manuscripta math. 92, 303 - 323 (1997)

manuscripta mathematica

Tours de Hilbert des extensions cubiques cycliques de $\mathbb{Q}$

Christian Maire

Reçu le 29 avril 1996

In this paper, we study the problem of the Hilbert tower of a number field. We use a refinement of the result of Golod-Safarevic in the theory of the p-group, due to Schoof. Using the action of an abelian group on a finite p-group, and the characters theory of finite groups, we obtain a new criterion of the non finiteness of the Hilbert p-tower of a cubic cyclic extension over $\mathbb{Q}$. The used method give too some good results for a totally imaginary cyclic extension of degree 6 over $\mathbb{Q}$.

§1. Introduction.

Soit k un corps de nombres et soit p un nombre premier.
Notons par k_1 la p-extension abélienne non-ramifiée maximale de k ; k_1 est le p-corps de Hilbert de k.
Rappelons que l'application d'Artin donne un isomorphisme entre le p-groupe des classes cl_k de k et le groupe de Galois $Gal(k_1/k)$.
On peut alors construire à partir de k une suite de corps $(k_i)_{i\geq 0}$ de la manière suivante : $k_0 = k$ et k_{i+1} est le p-corps de Hilbert de k_i.
On note par L la réunion de ces extensions de k : c'est la p-tour de Hilbert de k ; L est également la p-extension non-ramifiée maximale de k.
On dit que la p-tour de k est finie lorsque l'extension L/k est finie et qu'elle est infinie dans le cas contraire.
En 1964, Golod et Safarevic ont donné un critère de non-finitude pour les p-tours ; il permet par exemple d'affirmer que le corps quadratique $\mathbb{Q}(\sqrt{-2.3.5.7.11.13})$ a une 2-tour infinie.
Ce critère est une conséquence d'un résultat de théorie des p-groupes, qui donne une condition nécessaire pour qu'un p-groupe G soit fini.
Plus tard (1965-...), Koch et Vinberg ont donné un rafinement du résultat de théorie des p-groupes de Golod-Safarevic ([K1], [K2], [V]) ; celui-ci fait intervenir les filtrations de Zassenhaus du groupe des relations d'un p-groupe G.

En 1986, Schoof a donné un rafinement homologique de l'inégalité de Golod-Safarevic ([Sc]) ; c'est ce résultat que nous utiliserons. En voici le rappel.
Soit G un p-goupe fini et soit I l'idéal d'augmentation de l'algèbre $\mathbb{F}_p[G]$.
Si A est un G-module, nous noterons par $H_i(A)$ le groupe homologique $H_i(G, A)$.
En utilisant les homomorphismes naturels suivants :

$$\cdots \longrightarrow H_1(I^k) \longrightarrow H_1(I^{k-1}) \longrightarrow \cdots \longrightarrow H_1(I)\,,$$

on obtient une filtration de $H_1(I)$ par les images des groupes $H_1(I^k)$ dans $H_1(I)$.
Notons alors par $R_k(G)$, $k \geq 2$, le quotient suivant :

$$R_k(G) = \frac{Im\left(H_1(I^{k-1}) \longrightarrow H_1(I)\right)}{Im\left(H_1(I^k) \longrightarrow H_1(I)\right)}\,,$$

et posons $r_k(G) = d_p R_k(G)$, où $d_p R_k(G)$ désigne le p-rang de $R_k(G)$.
On peut alors noter que

$$\sum_{k\geq 2} r_k(G) = r = d_p H_2(\mathbb{F}_p).$$

Si l'on note par d le p-rang de $H_1(\mathbb{F}_p)$, i.e le p-rang de G, on a donc le résultat suivant, établi par Schoof ([Sc], théorème 2.1) :
Soit G un p-groupe fini, alors

$$\sum_{k\geq 2} r_k(G)t^k - dt + 1 > 0, \quad \forall t \in]0;1[. \tag{1}$$

Rappelons que le résultat de Golod-Safarevic indique que $r > d^2/4$.

Nous allons appliquer le résultat de Schoof au groupe $G = Gal(L/k)$, où k est un corps de nombres et où L est la p-tour de Hilbert de k ; nous essayerons de majorer convenablement $r_2(G)$, voire de l'annuler dans certains cas (§3, §4 et §5), dans la perspective de contredire (1), ce qui montrera alors que la p-tour de Hilbert de k est infinie.

On obtiendra alors le résultat suivant (§5.1, théorème 5.2) :

Soit $k/\mathbb{Q}$ une extension cyclique de degré 3, et soit p un nombre premier différent de 2 et de 3 ; alors si le p-rang du groupe des classes de k est supérieur ou égal à 4, k a une p-tour de Hilbert infinie.

Notons que ce résultat améliore de 2 le rang obtenu par l'inégalité de Golod-Safarevic.

On aura également quelques résultats intéressants dans le cas où $k/\mathbb{Q}$ est une extension cyclique de degré 6 et totalement imaginaire (§5.2, théorème 5.5).

Enfin, dans le paragraphe 6, nous donnerons pour un p-groupe fini G une relation liant d à $r_2(G)$ et à $a_2(G)$, où $a_2(G) = d_p \frac{I^2}{I^3}$; ceci permettra d'obtenir immédiatement le résultat connu suivant :

Soient $p \neq 2$ et k un corps quadratique tels que le p-rang du groupe des classes de ce corps est supérieur ou égal à 2 ; notons par k_1 le p-corps de Hilbert de k. Alors le p-groupe des classes de k_1 est non trivial.

§2. Rappels.

2.1. Résultats classiques.

On peut retrouver l'ensemble de ces rappels dans [R].
Soient donc k un corps de nombres et p un nombre premier. Notons par L la p-tour de Hilbert de k que l'on suppose finie. Rappelons alors deux suites exactes :

$$1 \longrightarrow E_L \longrightarrow \mathcal{U}_L \longrightarrow \frac{\mathcal{U}_L}{E_L} \longrightarrow 1, \tag{2}$$

et

$$1 \longrightarrow \frac{\mathcal{U}_L}{E_L} \longrightarrow \frac{\mathcal{J}_L}{L^\times} \longrightarrow cl_L \longrightarrow 1, \tag{3}$$

où E_L est le groupe des unités de L, cl_L le groupe des classes de L, $\mathcal{J}_L$ le groupe des idèles de L, $\mathcal{U}_L = \prod_v U_{L_v}$, U_{L_v} étant le groupe des unités du corps complété L_v de L en v.

