ACTA ARITHMETICA
XCVI.3 (2001)

Racines d'unités cyclotomiques et divisibilité du nombre de classes d'un corps abélien réel

par

Cornelius Greither (München), Saïd Hachami (Rabat)
et Radan Kučera (Brno)

Introduction. Le nombre de classes h_K d'un corps abélien réel a la réputation d'être difficile à calculer, et pour cause. Si K est de conducteur premier, h_K a la tendance d'être petit. Par contre, si le conducteur de K est divisible par de nombreux premiers $q_1, \dots, q_l$, tous congrus à 1 modulo un premier p fixé auparavant, alors h_K a tendance d'être divisible par une puissance élevée de p, même si K est son propre corps des genres. Il existe au moins trois approches pour démontrer des résultats de ce type : d'une part, on peut exhiber directement des p-extensions non ramifiées de K et faire appel au corps de classes ; c'est ce qu'a fait Cornell dans [Co]. D'autre part, Cornell et Rosen [CR] ont employé une démarche sophistiquée faisant intervenir le corps central de classes et la cohomologie H^{-3}. Finalement, on peut travailler avec l'indice $[E : C]$, où $E = E_K$ désigne le groupe des unités de K, et C dénote les unités cyclotomiques. Ici on termine en appliquant la formule analytique pour le nombre de classes. Ce programme a été réalisé par le troisième auteur [Ku] pour $p = 2$ et K un composé de corps quadratiques.

Dans ce travail, nous nous proposons de transférer la démarche de Kučera au cas où p est un premier impair quelconque et K est un corps des genres de type $(p, \dots, p)$ (l fois p) quelconque. Dans certains cas, les résultats que nous obtenons ici reproduisent ou même améliorent ceux de Cornell et de Cornell et Rosen. Dans d'autres cas, plus nombreux, ces derniers résultats demeurent supérieurs numériquement, mais en tout cas nous offrons une approche nouvelle qui permet de trouver des unités non cyclotomiques de façon presque explicite, le seul ingrédient non complètement constructif étant une application du théorème 90 de Hilbert. Notre résultat principal affirme que h_K est divisible par $p^{2^l - l^2 + l - 2}$. En particulier, p^2 divise h_K si $l \geq 4$. (Ceci a été déjà démontré dans [CR].) Nous retrouvons par notre démarche (qui

2000 *Mathematics Subject Classification*: 11R20, 11R29, 11R34.

est complètement différente) quelques résultats de [CR] pour $l = 3$. Ici, la p-divisibilité de h_K dépend de certains coefficients a_{ij} (où $1 \le i \ne j \le 3$), et la comparaison entre les deux méthodes se révèle assez intéressante.

Cet article est basé sur la deuxième partie de la thèse de doctorat [Ha] de Saïd Hachami, écrite à l'Université Laval sous la direction de C. Greither ; il incorpore plusieurs améliorations dues à R. Kučera. Le premier auteur a été subventionné par CRSNG (OGP0183650). Nour tenons à remercier CICMA pour le soutien fourni au deuxième auteur. Le troisième auteur a été subventionné par le Ministère d'Education de la République Tchèque sous le projet MSM 143100009.

1. Une classe de corps et leurs unités cyclotomiques. Nous fixons un entier $l \ge 1$, et un nombre premier p impair. Soient $q_1, \dots, q_l$ des premiers distincts, tous congrus à 1 modulo p ; soit K_i le corps abélien de degré p et conducteur q_i sur $\mathbb{Q}$ ($i = 1, \dots, l$). Soit finalement $K = K_1 \dots K_l$ le composé. C'est une extension abélienne réelle de $\mathbb{Q}$. Le groupe G de Galois de K sur $\mathbb{Q}$ est facile à décrire : il est p-élémentaire de rang l, engendré par $\sigma_1, \dots, \sigma_l$, où tout σ_i fixe les corps K_j avec $j \ne i$, et la restriction induit un isomorphisme $\langle \sigma_i \rangle \to G(K_i/\mathbb{Q})$.

Nous aurons constamment besoin des nombres et unités cyclotomiques de K dans le sens de Sinnott [Si]. Pour ceci, encore un peu de notation : K_i est un sous-corps de $\mathbb{Q}(\zeta_{q_i})$. Pour tout sous-ensemble $I \subset \{1, \dots, l\}$ non vide, posons : $n_I = \prod_{i \in I} q_i$; $\zeta_I = e^{2\pi i/n_I}$; et puis K_I le composé des K_i, i parcourant I. Finalement on définit le "nombre cyclotomique" $x_I = N_{\mathbb{Q}(\zeta_I)/K_I}(1-\zeta_I)$. Il est bien connu que x_I est une unité si et seulement si $|I| > 1$.

Le *groupe des nombres cyclotomiques* est alors

$$D = \langle \{-1\} \cup \{x_I^\sigma \mid \sigma \in G,\ \emptyset \ne I \subset \{1, \dots, l\}\} \rangle.$$

C'est donc le $\mathbb{Z}G$-module engendré par l'ensemble $\{-1\} \cup \{x_I \mid \emptyset \ne I \subset \{1, \dots, l\}\}$, et c'est un sous-groupe de K^*. Retenons que $K = K_{\{1,\dots,l\}}$. Il est connu (voir [Si]) que le $\mathbb{Z}$-rang de D vaut $[K : \mathbb{Q}]+l-1 = p^l+l-1$. Le groupe C des *unités* cyclotomiques est défini comme $C = D \cap E$ (où $E = E_K$) ; son rang est $[K : \mathbb{Q}] - 1 = p^l - 1$, le même que le rang de E. En fait on a :

PROPOSITION 1.1 (Sinnott). $[E : C] = h_K \cdot 2^{p^l-1}$.

