A$. Puisque b est une puissance de p, on a, par l'algorithme d'Artin [7],

$$v_{u_\alpha}^*\left(\frac{1}{(T-\alpha)^b}\right) = v_{u_\alpha}\left(\frac{1}{(T-\alpha)}\right) = 1.$$

La proposition 9 découle alors de la proposition 7. ∎

3. *Minorations de $A(q)$*

a. *Première minoration*

THÉORÈME 3. *Sous la Conjecture* 1, *si* $q=p^n$, p *premier*, $n\geqslant 2$, *et* q *distinct de* 4, 8, 9, *et* 16, *alors*

$$A(q)>\frac{\sqrt{q+1}-2}{2(p-1)}.$$

Preuve. Soit $B\subset \mathbf{F}_q$, avec $\#B=b=p^{n-1}=q/p$. La plus petite valeur de a telle que

$$(a-1)+pb\leqslant (a-1)^2/4$$

est $a_0=3+\lceil 2\sqrt{q+1}\,\rceil$. Cette inégalité, d'après la Conjecture 1 et la proposition 8, assure la non finitude de la p-tour de corps au-dessus de $(K, S, \mathfrak{m})$ construite en I, §3 dès que $a-1\geqslant 2$. Si

$$3+\lceil 2\sqrt{q+1}\,\rceil+q/p\leqslant q,$$

c'est-à-dire sous les hypothèses du théorème, on peut choisir un ensemble A dans $\mathbf{F}_q$, disjoint de B, tel que $\#A=a_0$. Dans ce cas, le genre g_n de K_n est donné par la formule de Hurwitz (cf. [17])

$$2g_n-2=[K_n: K_0](2g_0-1)+\deg(\mathfrak{d}(K_n/K_0)).$$

D'après le Théorème 1 et la Proposition 4, $\deg(\mathfrak{d}(K_n/K_0))\leqslant([K_n/K_0]-1)\deg \mathfrak{m}$, d'où

$$g_n\leqslant [K_n/K_0](g_0-1)+([K_n: K_0]-1)+1=[K_n/K_0]\,g_0.$$

Ainsi,

$$\begin{aligned}A(q)&\geqslant \lim_{n\to\infty}\frac{\{\text{nombre de places de degré 1 de } K_n\}}{g_n}\geqslant \lim_{n\to\infty}\frac{\#S_n}{g_n}\\&\geqslant \lim_{n\to\infty}\frac{[K_n: K_0]\,\#S_0}{[K_n: K_0]\,g_0}=\frac{\#S_0}{g_0}\\&=\frac{pb}{a(p-1)-p}=\frac{q}{(3+\lceil 2\sqrt{q+1}\,\rceil)(p-1)-p}\\&>\frac{\sqrt{q+1}-2}{2(p-1)}.\end{aligned}$$

Cela démontre le théorème 3. ∎

Remarque. $q/((3+\lceil 2\sqrt{q+1}\,\rceil)(p-1)-p)-(\sqrt{q+1}-2)/2(p-1)$ est petit, de l'ordre de quelques unités.

b. *Seconde minoration*

THÉORÈME 4. *Sous la Conjecture* 1, *si* $q=p^n$, p *impair*, $n\geqslant 2$ *et* q *distinct de* 9, 25, 27, 49, 81, 121, *et de* 169, *alors*

$$A(q)>\frac{\sqrt{pq+1}-2}{4(p-1)}.$$

Preuve. Choisissons un ensemble $A'\subset \mathbf{F}_q$, tel que pour tout $\alpha\in A'$, $T^2-\alpha$ soit irréductible sur $\mathbf{F}_q[T]$. Cela est possible si p est impair, et si $\#A'=a\leqslant (q-1)/2$. On construit alors $K=k_0(y)$, où

$$y^p-y=\prod_{\beta\in B'}(T-\beta)^2\left(\sum_{\alpha\in A'}\frac{1}{(T^2-\alpha)^b}\right)$$

avec $B'=\mathbf{F}_q$, et $K_\alpha=K(y_\alpha)$ pour $\alpha\in A'$, où

$$y_\alpha^p-y_\alpha=\prod_{\beta\in B'}(T-\beta)^2\left(\frac{1}{(T^2-\alpha)^b}+\sum_{\alpha'\neq\alpha}\frac{1}{(T^2-\alpha')^{b/p}}\right).$$