Comme l'extension L/k est non ramifiée, on a

$$\hat{H}^n(G,\mathcal{U}_L) = 1,\ \forall n \in \mathbb{Z},$$

où $G = Gal(L/k)$.
(2) apporte alors

$$\hat{H}^n(G,\frac{\mathcal{U}_L}{E_L}) \simeq \hat{H}^{n+1}(G,E_L).$$

Comme L est la p-tour de Hilbert de k, alors $(|cl_L|,p) = 1$, et ainsi

$$\hat{H}^n(G,cl_L) = 1,\ \forall n \in \mathbb{Z}.$$

(3) apporte alors

$$\hat{H}^n(G,\frac{\mathcal{U}_L}{E_L}) \simeq \hat{H}^n(G,\frac{\mathcal{J}_L}{L^\times}).$$

En utilisant ensuite l'isomorphisme suivant (cf. [T]):

$$\hat{H}^{n-2}(G,\mathbb{Z}) \simeq \hat{H}^n(G,\frac{\mathcal{J}_L}{L^\times}),$$

et en prenant $n = -1$, on obtient

$$\frac{E_k}{N_{L/k}E_L} \simeq H_2(G,\mathbb{Z}), \tag{4}$$

où E_k est le groupe des unités de k.

2.2. Réprésentations linéaires des groupes finis.

On peut trouver une partie de ces rappels dans [Se1].
Soient Δ un groupe abélien fini et p un nombre premier étranger à l'ordre de Δ.
Si $\bar{M}$ désigne un $\mathbb{F}_p[\Delta]$-module, on sait alors que $\bar{M}$ est un $\mathbb{F}_p[\Delta]$-module projectif; les $\mathbb{Z}_p[\Delta]$-modules projectifs étant en correspondance bijective avec les $\mathbb{F}_p[\Delta]$-modules projectifs, on peut donc remonter $\bar{M}$ en un unique $\mathbb{Z}_p[\Delta]$-module projectif M.
Ainsi à tout $\mathbb{F}_p[\Delta]$-module $\bar{M}$, on associe un $\mathbb{Q}_p[\Delta]$-module $M \otimes \mathbb{Q}_p$.

On rappelle ensuite que si deux $\mathbb{Z}_p[\Delta]$-modules projectifs définissent des $\mathbb{Q}_p[\Delta]$-modules isomorphes après produit tensoriel avec $\mathbb{Q}_p$, alors ceux-ci sont isomorphes.
Enfin, on sait que si les caractères de deux $\mathbb{Q}_p[\Delta]$-modules sont égaux, alors ces modules sont isomorphes.

De ceci, il résulte que montrer la trivialité de $\bar{M}$ revient à montrer la trivialité du caractère de $M \otimes \mathbb{Q}_p$; de même, déterminer le p-rang de $\bar{M}$, revient à compter le nombre de caractères $\mathbb{C}_p[\Delta]$-irréductibles intervenant dans la décomposition du caractère de $M \otimes \mathbb{Q}_p$.

Pour un $\mathbb{F}_p[\Delta]$-module $\bar{M}$, nous noterons par $\chi[\bar{M}]$ le caractère de $M \otimes \mathbb{Q}_p$; de plus, l'inégalité $\chi[A] \leq \chi[B]$ signifiera que le caractère du $\mathbb{Q}_p[\Delta]$-module A divise celui de B, i.e

$$\chi[B] = \chi[A] + \textit{somme de caractères.}$$

Notons alors que si l'on a la suite exacte de $\mathbb{F}_p[\Delta]$-modules

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1,$$

alors

$$\chi[B] = \chi[A] + \chi[C]\ ;$$

si l'on a seulement une injection de A vers B (ou bien une surjection de B vers A), alors

$$\chi[A] \leq \chi[B].$$

Enfin, on rappelle que les caractères $\mathbb{Q}_p[\Delta]$-irréductibles s'obtiennent de la façon suivante : Soit ψ un caractère $\mathbb{C}_p[\Delta]$-irréductible de Δ (donc de degré 1) et soit D_ψ le groupe de décomposition de p dans $\mathbb{Q}(\mathcal{O}(\psi))/\mathbb{Q}$, où $\mathcal{O}(\psi)$ est l'ordre de ψ ; alors le caractère $\mathbb{Q}_p[\Delta]$-irréductible associé à ψ est la somme des $\mathbb{Q}_p$-conjugués de ψ, i.e

$$\chi = \sum_{u \in D_\psi} \psi^u.$$

De plus, par cette construction, on obtient l'ensemble des caractères $\mathbb{Q}_p[\Delta]$-irréductibles.

§3. Majorations de $\chi[R_k(G)]$.

A présent, on se place dans la situation suivante :
p est un nombre premier, k désigne un corps de nombres et $k/\underline{k}$ une extension galoisienne de groupe de Galois Δ, avec $|\Delta|$ étranger à p.

Notons par L la p-tour de k, que l'on suppose finie, et par G le groupe de Galois de L/k. Par maximalité de L, $L/\underline{k}$ est galoisienne ; ainsi Δ agit sur l'ensemble des groupes homologiques $H_i(G, A)$, notés $H_i(A)$ (cf. [Se2], Chapitre VII). En particulier, Δ agit sur $R_k(G)$.

Enonçons le résultat principal de cette partie, résultat qui donne deux majorations différentes de $\chi[R_k(G)]$, et qui ne fait intervenir que la partie abélienne de G.

Théorème 3.1 : Majorations de $\chi[R_k(G)]$.
Soit k un corps de nombres, et soit p un nombre premier.
Supposons que la p-tour de Hilbert L de k est finie.
Notons par G le groupe de Galois de L/k, par I^* l'idéal d'augmentation de l'algèbre $\mathbb{F}_p[G^{ab}]$, et par E_k le groupe des unités de k.
Alors on a les deux majorations de $\chi[R_k(G)]$ suivantes :

(i) $$\chi[R_k(G)] \leq \chi^k\left[\frac{G^{ab}}{(G^{ab})^p}\right] - \chi\left[\frac{I^{*k}}{I^{*k+1}}\right],$$

(ii) $$\chi[R_k(G)] \leq \chi\left[\frac{G^{ab}}{(G^{ab})^p}\right] + \chi\left[\frac{E_k}{(E_k)^p}\right],$$

pour tout $k \geq 2$.