(C'est le Théorème 4.1 de [Si] ; le "facteur genre" représenté par la fraction dans cette formule vaut 1, et le terme $(R : U)$ vaut également 1, d'après le Théorème 5.4 de loc.cit.)

Puisque nous ne nous intéressons qu'à la divisibilité de h_K par une puissance de p, nous pouvons remplacer h_K par l'indice $[E : C]$ dans tous les calculs à venir.

L'idée principale est de trouver beaucoup d'éléments de C qui sont des p-ièmes puissances dans E mais *non* dans C. La structure de D et C comme $\mathbb{Z}G$-module est compliquée, mais il suffira de disposer d'une bonne $\mathbb{Z}$-base de D :

PROPOSITION 1.2. *Posons* $S_I = \{\prod_{i\in I}\sigma_i^{a_i} \mid 0 \le a_i \le p-2\}$ *pour tout* $\emptyset \ne I \subset \{1,\dots,l\}$ (*donc* $S_I \subset G$). *Alors*

$$B = \{x_I^\sigma \mid \emptyset \ne I \subset \{1,\dots,l\},\ \sigma \in S_I\} \cup \{x_{\{i\}}^{\sigma_i^{p-1}} \mid i = 1,\dots,l\}$$

est une $\mathbb{Z}$*-base de* $D/\{\pm 1\} = D/torsion$.

Démonstration. Le cardinal de B est

$$\sum_{I\ne\emptyset}(p-1)^{|I|} + l = \sum_{1\le a\le l}\binom{l}{a}(p-1)^a + l = (p-1+1)^l - 1 + l,$$

ce qui est égal au rang de D. Il suffit donc de montrer que B engendre D modulo $\{\pm 1\}$. On va montre par récurrence sur $a = |I|$ que les x_I^σ ($\sigma \in G$) se trouvent tous dans $\pm\langle B\rangle$. Pour $|I| = 1$, ceci résulte directement de la définition de B. Prenons I de cardinal au moins 2. Soit $D_{<I}$ engendré par tous les x_J^σ où J parcourt les parties propres de I. Par récurrence nous savons déjà que $D_{<I}$ est contenu dans $\pm\langle B\rangle$.

Soit A le $\mathbb{Z}G$-sous-module de $D/D_{<I}$ engendré par l'image de x_I. Prenons $i \in I$; soit $N_i = 1 + \sigma_i + \ldots + \sigma_i^{p-1}$ l'élément normique attaché au groupe $\langle\sigma_i\rangle$. Alors la relation bien connue

$$N_{K_I/K_{I-\{i\}}}(1-\zeta_I) = (1-\zeta_{I-\{i\}})^{(1-\mathrm{Frob}_{q_i}^{-1})}$$

entraîne que N_i annule le module A, pour tout i dans I. C'est une conséquence facile que A est déjà engendré (en tant que $\mathbb{Z}$-module) par les x_I^σ où $\sigma = \prod_i \sigma_i^{a_i}$ et les a_i varient seulement entre 0 et $p-2$: les termes x_I^σ avec des a_i valant $p-1$ sont rendus superflus par les relations. Donc B engendre tous les conjugués de x_I modulo $D_{<I}$; or on avait déjà $D_{<I} \subset \pm\langle B\rangle$, ce qui termine la récurrence.

2. Extraction de racines, et calculs d'indices. Nous gardons toute la notation de la section précédente, et nous allons fabriquer un sous-module $U \subset D$ (en fait $U \subset C$) dont "presque tous les éléments" sont des p-ièmes puissances dans K. Pour $\emptyset \ne I \subset \{1,\dots,l\}$, posons

$$y_I = x_I^{e_I} \quad \text{avec} \quad e_I = \prod_{i\in I}(1-\sigma_i)^{p-2}\,;$$

$$U = \langle y_I^\sigma \mid \emptyset \ne I \subset \{1,\dots,l\},\ \sigma \in G\rangle \subset C.$$

La proposition suivante servira pour extraire des racines d'éléments de U plus loin. Soit L le sous-groupe multiplicatif libre de $\mathbb{Q}^*$ engendré par $q_1,\dots,q_l$.

Proposition 2.1. *Pour tout $u \in U$ et $\sigma \in G$ il existe $\psi_u(\sigma) \in L$ et $f_u(\sigma) \in D$ tels que*

$$u^{1-\sigma} = \psi_u(\sigma) \cdot f_u(\sigma)^p.$$

De plus, la classe de $\psi_u(\sigma)$ dans L/L^p est uniquement déterminée.

Démonstration. L'unicité de $\psi_u(\sigma)$ modulo L^p est une conséquence du fait que $K^p \cap L = L^p$; ce dernier fait est clair puisque l'extension $K/\mathbb{Q}$ est normale et ne contient pas ζ_p, donc elle ne contient aucune extension non triviale $\mathbb{Q}(\sqrt[p]{x})$.