On construit la p-tour de corps au-dessus de $(K, S, \mathfrak{m})$, où S est l'ensemble des places de K au-dessus de toutes les places $(T-\beta)$, $\beta\in B'$, et $\mathfrak{m}=2\mathfrak{p}_\infty$. Ainsi, $\#S=pq$. Le même raisonnement que précédemment permet de montrer que le genre g_0 de K est donné par

$$g_0-1=2a(p-1)-p,$$

et que l'on a

$$d_p(\mathrm{Gal}(K_1/K))\geqslant a-1.$$

La plus petite valeur de a telle que

$$a-1+pq\leqslant (a-1)^2/4$$

est $a=3+\lceil 2\sqrt{pq+1}\,\rceil$; les hypothèses du théorème impliquent que cette valeur est inférieure à $(q-1)/2$. On minore alors $A(q)$ de la même façon. ∎

Remarques. (1) La minoration du Théorème 4 est meilleure que celle du Théorème 3 pour toutes les valeurs de p distinctes de 2 et 3.

(2) On pourait donner une autre minoration de $A(q)$ pour $p=2$ en considérant des places irréductibles de la forme $(T^2-T-\alpha)$.

COROLLAIRE 1. *Sous la Conjecture* 1, *pour tout nombre premier* p, *il existe une constante* $c(p)$ *telle que, pour toute puissance* q *de* p, *on ait (sauf pour* $q=4, 8, 9, 16, 25, 27, 49, 81, 121,$ *et* 169),

$$A(q) \geqslant c(p)(\sqrt{q}-1).$$

On peut prendre $c(p)=1/4(p-1)$ *si* p *est impair, et* $c(2)=1/3$.

Preuve. Le Théorème 4 prouve le Corollaire pour p impair, et le Théorème 3 pour $p=2$. ∎

Remarque. Puisque $A(q)>c \log q>0$ pour tout q (Serre, non publié), le Corollaire 1 implique

COROLLAIRE 2. *Sous la Conjecture* 1, *il existe pour tout* p *une constante* $c'(p)$ *telle que pour tout* q *puissance de* p, *on ait*

$$A(q) \geqslant c'(p)(\sqrt{q}-1).$$

Rappelons la conjecture usuelle:

Conjecture 2. Pour tout q, $A(q)=\sqrt{q}-1$.

IV. MINORATIONS DE $A(q)$ NON CONDITIONNELLES

1. *La ℓ-tour de corps de classes de Hilbert*

Le résultat de cette partie a été annoncé dans [9]. On pose $k_0=\mathbf{F}_q(T)$, et on suppose que $q\equiv 1 \pmod{\ell}$. Soient A et B deux parties non vides et disjointes de $\mathbf{F}_q$. On considère le corps $K_0=k_0(U)$, où

$$U'=\prod_{\alpha\in A}(T-\alpha),$$

ainsi que le corps $K_\alpha=k_0(U_\alpha)$, où

$$U_\alpha'=T-\alpha, \qquad \text{pour} \quad \alpha\in A.$$

On pose

$$\mathbf{F}_q^{*\ell}=\{x^\ell\,;\,x\in\mathbf{F}_q^*\}.$$

On suppose que pour tout $\alpha\in A$ et tout $\beta\in B$, $\beta-\alpha$ est une puissance ℓ-ième dans $\mathbf{F}_q$, ce que l'on note

$$B-A\subset\mathbf{F}_q^{*\ell}.$$

On note enfin S_0 l'ensemble des places de K_0 au-dessus des places $(T-\beta)$ de k_0, pour tout $\beta \in B$; on a $|S_0| = \ell\,|B|$; toute place de S_0 est de degré 1.