Dans les paragraphes 3.1 et 3.2, nous montrerons successivement les deux majorations de $\chi[R_k(G)]$; dans le paragraphe 3.3, on donnera un résultat qui permet d'obtenir $\chi\left[\frac{I^{*2}}{I^{*3}}\right]$ à partir de $\chi\left[\frac{G^{ab}}{(G^{ab})^p}\right]$ (théorème 3.8).

3.1. Première majoration.

3.1.1. Première relation.

Pour $k \geq 2$, on a la suite exacte

$$0 \longrightarrow I^k \longrightarrow I^{k-1} \longrightarrow \frac{I^{k-1}}{I^k} \longrightarrow 0\,,$$

où I est l'idéal d'augmentation de l'algèbre $\mathbb{F}_p[G]$; cette suite exacte devient

$$\cdots \longrightarrow H_1(I^k) \longrightarrow H_1(I^{k-1}) \longrightarrow H_1(\frac{I^{k-1}}{I^k}) \longrightarrow H_0(I^k) \longrightarrow H_0(I^{k-1}) \longrightarrow H_0(\frac{I^{k-1}}{I^k}) \longrightarrow 0,$$

plus précisémment

$$\cdots \longrightarrow H_1(I^k) \longrightarrow H_1(I^{k-1}) \longrightarrow H_1(\frac{I^{k-1}}{I^k}) \longrightarrow \frac{I^k}{I^{k+1}} \longrightarrow 0,$$

d'où

$$0 \longrightarrow \frac{H_1(I^{k-1})}{Im\,(H_1(I^k) \longrightarrow H_1(I^{k-1}))} \longrightarrow H_1(\frac{I^{k-1}}{I^k}) \longrightarrow \frac{I^k}{I^{k+1}} \longrightarrow 0,\ \forall k \geq 2.$$

Cette suite exacte est en fait une suite de $\mathbb{F}_p[\Delta]$-modules ; il vient alors en termes de caractères

$$\chi\left[H_1(\frac{I^{k-1}}{I^k})\right] = \chi\left[\frac{I^k}{I^{k+1}}\right] + \chi\left[\frac{H_1(I^{k-1})}{Im\,(H_1(I^k) \longrightarrow H_1(I^{k-1}))}\right],\ \forall k \geq 2.$$

3.1.2. Passage à l'abélianisé.

Notons par I^* l'idéal d'augmentation de $\mathbb{F}_p[G^{ab}]$, G^{ab} étant l'abélianisé de G. Il vient alors immédiatement, par la projection $\mathbb{F}_p[G] \to \mathbb{F}_p[G^{ab}]$, l'inégalité

$$\chi\left[\frac{I^{*k}}{I^{*k+1}}\right] \leq \chi\left[\frac{I^k}{I^{k+1}}\right],\ \forall k \geq 1.$$

En résumé, nous avons

$$\chi\left[H_1(\frac{I^{k-1}}{I^k})\right] \geq \chi\left[\frac{I^{*k}}{I^{*k+1}}\right] + \chi\left[\frac{H_1(I^{k-1})}{Im\,(H_1(I^k) \longrightarrow H_1(I^{k-1}))}\right],\ \forall k \geq 2.$$

3.1.3. Introduction de $\chi[R_k(G)]$.

On part de la suite d'homomorphismes

$$\cdots \longrightarrow H_1(I^k) \longrightarrow H_1(I^{k-1}) \longrightarrow \cdots \longrightarrow H_1(I^2) \longrightarrow H_1(I).$$

Définissons alors par $\hat{\varphi}_{k-1}$ l'homomorphisme suivant :

$$\begin{aligned} \hat{\varphi}_{k-1} \ :\ H_1(I^{k-1}) \ &\longrightarrow\ \frac{Im\left(H_1(I^{k-1}) \xrightarrow{\varphi_{k-1}} H_1(I)\right)}{Im\left(H_1(I^k) \xrightarrow{\varphi_k} H_1(I)\right)} \\ x \ &\longmapsto\ \varphi_{k-1}(x)\ \textit{modulo}\ \left[Im\left(H_1(I^k) \xrightarrow{\varphi_k} H_1(I)\right)\right]. \end{aligned}$$

On peut constater que $Im\left(H_1(I^k) \longrightarrow H_1(I^{k-1})\right)$ factorise $\hat{\varphi}_{k-1}$ de façon évidente ; de plus $\hat{\varphi}_{k-1}$ est trivialement surjective. Ainsi nous avons

$$\chi\left[\frac{H_1(I^{k-1})}{Im\,(H_1(I^k) \longrightarrow H_1(I^{k-1}))}\right] \geq \chi[R_k(G)],\ \forall k \geq 2.$$

En résumé, nous obtenons

$$\chi\left[H_1(\frac{I^{k-1}}{I^k})\right] \geq \chi\left[\frac{I^{*k}}{I^{*k+1}}\right] + \chi[R_k(G)],\ \forall k \geq 2.$$

3.1.4. Passage au produit tensoriel.

Il ne reste plus qu'à évaluer $\chi\left[H_1(\frac{I^{k-1}}{I^k})\right]$. Rappelons un résultat classique.

Lemme 3.2 :
Parce que G agit trivialement sur $\frac{I^{k-1}}{I^k}$, alors il existe un Δ-isomorphisme entre $H_1(\frac{I^{k-1}}{I^k})$ et $\frac{I}{I^2}\otimes\frac{I^{k-1}}{I^k}$.

Démonstration :
L'isomorphisme entre $\frac{I}{I^2}\otimes\frac{I^{k-1}}{I^k}$ et $H_1(\frac{I^{k-1}}{I^k})$ se déduit de l'application $\mathbb{F}_p$-bilinéaire suivante :

$$\begin{array}{ccc} \frac{I}{I^2}\times\frac{I^{k-1}}{I^k} & \longrightarrow & H_1(\frac{I^{k-1}}{I^k}) \\ (\sum_{s\in G} a_s(s-1), a) & \mapsto & \Theta\in Z_1(\frac{I^{k-1}}{I^k}),\ \Theta(s)=a_s a. \ \square \end{array}$$

Il vient alors en termes de caractères

$$\chi\left[H_1(\frac{I^{k-1}}{I^k})\right]=\chi\left[\frac{I}{I^2}\right]\cdot\chi\left[\frac{I^{k-1}}{I^k}\right],\quad \forall k\geq 2.$$