Pour établir l'existence, il suffit bien sûr de prendre $u = y_I$, avec $\emptyset \neq I \subset \{1, \dots, l\}$ comme toujours. Notons de plus que si la proposition est vraie pour u fixé et deux éléments σ et τ, alors elle est vraie pour $\sigma\tau$:

$$(*) \qquad \begin{aligned} u^{1-\sigma\tau} = u^{1-\sigma} u^{\sigma(1-\tau)} &= \psi_u(\sigma) \cdot f_u(\sigma)^p \psi_u(\tau)^\sigma \cdot f_u(\tau)^{p\sigma} \\ &= \psi_u(\sigma)\psi_u(\tau)(f_u(\sigma) f_u(\tau)^\sigma)^p, \end{aligned}$$

il suffira donc de prendre $\psi_u(\sigma\tau) = \psi_u(\sigma)\psi_u(\tau)$ et $f_u(\sigma\tau) = f_u(\sigma) f_u(\tau)^\sigma$. Nous pourrons donc prendre $\sigma = \sigma_i$, et même $i \in I$ (autrement $y_I^{1-\sigma_i} = 1$). Une récurrence sur $|I|$ nous permet de supposer que la proposition est vraie pour tout u engendré par les y_J avec J partie propre de I.

Par un calcul élémentaire on trouve que

$$(1-\sigma_i)^{p-2}(1-\sigma_i) = (1-\sigma_i)^{p-1} = N_i + p\alpha$$

pour un $\alpha \in \mathbb{Z}[\sigma_i]$ convenable. En posant $J = I - \{i\}$, nous trouvons

$$y_I^{1-\sigma_i} = x_I^{(N_i + p\alpha)\prod_{j\in J}(1-\sigma_j)^{p-2}} = (x_I^{N_i})^{\prod_{j\in J}(1-\sigma_j)^{p-2}} \cdot w^p,$$

où w est un élément de D.

Si J n'est pas vide, alors $x_I^{N_i}$ est de la forme $x_J^{1-\tau}$ avec $\tau \in \langle \sigma_j \rangle_{j\in J}$ (c'est la relation du système eulérien), et le dernier terme s'évalue grâce à l'hypothèse de récurrence, ce qui nous donne

$$y_I^{1-\sigma_i} = y_J^{1-\tau} \cdot w^p = \psi_{y_J}(\tau) f_{y_J}(\tau)^p w^p,$$

et on a terminé. Dans le cas $J = \emptyset$ on trouve $x_I^{N_i} = q_i \in L$, et on a également terminé.

De la formule $(*)$ et du fait que $\psi_u(\sigma) \in L/L^p$ est bien défini par la formule de 2.1, on tire aussitôt :

Corollaire 2.2. *Pour tout $u \in U$, l'application $\psi_u : G \to L/L^p$ est un homomorphisme.*

Définition. Soit $\Psi : U \to \mathrm{Hom}(G, L/L^p)$ donné par $\Psi(u) = \psi_u$.

Lemme 2.3. *Ψ est un homomorphisme.*

Démonstration. C'est bien clair en vue de la construction de Ψ.

Considérons maintenant $u \in \ker(\Psi)$. D'après la proposition 2.1 on trouve une écriture

$$u^{1-\sigma} = f_u(\sigma)^p$$

avec $f_u(\sigma) \in D$ pour tout $\sigma \in G$. Observons que $f_u(\sigma) \in D$ est unique puisque K ne contient pas ζ_p. La formule $(*)$ ci-haut montre :

LEMME 2.4. *$f_u : G \to D$ est un 1-cocycle.*

La proposition clé de cette section est maintenant la suivante :

PROPOSITION 2.5. *Pour tout $u \in \ker(\Psi) \subset U$, il existe $\alpha(u) \in K^*$ et $\varphi(u) \in L$ tels que*

$$u = \varphi(u) \cdot \alpha(u)^p.$$

De plus, $\varphi(u)$ est bien défini modulo L^p, et $\varphi : \ker(\Psi) \to L/L^p$ est un homomorphisme.

Démonstration. Pour voir l'unicité de $\varphi(u)$ modulo L^p, on raisonne comme dans la démonstration de la proposition 2.1.

Pour l'existence, nous citons d'abord le lemme 2.4 qui fournit $u^{1-\sigma} = f_u(\sigma)^p$ avec un 1-cocycle $f_u : G \to D$. D'après le théorème 90 de Hilbert, il existe $\alpha \in K^*$ tel que $\alpha^{1-\sigma} = f_u(\sigma)$ pour tout $\sigma \in G$. Nous affirmons que $u\alpha^{-p}$ est un nombre rationnel. En effet, $(u\alpha^{-p})^{1-\sigma} = u^{1-\sigma}(\alpha^{1-\sigma})^{-p} = f_u(\sigma)^p f_u(\sigma)^{-p} = 1$ pour tout $\sigma \in G$.

Donc $u = c \cdot \alpha^p$ pour un $c \in \mathbb{Q}$. Puisque u est une unité, et les premiers $q_1, \ldots, q_l$ sont les seuls qui se ramifient dans $K/\mathbb{Q}$, on voit que la q-valuation de c est un multiple de p pour tout premier q distinct de $q_1, \ldots, q_l$. Quitte à multiplier α par un rationnel, on peut donc s'arranger pour que c soit dans L (noter aussi que -1 est une p-ième puissance). Ceci achève la preuve.