PROPOSITION 10. *Supposons* $q \equiv 1 \pmod{\ell}$ *et* $(|A|, \ell) = 1$. *Les corps* K_α, *où* α *parcourt tous les éléments de* A *sauf un, sont des extensions cycliques de degré* ℓ *de* K_0, *indépendantes et non ramifiées, où les éléments de* S_0 *se décomposent totalement. De plus*

$$d_\ell(G) = d_\ell(G_1) \geqslant |A| - 1.$$

Preuve. Le principe est le même que pour la Proposition 8. ∎

2. *Minorations de* $A(q)$

PROPOSITION 11. *Soit* ℓ *un nombre premier tel que* $q \equiv 1 \pmod{\ell}$. *Si on peut trouver deux parties disjointes* A *et* B *de* $\mathbf{F}_q$, *telles que* $|A| = a \geqslant 2$, $|B| = b \geqslant 1$, *et*

(a) $B - A \subset \mathbf{F}_q^{*\ell}$,

(b) $a + \ell b \leqslant (a-1)^2/4$,

(c) $(a, \ell) = 1$.

Alors

$$A(q) \geqslant \frac{2b\ell}{(a-1)(\ell-1)}.$$

Preuve. On construit le couple (K_0, S_0) à partir des ensembles A et B. La condition (b) de l'énoncé permet d'affirmer, via la Proposition 10 et le Théorème 2, que la ℓ-tour de corps de classes de Hilbert au-dessus de (K_0, S_0) est infinie. Ainsi,

$$A(q) \geqslant \lim_{\pm n \to \infty} \{\text{nombre de places de degré 1 de } K_n\}/g_n \geqslant \lim_{n \to \infty} \frac{|S_n|}{g_n}.$$

Or, l'extension K_n/K_0 est non ramifiée, donc $2g_n - 2 = [K_n : K_0](2g_0 - 2)$. Par suite,

$$A(q) \geqslant \lim_{n \to \infty} \frac{[K_n : K_0]\,|S_0|}{[K_n : K_0](g_0 - 1) + 1}$$

$$= \frac{|S_0|}{g_0 - 1} = \frac{\ell b}{g_0 - 1},$$

puisque $\lim_{n\to\infty}[K_n:K_0]=+\infty$. La formule de Hurwitz appliquée à K_0/k_0 où $k_0=\mathbf{F}_q(T)$, montre que

$$g_0-1=\frac{(a+1)(\ell-1)}{2}-\ell<\frac{(a-1)(\ell-1)}{2}.$$

Cela résulte de ce que l'indice de ramification e_α d'une place $(T-\alpha)$, où $\alpha\in A$, divise $[K_0:k_0]=\ell$; ces places sont donc totalement ramifiées. De même, l'hypothèse $(a,\ell)=1$ implique que l'indice de ramification e_∞ de la place à l'infini est égal à ℓ; les ramifications sont modérées car l'hypothèse $q\equiv 1 \pmod{\ell}$ implique $(\ell,q)=1$; cela montre la Proposition 10. ▮

En particulier:

COROLLAIRE. *Si Q est une puissance de q, si $Q\equiv 1 \pmod{\ell}$, et si $\mathbf{F}_q\subset\mathbf{F}_Q^\ell$, alors*

$$A(Q)\geqslant\frac{\sqrt{\ell(q-1)}-2\ell}{\ell-1},$$

pour peu que $q>4\ell+1$.

Preuve. On applique la Proposition 11 pour un couple A et B formant une partition de $\mathbf{F}_q$. On calcule alors la plus petite valeur de a (resp. la plus grande valeur de b) vérifiant la condition b) de la Proposition 11, ainsi que la relation $a+b=q$. Il faut s'assurer que $(a,\ell)=1$, ce qui n'est pas toujours vrai pour cette valeur de a, c'est pourquoi on augmente a (resp. diminue b) d'une unité. La Proposition 11 donne alors une minoration compliquée de $A(q)$, elle-même minorée par celle du corollaire. La condition $q>4\ell+1$ implique les conditions $a\geqslant 2$ et $b\geqslant 1$. ▮