Il est difficile d'évaluer $\chi\left[\frac{I^{k-1}}{I^k}\right]$, en effet cela nécessite la connaissance de l'action de Δ sur G, i.e la connaissance de G ! Par contre, on peut remarquer que $\left(\frac{I}{I^2}\right)^{\otimes k}$ se surjecte vers $\frac{I}{I^2}\otimes\frac{I^{k-1}}{I^k}$, $k\geq 2$. Ainsi, il vient

$$\chi\left[\frac{I}{I^2}\right]\cdot\chi\left[\frac{I^{k-1}}{I^k}\right]\leq\chi^k\left[\frac{I}{I^2}\right],\quad \forall k\geq 2.$$

On peut noter que pour k égal à 2, il n'y a aucune perte d'information dans l'inégalité précédente.
En notant finalement que $\frac{I}{I^2}$ est Δ-isomorphe à $\frac{G^{ab}}{(G^{ab})^p}$ (cf. [Se2], chapitre VII), nous obtenons alors la première majoration de $\chi[R_k(G)]$:

$$\chi[R_k(G)]\leq\chi^k\left[\frac{G^{ab}}{(G^{ab})^p}\right]-\chi\left[\frac{I^{*k}}{I^{*k+1}}\right].$$

3.2. Seconde majoration de $\chi[R_k(G)]$.

Tout d'abord notons que

$$\chi[R_k(G)]\leq\chi[H_1(I)].$$

Partons ensuite de

$$1\longrightarrow\mathbb{Z}\xrightarrow{p}\mathbb{Z}\longrightarrow\mathbb{F}_p\longrightarrow 1,$$

pour en déduire

$$\cdots\longrightarrow H_2(\mathbb{Z})\xrightarrow{p}H_2(\mathbb{Z})\longrightarrow H_2(\mathbb{F}_p)\longrightarrow H_1(\mathbb{Z})\xrightarrow{p}H_1(\mathbb{Z})\longrightarrow\cdots,$$

plus précisémment

$$1 \longrightarrow \frac{H_2(\mathbb{Z})}{p.H_2(\mathbb{Z})} \longrightarrow H_2(\mathbb{F}_p) \longrightarrow H_1(\mathbb{Z})[p] \longrightarrow 1.$$

Or on sait que $H_2(\mathbb{Z})$ s'identifie au quotient $E_k/N_{L/k}E_L$ (cf. Rappels), et que $H_1(\mathbb{Z})$ est isomorphe à G^{ab} (cf. [Se2], chapitre VII). Ainsi, il vient la suite exacte

Proposition 3.3 :

$$1 \longrightarrow \frac{E_k}{(E_k)^p \,.N_{L/k}E_L} \longrightarrow H_2(\mathbb{F}_p) \longrightarrow G^{ab}[p] \longrightarrow 1.$$

On sait ensuite que $H_1(I)$ s'identifie à $H_2(\mathbb{F}_p)$, ceci par la suite exacte

$$1 \longrightarrow I \longrightarrow \mathbb{F}_p[G] \longrightarrow \mathbb{F}_p \longrightarrow 1.$$

Ainsi, on obtient

$$\chi\left[R_k(G)\right] \leq \chi\left[H_1(I)\right] = \chi\left[H_2(\mathbb{F}_p)\right] \leq \chi\left[G^{ab}[p]\right] + \chi\left[\frac{E_k}{(E_k)^p}\right].$$

Finalement, pour obtenir la seconde majoration de $\chi\left[R_k(G)\right]$, il suffit de montrer le lemme suivant :

Lemme 3.4 :

$$\chi\left[\frac{G^{ab}}{(G^{ab})^p}\right] = \chi\left[G^{ab}[p]\right].$$

Démonstration :
Supposons que $G^{ab} = \langle h_1^* \rangle \times \cdots \langle h_d^* \rangle$, avec h_i^* d'ordre égal à p^{o_i} ($d = d_pG$).
Il est immédiat que $\{h_1^*, \cdots, h_d^* \ mod (G^{ab})^p\}$ forme une $\mathbb{F}_p$-base de $\dfrac{G^{ab}}{(G^{ab})^p}$.
De même, $\{(h_1^*)^{p^{o_1-1}}, \cdots, (h_d^*)^{p^{o_d-1}}\}$ forme une $\mathbb{F}_p$-base de $G^{ab}[p]$.
Il suffit ensuite de remarquer que si pour $s \in \Delta$, $h_i^{*s} = h_i^{*a_i(s)} \cdots$, où $a_i(s) \in \mathbb{Z}$, alors $\left((h_i^*)^{p^{o_i-1}}\right)^s = (h_i^*)^{(p^{o_i-1})a_i(s)} \ldots$. □

Remarque 3.5 :
La proposition 3.3 apporte l'inégalité

$$r - d \leq d_pE_k,$$

où $r = d_pH_2(\mathbb{F}_p)$ et où $d = d_pG$.

3.3. Calcul de $\chi\left[\dfrac{I^{*2}}{I^{*3}}\right]$.

Dans ce paragraphe, on donne un résultat qui permet d'obtenir le caractère de $\dfrac{I^{*2}}{I^{*3}}$ à partir de $\chi\left[\dfrac{G^{ab}}{(G^{ab})^p}\right]$.

Théorème 3.8 : ([M], chapitre III, proposition 3.4.2)
Soit p un nombre premier différent de 2.
Si $\sum_{i=1}^{d} \psi_i$ désigne la décomposition en caractères $\mathbb{C}_p[\Delta]$-irréductibles de $\chi\left[\frac{G^{ab}}{(G^{ab})^p}\right]$ (on peut retrouver plusieurs fois le même caractère), alors on a

$$\chi\left[\frac{I^{*2}}{I^{*3}}\right] = \sum_{i=1}^{d} \sum_{\substack{j=1 \\ j \geq i}}^{d} \psi_i \psi_j.$$

Il est intéressant de rappeler également une $\mathbb{F}_p$-base de $\frac{I^{*2}}{I^{*3}}$: pour cela supposons que $\frac{G^{ab}}{(G^{ab})^p}$ est engendré par $h_1^*, \ldots, h_d^*$ *mod* $(G^{ab})^p$ en tant que $\mathbb{F}_p$-espace vectoriel ($h_i^* \in G^{ab}$) ; la famille $(h_i^*)_i$ forme un système minimal de générateurs de G^{ab}. Notons par X_i l'élément $h_i^* - 1$.
On a alors le résultat suivant (cf. [M], chapitre III, proposition 3.4.1) :

Proposition 3.9 :
La sous famille de $(X_iX_j)_{i \leq j}$ modulo $(X_kX_mX_n)_{k,m,n}$, composée uniquement d'éléments non nuls, forme une $\mathbb{F}_p$-base de $\frac{I^{*2}}{I^{*3}}$.