DÉFINITION. Posons $N = \ker(\varphi)$ où $\varphi : \ker(\Psi) \to L/L^p$ est donné par la proposition 2.5.

REMARQUE 2.6. Tout élément de N est une p-ième puissance dans K d'après 2.5, et même une p-ième puissance dans E puisque $N \subset U \subset E$.

LEMME 2.7. *L'indice $[U : N]$ divise $p^l|\mathrm{Im}(\Psi)|$, et $|\mathrm{Im}(\Psi)|$ divise p^{l^2}.*

Démonstration. Le deuxième énoncé est clair puisque Ψ prend ses valeurs dans l'espace vectoriel $\mathrm{Hom}(G, L/L^p)$ sur $\mathbb{Z}/p$, qui est de dimension $\mathrm{rg}_p(G) \cdot \mathrm{rg}_p(L/L^p) = l \cdot l = l^2$.

Pour le premier, notons que $[U : N] = [U : \ker(\Psi)][\ker(\Psi) : N]$; le facteur $[\ker(\Psi) : N]$ est égal à l'ordre de l'image de φ qui à son tour divise p^l, et le facteur $[U : \ker(\Psi)]$ vaut $|\mathrm{Im}(\Psi)|$.

Nous allons maintenant passer à l'étude de l'indice $[E : C]$. Rappelons que $C = D \cap E$ et que $U \subset C$. Il nous faut un lemme préparatoire.

Lemme 2.8. *La famille* $\{y_I C^p \mid \emptyset \neq I \subset \{1,\dots,l\}\} \cup \{y_{\{i\}}^{\sigma_i} C^p \mid i = 1,\dots,l\}$ *est libre sur* $\mathbb{Z}/p$ *dans l'espace vectoriel* C/C^p *(même dans* D/D^p*).*

Démonstration. Rappelons que $y_I = x_I^{e_I}$ avec $e_I = \prod_{i\in I}(1-\sigma_i)^{p-2}$. Par conséquent, les classes $y_I D^p$ pour $|I| > 2$ proviennent de certaines combinaisons d'éléments de base x_I^σ comme dans la proposition 1.2 (σ étant toujours de degré au plus $p-2$ en toute "variable" σ_i), et font partie d'une $\mathbb{Z}$-base de D. Pour $I = \{i\}$, on trouve également que les deux éléments $x_I^{e_I}$ et $x_I^{e_I(1-\sigma_i)}$ font partie d'une $\mathbb{Z}$-base de D et restent donc libres dans D/D^p.

Pour l'énoncé de l'avant-dernier résultat, définissons $d \geq 0$ par $|\mathrm{Im}(\Psi)| = p^d$. Rappelons que d est trivialement borné par l^2.

Théorème 2.9. *On a les divisibilités suivantes* :

$$p^{2^l-d-1} \mid [E : C],$$

et par conséquent (*voir la proposition* 1.1)

$$p^{2^l-d-1} \mid h_K.$$

Démonstration. Nous allons effectivement montrer que p^{2^l-d-1} divise l'ordre de E/E^pC, c'est-à-dire, que la dimension de E/E^pC sur $\mathbb{Z}/p$ vaut au moins $2^l - d - 1$. De la suite courte exacte $0 \to C/C \cap E^p \simeq E^pC/E^p \to E/E^p \to E/E^pC \to 0$ et du fait que E/E^p est un espace vectoriel de dimension $p^l - 1$ sur $\mathbb{Z}/p$ (Dirichlet), on déduit qu'il suffit de montrer que

$$\dim_{\mathbb{Z}/p}(C/C \cap E^p) \leq p^l - 2^l + d.$$

Selon la remarque 2.6, nous savons que $N \subset E^p$. Soit $\overline{N}$ l'image de N dans C/C^p. Donc $C/C \cap E^p$ est image épimorphe de $(C/C^p)/\overline{N}$. Or la dimension de C/C^p vaut encore $p^l - 1$; il suffira donc de montrer que

$$\dim_{\mathbb{Z}/p}(\overline{N}) \geq 2^l - d - 1.$$

Or le lemme 2.8 nous apprend que $\dim_{\mathbb{Z}/p}(\overline{U})$ est au moins $2^l - 1 + l$. Comme dernière réduction, nous sommes donc amenés à montrer que $\dim_{\mathbb{Z}/p}(\overline{U}/\overline{N})$ ne dépasse pas $l + d$. Mais c'est une conséquence immédiate du lemme 2.7.

Remarquons tout de suite que le théorème précédent donne la divisibilité de h_K par $p^{2^l-l^2-1}$. Malheureusement, cet énoncé est vide pour $l \leq 4$. C'est d'accord pour $l = 1$ et $l = 2$ car des exemples montrent qu'on ne peut s'attendre à une divisibilité de h_K par p, mais c'est dommage pour $l = 3$ et $l = 4$. Le reste de cet article sera consacré à une étude détaillée du nombre d, dans le but d'améliorer le théorème 2.9.

3. Etude de l'image de Ψ, et résultats finaux. Le résultat de cette section est le suivant :

THÉORÈME 3.1. $d \leq l^2 - l + 1$.