THÉORÈME 5. *Supposons que $q>4\ell+1$. Soit k un entier non nul et supposons que q soit une racine primitive k-ième de l'unité dans $\mathbf{F}_\ell$. Si $k=1$ (i.e., si $q\equiv 1 \pmod{\ell}$), alors*

$$A(q^\ell)\geqslant\frac{\sqrt{\ell(q-1)}-2\ell}{\ell-1};$$

si $k\geqslant 2$, alors

$$A(q^k)\geqslant\frac{\sqrt{\ell(q-1)}-2\ell}{\ell-1}.$$

EXEMPLES. (1) Si q est impair, $q>9$, le Théorème 5 donne $A(q^2)\geqslant\sqrt{2}\sqrt{q-1}-4$, ce qui est moins bon que la borne $A(q^2)=q-1$ de Tsfasman, Vladut, et Zink citée dans [15].

(2) Si $q \equiv 1 \pmod 3$ (resp. si $q \equiv 2$ ou $4 \pmod 7$), alors

$$A(q^3) \geqslant \frac{\sqrt{3}}{2}\sqrt{q-1} - 3 \qquad \text{pour} \quad q > 13$$

(resp.

$$A(q^3) \geqslant \frac{\sqrt{7}}{6}\sqrt{q-1} - \frac{7}{3} \qquad \text{pour} \quad q > 29).$$

Signalons que Zink a montré le résultat meilleur $A(q^3) \geqslant 2(q^2-1)/(q+2)$.

(3) De même, si $q \equiv 1 \pmod 5$ (resp. $q \equiv 4$, 5, 8, ou 9 $\pmod{11}$), alors

$$A(q^5) \geqslant (\sqrt{5}/4)\sqrt{q-1} - (5/2) \qquad \text{pour} \quad q > 21$$

(resp.

$$A(q^5) \geqslant (\sqrt{11}/10)\sqrt{q-1} - (11/5) \qquad \text{pour} \quad q > 45).$$

Preuve. Le théorème 5 découle du corollaire de la Proposition 11 et des deux remarques suivantes:

(1) si $q \equiv 1 \pmod \ell$, tous les éléments de $\mathbf{F}_q$ sont des puissances ℓ-ièmes dans $\mathbf{F}_{q^\ell}$.

(2) si $(\ell, q-1) = 1$, tous les éléments de $\mathbf{F}_q$ sont des puissances ℓ-ièmes dans $\mathbf{F}_q$, donc aussi dans $\mathbf{F}_{q^k}$.

L'hypothèse q racine primitive k-ième de l'unité dans $\mathbf{F}_\ell$ signifie que $Q = q^k \equiv 1 \pmod \ell$, ce qui est une hypothèse primordiale du corollaire 1. ∎

Remarque. Le théorème 5 donne des résultats meilleurs que celui de Serre ($A(q) > c \log q$) lorsque l'on se restreint à des familles de q vérifiant certaines relations de congruences. Malheureusement, il y a des valeurs de q pour lesquelles le Théorème 5 ne donne aucun renseignements, par exemple si q est premier; on ne peut donc déduire du Théorème 5 une minoration de $A(q)$ valable pour tout q, meilleure que celle de Serre.

V. Applications

1. *Codes correcteurs d'erreurs*

Pour des justifications de ce qui suit, voir [10] ou [14]. Les Théorèmes 3 et 4 permettent d'affirmer que sous la Conjecture 1, si $q = p^n$, $n \geqslant 1$, q distinct de certaines valeurs, et si

$$\frac{2(p-1)}{\sqrt{q+1}-2} < \log_q \frac{2q-1}{q},$$

ou bien si $p \neq 2$, q distinct de certaines valeurs, et si

$$\frac{4(p-1)}{\sqrt{pq+1}-2} < \log_q \frac{2q-1}{q},$$

alors il existe une famille de codes sur $\mathbf{F}_q$ ayant un point d'accumulation au-dessus de la borne de Varshamov–Gilbert.