Remarque 3.10 :
Pour $p \neq 2$, tout élément de $\frac{I^{*2}}{I^{*3}}$ s'écrit de manière unique

$$\sum_{i \leq j} a_{i,j}(h_i^* - 1)(h_j^* - 1) \text{ modulo } I^{*3},$$

$a_{i,j} \in \mathbb{F}_p$; en particulier, le p-rang de $\frac{I^{*2}}{I^{*3}}$ est égal à $d + d.\frac{d-1}{2}$, d désignant le p-rang de G.
Pour $p = 2$, tout dépend de la structure de G ; en effet, on peut par exemple avoir $h_i^{*2} = 1$ et ainsi le terme $(h_i^* - 1)^2$ disparait. Plus précisémment, si $G^{ab} \simeq (\mathbb{Z}/2\mathbb{Z})^{d_2} \times G'$, avec G' d'exposant supérieur ou égal à 4, alors le 2-rang de $\frac{I^{*2}}{I^{*3}}$ est égal à

$$d + d.\frac{d-1}{2} - d_2.$$

Exemple élémentaire 3.11 :
On prend Δ cyclique d'ordre 3 et $p = 2$; on a trois caractères $\mathbb{C}_p[\Delta]$-irréductibles :

$$\begin{aligned} \psi_0 &: s \longrightarrow 1, \\ \psi_1 &: s \longrightarrow \zeta, \\ \psi_2 &: s \longrightarrow \zeta^2, \end{aligned}$$

où ζ est une racine cubique de l'unité (non triviale), et où $\Delta = \langle s \rangle$.
Supposons que G^{ab} ait pour structure $C_2 \times C_2 \times C_2 \times C_2$, avec l'action de Δ définie par :

$$\chi\left[\frac{G^{ab}}{(G^{ab})^2}\right] = 2\psi_1 + 2\psi_2 \ ;$$

alors avec le théorème 3.8, on a

$$\chi\left[\frac{I^{*2}}{I^{*3}}\right] = \psi_1 + \psi_2 + 4\psi_0.$$

§4. Exemples d'annulation de $r_2(G)$.

4.1. Cas quadratique.

On se fixe le cadre suivant :
p est un nombre premier différent de 2 et k un corps quadratique. On note par Δ le groupe de Galois de $k/\mathbb{Q}$. On suppose que la p-tour de Hilbert L de k est finie et on note par G le groupe de Galois de L/k.
On a deux caractères $\mathbb{C}_p[\Delta]$-irréductibles :

$$\begin{aligned} \psi_0 &: s \longrightarrow 1, \\ \psi_1 &: s \longrightarrow -1, \end{aligned}$$

où $\Delta = \langle s \rangle$.
Il est clair que

$$\chi\left[\frac{E_k}{(E_k)^p}\right] \leq \psi_1 ;$$

de même, on peut remarquer que

$$\chi\left[\frac{cl_k}{(cl_k)^p}\right] = d.\psi_1 ,$$

où $d = d_p cl_k$.
Par le théorème 3.1, il vient

$$\begin{aligned} &(i) \quad \chi[R_2(G)] \leq \frac{d(d-1)}{2}\psi_0, \\ &(ii) \quad \chi[R_2(G)] \leq (d+1)\psi_1. \end{aligned}$$

Ainsi $\chi[R_2(G)] = 0$, et par conséquent $r_2(G) = 0$; alors l'inégalité

$$\sum_{k\geq 2} r_k(G)t^k - dt + 1 > 0$$

devient

$$\sum_{k\geq 3} r_k(G)t^k - dt + 1 > 0.$$

Rappelons que

$$r - d \leq 1, \quad \text{remarque 3.5.}$$

Ainsi, si k admet une p-tour de Hilbert finie, on a avec (1)

$$t^3(d+1) - dt + 1 > 0, \quad \forall t \in]0;1[,$$

i.e

$$d_p cl_k \leq 2.$$

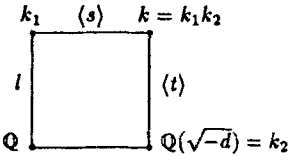
On a alors le résultat suivant établi par Schoof :

Proposition 4.1 ([Sc], théorème 4.3) :
Soit k un corps quadratique et soit p un nombre premier différent de 2 ; alors si $d_p cl_k \geq 3$, k a une p-tour de Hilbert infinie.

Remarque 4.2 :
De manière identique, on a le résultat suivant :
Soient p un nombre premier différent de 2 et $\underline{k}$ un corps quadratique imaginaire différent de $\mathbb{Q}(\sqrt{-3})$ tels que $cl_{\underline{k}}(p) = 1$. Alors toute extension quadratique k de $\underline{k}$ dont le p-rang du groupe des classes est supérieur ou égal à 3, a une p-tour de Hilbert infinie.

4.2. Autres exemples.

On considère la situation suivante :



où $k_1/\mathbb{Q}$ est une extension cyclique de degré l, l non nécessairement premier, et $d > 0$ sans facteur carré ; on suppose de plus que k_1 est totalement réel.
Soit p un nombre premier, p ne divisant pas $2l$. Notons par Δ le groupe de Galois de $k/\mathbb{Q}$; Δ est le produit direct de $\langle s \rangle$ avec $\langle t \rangle$, où $\langle s \rangle$ est le groupe de Galois de k/k_1 et $\langle t \rangle$ celui de k/k_2 ; G désignera le groupe de Galois de L/k, L étant la p-tour de Hilbert de k.
Nous avons $2l$ caractères $\mathbb{C}_p[\Delta]$-irréductibles : soit ζ une racine primitive l^{eme} de l'unité, alors les caractères $\mathbb{C}_p[\Delta]$-irréductibles sont définis par

$$\begin{aligned}
\psi_0 &: s \longrightarrow 1 \ ; \ t \longrightarrow 1 \\
\psi_1 &: s \longrightarrow 1 \ ; \ t \longrightarrow \zeta \\
&\dots \qquad \dots \\
\psi_{l-1} &: s \longrightarrow 1 \ ; \ t \longrightarrow \zeta^{l-1} \\
\psi_l &: s \longrightarrow -1 \ ; \ t \longrightarrow 1 \\
\psi_{l+i} &= \psi_l \psi_i \quad i = 1, \dots, l-1.
\end{aligned}$$