Ceci donne, en vue du théorème 2.9, le résultat principal de ce travail :

THÉORÈME 3.2. *Le nombre de classes d'un corps abélien K, composé de l corps de degré premier p et conducteur q_i, où les q_i sont des premiers distincts entre eux et congrus à 1 modulo p, est divisible par $p^{2^l - l^2 + l - 2}$.*

On voit que l'exposant du théorème prend des valeurs positives à partir de $l = 4$. Nous allons quand même dans la suite obtenir au moins un résultat partiel pour $l = 3$.

Faisons brièvement la comparaison avec les résultats de Cornell [Co]. (Remarquons d'ailleurs qu'il semble que la version longue, annoncée dans l'article court [Co], n'ait jamais paru.) Avec notre notation, le résultat de Cornell dit que $p^{p^{l-4}-1}$ divise h_K. Ce qu'il montre effectivement, c'est que l'espace vectoriel Cl_K/pCl_K sur $\mathbb{Z}/p$ est de dimension au moins $p^{l-4} - 1$. Sa méthode ne donne rien pour $l = 3$ ou $l = 4$. Notre résultat est plus fort que le sien dans les cas suivants : $l = 4$ évidemment ; $l = 5$ et $p \leq 11$ (en fait, pour $p = 11$, c'est l'égalité) ; $l = 6$ et $p \leq 5$; $l = 7, 8, 9, 10$ et $p = 3$. Dans tous les cas qui restent (une infinité bien sûr), la borne inférieure de Cornell est la meilleure.

Dans [CR], les auteurs obtiennent que $p^{l(l-3)/2}$ divise h_K. Ceci égale notre résultat pour $l = 4$, mais c'est plus faible que le nôtre pour $l > 4$. Le cas $l = 3$ offre un intérêt particulier ; voir la discussion vers la fin de ce travail.

Tout le reste de cette section est occupé par la démonstration du théorème 3.1, qui est raffinée mais très technique. Nous allons essayer d'en faire ressortir l'idée, à l'aide du cas $l = 3$.

Fixons un peu de notation. On a une égalité $\mathrm{Frob}_{q_i} = \prod_{j \neq i} \sigma_j^{a_{ij}}$; c'est l'automorphisme de Frobenius attaché au premier q_i sur le composé de tous les K_j, $j \neq i$. Les a_{ij} définissent une matrice A de format l par l à coefficients dans $\mathbb{Z}/p$, dont la diagonale n'est pas définie. Rappelons que $N_i = 1 + \sigma_i + \ldots + \sigma_i^{p-1}$. Alors, si $i \in I$ et $J = I - \{i\}$ n'est pas vide,

$$x_I^{N_i} = x_J^{1 - \mathrm{Frob}_{q_i}^{-1}} = x_J^{1 - \prod_{j \neq i} \sigma_j^{-a_{ij}}}.$$

Rappelons aussi que $y_I^{1-\sigma_i}$ est égal au produit de $x_I^{N_i \prod_{j \in J} (1-\sigma_j)^{p-2}}$ par une p-ième puissance d'un élément de D. Finalement, il est aisé de voir qu'on a la règle $\Psi(u^\tau)(\sigma) = \Psi(u)(\sigma)$; en d'autres mots, l'homomorphisme $\Psi(-)(\sigma)$, pour $\sigma \in G$ fixé, est G-équivariant, si l'on munit L/L^p de la G-action triviale. Nous allons maintenant prendre $l = 3$ et calculer, à titre d'exemple, la valeur

$\Psi(y_{1,2,3})(\sigma_1)$. Ici, $y_{1,2,3}$ est une notation abrégée pour $y_{\{1,2,3\}}$. Tout le calcul qui suit doit se lire dans D/D^p.

$$\begin{aligned}\Psi(y_{1,2,3})(\sigma_1) &= y_{1,2,3}^{1-\sigma_1} = x_{1,2,3}^{N_1(1-\sigma_2)^{p-2}(1-\sigma_3)^{p-2}}\\ &= y_{2,3}^{1-\mathrm{Frob}_{q_1}^{-1}}\\ &= \Psi(y_{2,3})(\mathrm{Frob}_{q_1}^{-1})\\ &= \Psi(y_{2,3})(\sigma_2)^{-a_{12}}\Psi(y_{2,3})(\sigma_3)^{-a_{13}}\\ &= (y_3^{1-\mathrm{Frob}_{q_2}^{-1}})^{-a_{12}}(y_2^{1-\mathrm{Frob}_{q_3}^{-1}})^{-a_{13}}\\ &= (\Psi(y_3)(\sigma_3)^{-a_{23}})^{-a_{12}}(\Psi(y_2)(\sigma_2)^{-a_{32}})^{-a_{13}}.\end{aligned}$$