THÉORÈME 6. *Sous la Conjecture* 1, *si p est premier, et si* $q = p^n$, *il existe une famille de codes sur* $\mathbf{F}_q$ *ayant un point d'accumulation au-dessus de la borne de Varshamov–Gilbert dans chacun des cas suivants*:

(1) $n \geqslant 2$ *et* $p \geqslant 11683$

(2) $n \geqslant 3$ *et* $p \geqslant 79$

(3) $n \geqslant 4$ *et* $p \geqslant 17$

(4) $n \geqslant 5$ *et* $p \geqslant 7$

(5) $n \geqslant 6$ *et* $p \geqslant 5$

(6) $n \geqslant 8$ *et p quelconque.*

Remarque. Compte tenu du fait que la conclusion du Théorème 6 est vraie si q est un carré supérieur à 49 (cf. [15]), on en déduit

COROLLAIRE. *Sous la Conjecture* 1, *si p est premier, et si* $q = p^n$, *il existe une famille de codes sur* $\mathbf{F}_q$ *ayant un point d'accumulation au-dessus de la borne de Varshamov–Gilbert dans chacun des cas suivants*:

(1) $n \geqslant 2$ *et* $p \geqslant 79$

(2) $n \geqslant 4$ *et* $p \geqslant 7$

(3) $n \geqslant 6$ *et* $p \geqslant 5$

(4) $n \geqslant 8$ *et p quelconque.*

De même, le Théorème 5 montre le Théorème suivant, annoncé dans [9] et explicité dans [10].

THÉORÈME 7. *Sous les hypothèses et notations du théorème* 5, *si*

$$\frac{\ell-1}{\sqrt{\ell(q-1)}-2\ell} < \log_{q^\ell} \frac{2q^\ell-1}{q^\ell},$$

(*resp., si*

$$\frac{\ell-1}{\sqrt{\ell(q-1)}-2\ell} < \log_{q^k} \frac{2q^k-1}{q^k}),$$

alors il existe une famille de codes sur $\mathbf{F}_{q^\ell}$ (*resp.* $\mathbf{F}_{q^k}$), *dépassant la borne de Varshamov–Gilbert.*

Par exemple, si q est impair, cela montre l'existence de familles de codes sur $\mathbf{F}_{q^2}$ dépassant la borne de Varshamov–Gilbert pour $q \geqslant 191$, ce qui est moins bon que le résultat annoncé dans [15]. De même, si $q \geqslant 1657$, et si $q \equiv 1 \pmod 3$, cela donne de telles familles sur $\mathbf{F}_{q^3}$; si $q \geqslant 16{,}981$ et si $q \equiv 1 \pmod 5$, on a la même conclusion sur $\mathbf{F}_{q^5}$.

2. *Réseaux*

Nous suivons ici Rosenbloom et Tsfasman [11, 14]. Si L est un réseau de $\mathbf{R}^N$, on définit sa densité

$$\Delta = \Delta(L) = \limsup_{c \to \infty} \frac{\text{volume } (S \cap B_c)}{\text{volume } B_c},$$

où B_c est la boule centrée à l'origine, de rayon c, et

$$S = \{x \in \mathbf{R}^N ; d(x, L) \leqslant d/2\},$$

avec

$$d = \text{Min}\{|u - v| ; u, v \in L, u \neq v\}.$$

L'exposant de densité $\lambda(L)$ de L est défini par

$$\lambda(L) = -\frac{1}{N} \log \Delta(L).$$

Si $\{L_n\}$ est une famille de réseaux de $\mathbf{R}^N$, on pose

$$\lambda(\{Ln\}) = \limsup_{n \to \infty} \lambda(L_n).$$

Rosenbloom et Tsfasman ont montré (cf. [11, 14]) que si A est une minoration de $A(q)$, alors il existe une famille de courbes sur $\mathbf{F}_q$ donnant naissance à une famille $\{L_n\}$ de réseaux de $\mathbf{R}^N$, avec

$$\lambda(\{L_n\}) \leqslant -\log \sqrt{\pi e} + \log \sqrt{q+1} + \frac{2}{A} \log(1 + \sqrt{q}),$$

d'où les Théorèmes:

THÉORÈME 8. *Sous la Conjecture* 1, *pour tout q pour lequel le Théorème* 3 (*resp. le Théorème* 4) *est valable, il existe une famille de courbes sur* $\mathbf{F}_q$ *donnant naissance à une famille* $\{L_n\}$ *de réseaux de* $\mathbf{R}^N$, *avec*

$$\lambda(\{L_n\}) \leqslant -\log \sqrt{\pi e} + \log \sqrt{q+1} + \frac{4(p-1)}{\sqrt{q+1} - 2} \log(1 + \sqrt{q}),$$

(*respectivement, avec*

$$\lambda(\{L_n\}) \leqslant -\log\sqrt{\pi e} + \log\sqrt{q+1} + \frac{8(p-1)}{\sqrt{pq+1}-2}\log(1+\sqrt{q}).$$

De même, les minorations non conditionnelles montrent:

THÉORÈME 9. *Pour tout q tel que le Théorème 5 soit valable, il existe une famille de courbes sur* $\mathbf{F}_{q^\ell}$ *(resp. sur* $\mathbf{F}_{q^k}$*), donnant naissance à une famille* $\{L_n\}$ *de réseaux de* $\mathbf{R}^N$*, avec*

$$\lambda(\{L_n\}) \leqslant -\log\sqrt{\pi e} + \log\sqrt{q+1} + \frac{2(\ell-1)}{\sqrt{\ell(q-1)}-2\ell}\log(1+\sqrt{q}).$$

BIBLIOGRAPHIE

1. J. W. S. CASSELS ET A. FRÖHLICH, "Algebraic Number Theory," Academic Press, New York, 1967.
2. V. G. DRINFEL'D ET S. G. VLADUT, Number of points of an algebraic curve, *Funktsional. Anal. i Prilozhen.* **17** (1983), 68–69; *Funct. Anal.* **17** (1983), 53–54.
3. E. S. GOLOD ET I. R. SHAFAREVICH, On class fields towers, *Izv. Akad. SSSR* **28** (1964), 261–272 [en Russe]; traduction anglaise *Amer. Math. Soc. Transl. (2)* **48**, 91–102.
4. Y. IHARA, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo Sec. 1A* **28** (1982), 721–724.
5. K. IWASAWA, A note on the group of units of an algebraic number field, *J. Math. Pures Appl.* **35** (1956), 189–192.
6. S. IYANAGA, "The Theory of Numbers," North-Holland, Amsterdam, 1975.
7. G. LACHAUD, Artin–Schreier curves, exponential sums and the Carlitz–Uchiyama bound for geometric codes, *J. Number Theory*, à paraître.
8. G. NEUKIRCH, "Class Field Theory," Springer-Verlag, Berlin/New York, 1986.
9. M. PERRET, Sur le nombre de points d'une courbe sur un corps fini: Application aux codes correcteurs d'erreurs, *C. R. Acad. Sci. Paris Sér. I* **309** (1989), 177–182.
10. M. PERRET, Families of codes exceeding the Varshamov–Gilbert bound, *in* "Actes du colloque '3 journées sur le codage,'" Lecture Notes on Computer Sciences, Vol. 388, Springer-Verlag, Berlin/New York, 1989.
11. M. ROSENBLUM ET M. TSFASMAN, Multiplicative lattices in global fields, *Invent. Math.*, à paraître.
12. J. P. SERRE, "Cohomologie Galoisienne," Lecture Notes in Mathematics, Vol. 5, Springer-Verlag, Berlin, 1965.
13. J. P. SERRE, "Corps locaux," Hermann, Paris, 1968.
14. M. A. TSFASMAN, Global fields, codes and sphere packings, à paraître.
15. M. A. TSFASMAN, S. G. VLADUT, ET T. ZINK, Modular curves, Shimura curves, and Goppa codes, better than the Varshamov–Gilbert bound, *Math. Nachr.* **109** (1982), 21–28.
16. A. WEIL, "Variétés Abéliennes et Courbes Algébriques," Hermann, Paris, 1948.
17. A. WEIL, "Basic Number Theory," Springer-Verlag, New York, 1967.