On peut remarquer que pour $0 \leq i \leq l-1$, $\psi_{l-i} = \psi_i^{-1}$, $\psi_{2l-i} = (\psi_{l+i})^{-1}$, puis que les caractères $(\psi_i)_{i \leq l-1}$ peuvent-être vus comme caractères du groupe $Gal(k_1/\mathbb{Q})$, et ψ_l comme caractère de $Gal(k_2/\mathbb{Q})$.
Supposons que k ne contient pas les racines p^{emes} de l'unité, alors il vient

$$\chi\left[\frac{E_k}{(E_k)^p}\right] = \sum_{j=1}^{l-1} \psi_j.$$

Supposons également que le caractère de $\dfrac{cl_k}{(cl_k)^p}$ est de la forme $a\psi_l + \psi_i + \psi_{l-i}$, i compris entre 1 et $l-1$ (ici, $d_p cl_k = d = a+2$), alors

$$\chi^2\left[\frac{cl_k}{(cl_k)^p}\right] - \chi\left[\frac{I^{*2}}{I^{*3}}\right] = (a^2/2 - a/2 + 1)\psi_0 + a\psi_{l+i} + a\psi_{2l-i}.$$

En appliquant le théorème 3.1, on obtient

$$(i) \quad \chi[R_2(G)] \leq (a^2/2 - a/2 + 1)\psi_0 + a\psi_{l+i} + a\psi_{2l-i},$$

$$(ii) \quad \chi[R_2(G)] \leq \left(\sum_{1 \leq j \leq l-1} \psi_j\right) + a\psi_l + \psi_i + \psi_{l-i}\ .$$

Ainsi $r_2(G) = 0$. Alors si k admet une p-tour finie L, on a

$$rt^3 - dt + 1 > 0, \quad \forall t \in]0;1[.$$

Il suffit ensuite de remarquer $r - d$ est inférieur ou égal à $l-1$, pour obtenir la proposition suivante :

Proposition 4.3 :
Sous les hypothèse de ce paragraphe (en particulier k ne contient pas μ_p), si k a une p-tour de Hilbert finie, on a alors

$$d_p cl_k < \frac{(l-1)t^3 + 1}{t - t^3}, \quad \forall t \in]0;1[.$$

Par la proposition 4.1, seuls les cas où $a \leq 2$ sont intéressants: pour $a = 0$, l'inégalité n'apporte rien ; pour $a = 1$, l'inégalité de la proposition 4.3 est fausse sur $]0;1[$ pour $l \leq 2$, on retrouve ainsi la remarque 4.2 ; pour $a = 2$ ($d_p cl_k = 4$), on note que si $l \leq 6$, alors l'inégalité est fausse sur $]0;1[$; on peut alors regrouper l'ensemble des résultats dans un tableau.
La première colonne A indique la valeur de l ; la colonne B indique pour comparaison la limite de l'inégalité

$$d \geq \frac{(l-1)t^2+1}{t-t^2},$$

i.e le cas où $r_2(G)$ est non annulé ; la colonne C donne les conditions sur p ; enfin, la colonne D donne les conditions d'infinitude de G pour le caractère χ de $\frac{cl_k}{(cl_k)^p}$.

A	B	C	D
l=2	5	$p \neq 2$	$d_p cl_k = d_p cl_{k_1} + d_p cl_{k_2} \geq 3$
l=3	6	$p \neq 2,3$	$d_p cl_k = 4$ avec $\chi = 2\psi_3 + \psi_1 + \psi_2$
l=4	6	$p \neq 2$	$d_p cl_k = 4$ avec $\chi = 2\psi_4 + \psi_1 + \psi_3$ ou $2\psi_4 + 2\psi_2$
l=5	7	$p \neq 2,5$	$d_p cl_k = 4$ avec $\chi = 2\psi_5 + \psi_1 + \psi_4$ ou $2\psi_5 + \psi_2 + \psi_3$
l=6	8	$p \neq 2,3$	$d_p cl_k = 4$ avec $\chi = 2\psi_6 + \psi_2 + \psi_4$ ou $2\psi_6 + 2\psi_3$ ou $2\psi_6 + \psi_1 + \psi_5$

En fait, dans certains cas les conditions sur χ peuvent-être remplacées par des conditions sur le groupe des classes des corps k_1 et k_2.
On obtient alors le résultat suivant :

Théorème 4.4 :
Soit p un nombre premier différent de 2.
Soit $k_1/\mathbf{Q}$ une extension cyclique de degré l totalement réelle, et soit k_2 un corps quadratique imaginaire ; $k = k_1 k_2$.
Supposons que k ne contient pas les racines p^{emes} de l'unité, et que

$$d_p cl_k = 2 d_p cl_{k_1} = 2 d_p cl_{k_2} = 4.$$

Alors dans une des situations suivantes, k a une p-tour de Hilbert infinie.

i) $l = 3$ *et* $p \equiv 2$ (3).

ii) $l = 4$ *et* $p \equiv 3$ (4).

iii) $l = 5$ *et* $p \equiv -1$ (5).

iv) $l = 6$ *et* $p \equiv -1$ (6).

§5. Cas cycliques de degré 3 et 6 sur Q.

Dans cette partie, $k/\mathbb{Q}$ est une extension cubique cyclique (§5.1), ou bien cyclique de degré 6 et totalement imaginaire (§5.2). Notons par L la p-tour de Hilbert de k ; $G = Gal(L/k)$. En utilisant le théorème de Golod-Safarevic, on sait que dès que $d_p cl_k = d \geq 6$, alors k a une p-tour de Hilbert infinie. Notons ensuite que si $r_2(G) = 0$, le rafinement de Schoof permet de dire que la p-tour est infinie dès que $d \geq 4$ (on ne montrera pas que $r_2(G) = 0$). On va donc s'interesser aux situations $d = 4$ et $d = 5$. Les théorèmes principaux 5.2 et 5.5 sont les conséquences de la proposition suivante :

Proposition 5.1 :
Soit le polynôme

$$Q_{r_2,d}(t) = (d + 2 - r_2(G))t^3 + r_2(G)t^2 - dt + 1.$$

Alors $Q_{r_2,d}$ prend des valeurs négatives sur l'intervalle $]0;1[$, lorsque $d = 4$ et $r_2(G) \leq 2$, ainsi que lorsque $d = 5$ et $r_2(G) \leq 5$.