Or $\Psi(y_3)(\sigma_3) = y_3^{1-\sigma_3} = x_3^{N_3} = q_3$, et de façon analogue $\Psi(y_2)(\sigma_2) = q_2$. D'où le résultat final :

$$\Psi(y_{1,2,3})(\sigma_1) = q_3^{a_{23}a_{12}}q_2^{a_{32}a_{13}}.$$

Pour comprendre ce qui se passe en général, notons qu'on pourra, pour $i \in J \subset \{1,\dots,l\}$, certainement écrire

$$\Psi(y_J)(\sigma_i) = \prod_{j\in J} q_j^{m(J;i,j)};$$

remarquons que $\Psi(y_J)(\sigma_i) = 1$ pour i non dans J. Les entiers $m(J;i,j)$ ne sont déterminés que modulo p ; ils forment une matrice géante dont les rangées sont indexées par les parties J non vides de $\{1,\dots,l\}$, et les colonnes sont, pour l'instant, indexées par les paires (i,j). Nous allons tâcher de réduire la taille de la matrice. Pour l'instant, nous allons donner la matrice pour $l = 3$ au grand complet. On trouve facilement que $\Psi(y_1)(\sigma_1) = q_1$ et ainsi de suite. De même on trouve (le lecteur fournira aisément les quelques étapes) que $\Psi(y_{1,2})(\sigma_1) = q_2^{-a_{12}}$, et ainsi de suite. Voici la matrice :

$$\begin{array}{c} \\ \{1\}\\ \{2\}\\ \{3\}\\ \{1,2\}\\ \{1,3\}\\ \{2,3\}\\ \{1,2,3\}\end{array}\!\!\begin{array}{c}\begin{array}{ccccccccc}12 & 13 & 23 & 21 & 31 & 32 & 11 & 22 & 33\end{array}\\ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\ -a_{12} & 0 & 0 & -a_{21} & 0 & 0 & 0 & 0 & 0\\ 0 & -a_{13} & 0 & 0 & -a_{31} & 0 & 0 & 0 & 0\\ 0 & 0 & -a_{23} & 0 & 0 & -a_{32} & 0 & 0 & 0\\ a_{32}a_{13} & a_{23}a_{12} & a_{21}a_{13} & a_{23}a_{31} & a_{32}a_{21} & a_{31}a_{12} & 0 & 0 & 0\end{pmatrix}\end{array}$$

On constate tout de suite que le rang de cette matrice sera 3 plus le rang de la matrice M obtenue en retranchant les rangées indexées par les singletons, et les colonnes indexées par les paires (i,i). Ceci vaut en général, quitte à remplacer 3 par l, puisque le bloc nord-ouest de l rangées et $l^2 - l$ colonnes est toujours zéro, et le bloc nord-est $l \times l$ est toujours une matrice identité.

C'est maintenant un calcul facile de trouver le rang de la matrice M pour $l = 3$. (On élimine un à un les éléments de la dernière rangée.) Résultat: Le rang est non maximal (inférieur à quatre) si et seulement si $a_{12}a_{23}a_{31} = a_{21}a_{32}a_{13}$. A noter que les deux produits valent zéro si l'une parmi les trois premières rangées de M est zéro.

Soit maintenant $l \geq 3$ quelconque ; soit M la matrice des $m(J; i, j)$ où J parcourt les parties de cardinal au moins 2 de $\{1, \ldots, l\}$, et où (i, j) parcourt toutes les paires avec $i \neq j$, $1 \leq i, j \leq l$.

PROPOSITION 3.3. *Soit* $|J| = n$. *Alors*

$$m(J; i, j) = (-1)^{n-1} \sum_{k} \prod_{r=1}^{n-1} a_{k(r)k(r+1)},$$

où k *parcourt tous les chemins reliant* i *à* j *dans* J, *c'est-à-dire*, *toutes les applications bijectives* $k : \{1, \ldots, n\} \to J$ *telles que* $k(1) = i$ *et* $k(n) = j$.

NOTATION. Pour abréger dans la suite, posons $a(k) = \prod_{r=1}^{n-1} a_{k(r)k(r+1)}$. On pourrait appeler ceci la valeur de la matrice A le long le chemin k.

Démonstration. C'est une récurrence sur n sans surprise, dont tous les ingrédients sont déjà contenus dans notre calcul exemplaire pour $l = 3$; nous renonçons donc à donner les détails.

Le théorème 3.1 est donc équivalent à l'énoncé suivant : Le rang de la matrice M ne dépasse jamais $(l^2 - l + 1) - l = l^2 - 2l + 1$.

Notre méthode de démonstration consiste à considérer les a_{ij} comme des variables sur le corps $\mathbb{Z}/p$; pour ne pas compliquer la notation, gardons le même nom M pour notre matrice dans ce nouveau sens. Nous allons effectivement démontrer que le rang de M (dans ce nouveau sens) vaut *exactement* $l^2 - 2l + 1$. Ceci permet aussi de dire qu'il ne sera pas possible d'améliorer le théorème 3.1 en général, car les a_{ij} (considérés pour un instant de nouveau comme éléments de $\mathbb{Z}/p$, en fonction du corps K) ne sont soumis à aucune contrainte.

Pour suivre les développements il sera toujours utile de se reporter à la matrice explicite donnée ci-haut. Nous allons éliminer les rangées avec $|J| = 2$ et les colonnes (i, j) avec $i < j$; le résultat sera une matrice $\widetilde{M}$ telle que

$$\operatorname{rang}(M) = \operatorname{rang}(\widetilde{M}) + \binom{l}{2}.$$

En détail : Pour tout J_0 de cardinal deux, écrivons $J_0 = \{i, j\}$ avec $i < j$. L'élément en position $(J_0; i, j)$ (notons qu'il vaut a_{ij}!) est déclaré comme élément pivot, et on annule les autres éléments de sa colonne par le procédé d'usage : à toute rangée indexée J avec J_0 proprement contenu dans J, on additionne $-m(J; i, j)/a_{ij}$ fois la rangée J_0. Après avoir fait ceci pour tout J_0

de cardinal deux, les colonnes $i < j$ contiennent exactement un élément non nul, en rangée i, j. Si nous formons donc $\widetilde{M}$ comme annoncé, nous obtenons bien $\operatorname{rang}(M) = \operatorname{rang}(\widetilde{M}) + \binom{l}{2}$. Soit M^* la matrice obtenue de $\widetilde{M}$ en multipliant la colonne (j,i) $(i<j)$ par a_{ij}, pour éliminer les dénominateurs introduits par les opérations précédentes. Soit $m^*(J;j,i)$ l'entrée de M^* placée en ligne J et colonne (j,i). Ce qui permet de continuer, c'est l'observation que $m^*(J;j,i)$ peut bien être exprimé en langage de théorie des graphes. En effet, cette entrée est zéro si i ou j ne sont pas dans J, et elle vaut

$$a_{ij}m(J;j,i) - a_{ji}m(J;i,j) \qquad \text{si } i,j \in J.$$

Un peu de vocabulaire : Soit $|J| = n$. Une *boucle* b dans J sera une application bijective $b : \{0,\dots,n-1\} \to J$ et on identifiera deux boucles si l'une b' provient de l'autre b par un décalage cyclique de la numérotation par une constante c modulo n : $b'(i) = b(i+c)$ pour tout i. La boucle b *passe par* $i \to j$ s'il existe $0 \le t < n$ tel que ou bien $b(t) = i,\ b(t+1) = j$ (la boucle passe par $i \to j$ dans le bon sens), ou bien $b(t) = j,\ b(t+1) = i$ (la boucle passe à contre-sens). Nous rappelons que $a(b)$ est défini comme $\prod_{t=0}^{n-1} a_{b(t)b(t+1)}$. Nous pouvons donc écrire, en tenant compte de notre formule dans 3.3 pour $m(J;j,i)$ et $m(J;i,j)$:

$$m^*(J;j,i) = \sum_b \pm a(b),$$

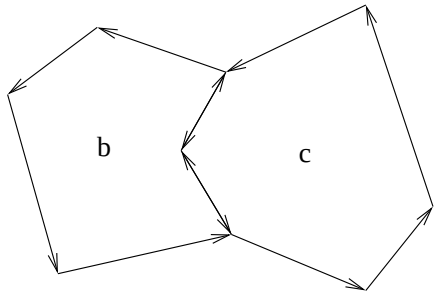
où l'on somme sur toutes les boucles de J passant par $i \to j$, et le signe est plus ou moins selon que la boucle passe dans le bon ou mauvais sens. Pour la suite, on notera $m^*(J;\{i,j\})$ plutôt que $m^*(J;j,i)$. Chaque ensemble $\{i,j\}$ est considéré comme arête orientée : la flèche pointe vers le plus grand parmi i et j.

On va montrer que toute rangée de M^* avec $|J| \ge 4$ est combinaison linéaire de rangées avec $|J| = 3$, et de plus, que l'espace engendré par les rangées avec $|J| = 3$ est de dimension $\binom{l}{2} - l + 1$. Ceci donne bien $\operatorname{rang}(M) = \operatorname{rang}(\widetilde{M}) + \binom{l}{2} = \binom{l}{2} - l + 1 + \binom{l}{2} = l^2 - 2l + 1$ comme requis.

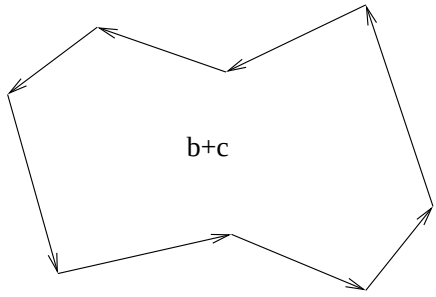
Regardons d'abord la rangée pour $J = \{i,j,k\}$. Choisissons une orientation du triangle J. Alors il existe exactement deux boucles : b^+, celle dans le sens de l'orientation, et b^-, l'opposée. Quelle est l'entrée $m^*(J;\{i,j\})$? Elle vaut : $a(b^+) - a(b^-)$ si b^+ passe par $i \to j$ dans le bon sens (d'abord le plus petit, et puis le plus grand parmi i et j), et $-a(b^+) + a(b^-)$ dans le cas contraire. Nous avons donc l'agréable surprise que, à un facteur constant non nul près, la rangée J est faite de chiffres 0, 1, et -1 : 0 si $\{i,j\}$ n'est pas partie du triangle J ; $+1$ si l'orientation sur $\{i,j\}$ coïncide avec l'orientation du triangle J, et -1 sinon.

Pour $|J| \ge 4$ les choses se compliquent car il y a de nombreuses boucles. En effet, les rangées seront des combinaisons linéaires convenables qui pro-

viennent de boucles. Pour chaque boucle b de J, on a une rangée R_b où $R_b(i,j)$ vaut 0, 1 ou -1 selon les mêmes règles qu'à la fin du dernier paragraphe. On peut, dans certains cas, additionner des boucles (sur des ensembles différents). Ceci est visualisé par le schéma suivant : soient b et c deux boucles qui ont un bout de chemin en commun, mais à contre-sens :



On obtient comme somme une boucle $b+c$:



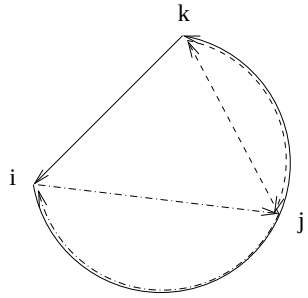
et bien évidemment $R_{b+c} = R_b + R_c$.