Notons que pour $d = 4$ et $r_2(G) = 2$, le minimum sur $]0;1[$ de $Q_{4,2}(t) = 4t^3 + 2t^2 - 4t + 1$ est atteint en $t_0 = \dfrac{-1+\sqrt{13}}{6}$ et vaut $\dfrac{46-13\sqrt{13}}{27} \simeq -0.032$.
Pour $d = 5$ et $r_2(G) = 5$, le minimum sur $]0;1[$ de $Q_{5,5}(t) = 2t^3 + 5t^2 - 5t + 1$ est atteint en $t_1 = \dfrac{-5+\sqrt{55}}{6}$ et vaut $\dfrac{404-55\sqrt{55}}{54} \simeq -0.072$.

5.1. Cas cubique.

On considère la situation suivante : $k/\mathbb{Q}$ désigne une extension cyclique de degré 3, avec k donc totalement réel ; Δ est le groupe de Galois de $k/\mathbb{Q}$.
Soit p un nombre premier différent de 2 et de 3 ; il y a trois caractères $\mathbb{C}_p[\Delta]$-irréductibles :

$$\begin{aligned} \psi_0 &: s \longrightarrow 1, \\ \psi_1 &: s \longrightarrow \zeta, \\ \psi_2 &: s \longrightarrow \zeta^2, \end{aligned}$$

où $\Delta = \langle s \rangle$, et où ζ est une racine cubique de l'unité (non triviale).
On rappelle alors que

$$\chi\left[\frac{E_k}{(E_k)^p}\right] = \psi_1 + \psi_2.$$

On a alors le résultat principal de ce paragraphe.

Théorème 5.2 :
Soit $k/\mathbb{Q}$ une extension cyclique de degré 3, et soit p un nombre premier différent de 2 et de 3.
Alors si $d_p cl_k \geq 4$, k a une p-tour de Hilbert infinie.

Rappelons que si G est fini, alors avec la remarque 3.5 ($r - d \leq 2$) et l'inégalité (1) de Schoof, on sait que le polynôme $Q_{r_2,d}$ doit être strictement positif sur $]0;1[$.
Ainsi, à partir de la proposition 5.1, pour démontrer le théorème 5.2, il suffit de montrer

Proposition 5.3 :
Soit p un nombre premier différent de 2 et de 3, et soit $k/\mathbb{Q}$ une extension cyclique de degré 3 telle que la p-tour de Hilbert L de k est finie ; $G = Gal(L/k)$.
Alors si $d_p cl_k = 4$, on a $r_2(G) \leq 2$; si $d_p cl_k = 5$, on a $r_2(G) \leq 4$.

Démonstration :
On montre cette proposition en utilisant le théorème 3.1. Détaillons les calculs.

1^{er} cas : $d_p cl_k = 4$.
Le caractère du p-groupe des classes de k peut se décomposer de trois façons différentes.
• $\chi\left[\frac{cl_k}{(cl_k)^p}\right] = 2\psi_1 + 2\psi_2$.
On a alors

$$\chi\left[\frac{I^{*2}}{I^{*3}}\right] = 3\psi_1 + 3\psi_2 + 4\psi_0.$$

En appliquant le théorème 3.1, on obtient

$$(i) \quad \chi[R_2(G)] \leq \psi_1 + \psi_2 + 4\psi_0$$
$$(ii) \quad \chi[R_2(G)] \leq 3\psi_1 + 3\psi_2.$$

Ainsi $r_2(G) \leq 2$.
• $\chi\left[\frac{cl_k}{(cl_k)^p}\right] = 3\psi_1 + \psi_2$. (idem pour $3\psi_2 + \psi_1$)
On a

$$\chi\left[\frac{I^{*2}}{I^{*3}}\right] = \psi_1 + 6\psi_2 + 3\psi_0 ,$$

i.e

$$(i) \quad \chi[R_2(G)] \leq 3\psi_0 + 3\psi_2,$$
$$(ii) \quad \chi[R_2(G)] \leq 4\psi_1 + 2\psi_2 ;$$

ainsi $r_2(G) \leq 2$.
• $\chi\left[\frac{cl_k}{(cl_k)^p}\right] = 4\psi_2$. (idem pour $4\psi_1$)
On a

$$\chi\left[\frac{I^{*2}}{I^{*3}}\right] = 10\psi_1 ,$$

i.e

$$(i) \quad \chi[R_2(G)] \leq 6\psi_1,$$
$$(ii) \quad \chi[R_2(G)] \leq \psi_1 + 5\psi_2 ;$$

ainsi $r_2(G) \leq 1$.

2^{eme} cas : $d_p cl_k = 5$.
• $\chi\left[\frac{cl_k}{(cl_k)^p}\right] = 5\psi_1$. (idem pour $5\psi_2$)
alors

$$(i) \quad \chi[R_2(G)] \leq 10\psi_2,$$
$$(ii) \quad \chi[R_2(G)] \leq 6\psi_1 + \psi_2 ;$$

ainsi $r_2(G) \leq 1$.
• $\chi\left[\frac{cl_k}{(cl_k)^p}\right] = 4\psi_1 + \psi_2$. (idem pour $\psi_1 + 4\psi_2$)
alors

$$(i) \quad \chi[R_2(G)] \leq 6\psi_2 + 4\psi_0,$$
$$(ii) \quad \chi[R_2(G)] \leq 5\psi_1 + 2\psi_2 ;$$

ainsi $r_2(G) \leq 2$.
• $\chi\left[\frac{cl_k}{(cl_k)^p}\right] = 3\psi_1 + 2\psi_2$. (idem pour $2\psi_1 + 3\psi_2$)
alors

$$(i) \quad \chi[R_2(G)] \leq 3\psi_2 + \psi_1 + 6\psi_0,$$
$$(ii) \quad \chi[R_2(G)] \leq 4\psi_1 + 3\psi_2 ;$$

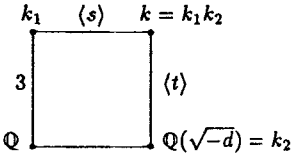
ainsi $r_2(G) \leq 4$. □

De façon identique, on a

Corollaire 5.4 :
Soit p un nombre premier différent de 2 et de 3, et soit $\underline{k}$ un corps quadratique imaginaire de p-groupe des classes trivial.
Soit $k/\underline{k}$ une extension cyclique de degré 3 ; alors si $d_p cl_k \geq 4$, k a une p-tour de Hilbert infinie.