Nous affirmons que toute boucle de longueur quelconque ≥ 3 est somme de triangles dans ce sens. En effet, c'est assez clair. Mais cela entraîne que tout R_b, b boucle sur J, est combinaison linéaire (même somme) de rangées R_c (c boucle sur un triangle). Puisque toute rangée J est une combinaison linéaire des R_b (b boucle sur J), on trouve que les rangées avec J de cardinal 3 engendrent toutes les rangées de M^*.

Mais ce n'est pas tout : même parmi les rangées provenant de triangles, il y a des relations de dépendance entre boucles triangulaires qui proviennent de boucles plus longues. Soient effectivement $1 \leq i < j \leq l$ tels que $j \neq i+1$. (Il y a $\binom{l}{2} - l + 1$ telles paires.) Toute paire (i,j) de ce type donne une boucle $i \to i+1 \to \ldots \to j \to i$, appelons-la $b(i,j)$. Tout triangle orienté s'exprime comme combinaison linéaire de boucles $b(i,j)$ convenables! Le cas générique est celui d'un triangle $i \to j \to k \to i$ avec $i < j < k$ et $j \neq i+1$, $k \neq j+1$. Alors on a la formule

$$(i \to j \to k \to i) = b(i,k) - b(i,j) - b(j,k).$$

Cette formule devient claire si l'on regarde le dessin suivant :



Nous laissons au lecteur le soin de discuter les cas non génériques (e.g., $j = i + 1$). Il est facile de voir que les rangées $R_{b(i,j)}$ associées à nos boucles spéciales sont linéairement indépendantes.

Ceci termine le calcul du rang des matrices M^*, $\widetilde{M}$, et finalement M ; comme nous l'avons dit, ceci démontre aussi le théorème 3.1.

Remarquons enfin que la borne générale du théorème 3.1 donne $d \leq 7$ pour $l = 3$, ce qui donne un exposant zéro dans la p-puissance qui divise h_K selon 3.2. Par conséquent, si la matrice M a un rang non maximal pour $l = 3$, nous trouvons bien que p divise h_K. Or nous avons trouvé, chemin faisant, un critère bien facile pour que $\mathrm{rang}(M) < 4$ (rappelons que M est obtenu en retranchant trois rangées et trois colonnes de la grosse matrice donnée au complet ci-haut) : on doit avoir une égalité $a_{12}a_{23}a_{31} = a_{21}a_{32}a_{13}$. Remarquons que [CR] offre un résultat légèrement plus fort : la dite égalité est même équivalente à ce que p divise h_K ; voir page 460 de loc.cit., surtout la matrice $(**)$. Appelons cette matrice M_{CR}. Notre résultat donne en fait que $p^{4-\mathrm{rang}(M)}$ divise h_K. Les résultats de [CR] disent que $p^{3-\mathrm{rang}(M_{\mathrm{CR}})}$ divise h_K. On trouve sans trop de peine qu'on a toujours $3 - \mathrm{rang}(M_{\mathrm{CR}}) \leq 4 - \mathrm{rang}(M)$, avec quelques cas d'inégalité : par exemple si a_{12} et a_{13} ne sont pas nuls et les quatre autres $a_{ij} = 0$, on trouve $1 < 2$. Donc dans un certain sens, nos résultats sont une légère amélioration sur [CR]. Ajoutons finalement que le travail [Fr] contient des critères précis pour que h_K soit divisible par p dans les cas $l = 1, 2, 3$, et on retrouve aussi le résultat que $p \,|\, h_K$ toujours lorsque $l > 3$.

Références

[Co] G. Cornell, *Exponential growth of the l-rank of the class group of the maximal real subfield of cyclotomic fields*, Bull. Amer. Math. Soc. 1 (1983), 55–58.

[CR] G. Cornell and M. Rosen, *The class group of an absolutely abelian l-extension*, Illinois J. Math. 32 (1988), 453–461.

[Fr] A. Fröhlich, *Central Extensions*, *Galois Groups*, *and Ideal Class Groups of Number Fields*, Contemp. Math. 24, Amer. Math. Soc., Providence, 1983.

[Ha] S. Hachami, *Unités cyclotomiques et cohomologie*, thèse de PhD, Université Laval, Décembre 1998.

[Ku] R. Kučera, *On the Stickelberger ideal and circular units of a compositum of quadratic fields*, J. Number Theory 56 (1996), 139–166.

[Si] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. 62 (1980), 181–234.

Institut für theor. Informatik und Mathematik
Fakultät für Informatik
Universität der Bundeswehr München
85577 Neubiberg, Allemagne
E-mail: greither@informatik.unibw-muenchen.de

École nationale d'administration Rabat
1, Avenue de la Victoire
BP 165, Rabat, Maroc

Přírodovědecká fakulta
Masarykova univerzita
Janáčkovo náměstí 2a
662 95 Brno, République Tchèque
E-mail: kucera@math.muni.cz

Received on 27.7.1999 (3663)