5.2. Cas cyclique de degré 6 sur $\mathbb{Q}$.

Dans ce paragraphe, on considère $k/\mathbb{Q}$ une extension cyclique de degré 6 et totalement imaginaire.
On a alors la situation suivante :



où $k_1/\mathbb{Q}$ est une extension cubique cyclique, et où k_2 est un corps quadratique imaginaire.
Notons par Δ le groupe de Galois de $k/\mathbb{Q}$; Δ est le produit direct de $\langle s \rangle$ avec $\langle t \rangle$, où $\langle s \rangle$ est le groupe de Galois de k/k_1 et $\langle t \rangle$ celui de k/k_2.
Soit p un nombre premier différent de 2 et de 3 ; notons alors par L la p-tour de Hilbert de k et par $G = Gal(L/k)$.
Soit ζ une racine cubique non triviale de l'unité ; nous avons alors 6 caractères $\mathbb{C}_p[\Delta]$-irréductibles :

$$\begin{array}{lcl} \psi_0 & : & s \mapsto 1 \ ; \ t \mapsto 1 \\ \psi_1 & : & s \mapsto 1 \ ; \ t \mapsto \zeta \\ \psi_2 & = & \psi_1^2 \\ \psi_3 & : & s \mapsto -1 \ ; \ t \mapsto 1 \\ \psi_4 & = & \psi_3\psi_1 \\ \psi_5 & = & \psi_3\psi_2 \end{array}$$

Notons que le caractère des unités de k est égal à $\psi_1 + \psi_2$.
On peut alors dresser deux tables des situations que l'on rencontre en terme de caractères lorsque $d = 4$ et lorsque $d = 5$ ($d = d_p cl_k$), en indiquant la borne de $r_2(G)$ obtenue avec le théorème 3.1.

$\underline{d = 4}$

Caractère de cl_k	$r_2(G) \leq$	Caractère de cl_k	$r_2(G) \leq$
$\psi_3 + 3\psi_4$	2	$\psi_3 + 3\psi_1$	1
$\psi_3 + 2\psi_4 + \psi_5$	2	$\psi_3 + 2\psi_1 + \psi_2$	1
$\psi_3 + \psi_1 + 2\psi_4$	4	$2\psi_3 + 2\psi_4$	2
$\psi_3 + \psi_1 + \psi_4 + \psi_5$	5	$2\psi_3 + \psi_4 + \psi_5$	2
$\psi_3 + \psi_1 + 2\psi_5$	3	$2\psi_3 + \psi_1 + \psi_4$	3
$\psi_3 + 2\psi_1 + \psi_4$	3	$2\psi_3 + \psi_1 + \psi_5$	2
$\psi_3 + 2\psi_1 + \psi_5$	2	$2\psi_3 + 2\psi_1$	1
$\psi_3 + \psi_1 + \psi_2 + \psi_4$	3	$2\psi_3 + \psi_1 + \psi_2$	0

$\underline{d = 5}$

Caractère de cl_k	$r_2(G) \leq$	Caractère de cl_k	$r_2(G) \leq$
$\psi_3 + 3\psi_1 + \psi_4$	3	$\psi_3 + 4\psi_4$	2
$\psi_3 + 3\psi_1 + \psi_5$	2	$\psi_3 + 3\psi_4 + \psi_5$	2
$\psi_3 + 2\psi_1 + \psi_2 + \psi_5$	4	$\psi_3 + 2\psi_4 + 2\psi_5$	2
$\psi_3 + 2\psi_1 + \psi_2 + \psi_4$	4	$2\psi_3 + 3\psi_1$	1
$\psi_3 + 2\psi_1 + 2\psi_4$	5	$2\psi_3 + 2\psi_1 + \psi_2$	1
$\psi_3 + 2\psi_1 + \psi_4 + \psi_5$	5	$2\psi_3 + 2\psi_1 + \psi_4$	4
$\psi_3 + 2\psi_1 + 2\psi_5$	3	$2\psi_3 + 2\psi_1 + \psi_5$	3
$\psi_3 + \psi_1 + \psi_2 + 2\psi_4$	4	$2\psi_3 + \psi_1 + \psi_2 + \psi_4$	4
$\psi_3 + \psi_1 + \psi_2 + \psi_4 + \psi_5$	5	$2\psi_3 + \psi_1 + 2\psi_4$	5
$\psi_3 + \psi_1 + 3\psi_4$	4	$2\psi_3 + \psi_1 + \psi_4 + \psi_5$	6
$\psi_3 + \psi_1 + 2\psi_4 + \psi_5$	6	$2\psi_3 + \psi_1 + 2\psi_5$	2
$\psi_3 + \psi_1 + \psi_4 + 2\psi_5$	5	$2\psi_3 + 3\psi_4$	2
$\psi_3 + \psi_1 + 3\psi_5$	3	$2\psi_3 + 2\psi_4 + \psi_5$	2

Ces tables ont été réalisées après avoir noté les points suivants :

(i) Si $d_p cl_{k_2} \geq 3$, la p-tour de k_2 est infinie (proposition 4.1), par conséquent il en est de même pour celle de k,

(ii) Si $d_p cl_{k_1} \geq 4$, la p-tour de k_1 est infinie (théorème 5.2), par conséquent il en est de même pour celle de k,

(iii) Le cas où ψ_3 n'intervient pas dans la décomposition du caractère χ du groupe des classes de k est parfaitement connu (corollaire 5.4),

(iv) L'existence de symétries pour les caractères.

Certaines combinaisons de caractères sont alors inutiles : en particulier $\chi = 3\psi_3 + \cdots$ (point (i)), $\chi = 2\psi_1 + 2\psi_2 + \cdots$ (point (ii)), ou bien regarder $\chi = \psi_3 + \psi_2 + 2\psi_5$ revient à regarder $\chi = \psi_3 + \psi_1 + 2\psi_4$ (point (iv)), où ici χ est le caractère du p-groupe des classes de k.
On obtient alors le résultat suivant :

Théorème 5.5 : *Soit p un nombre premier différent de 2 et de 3.*
Soit $k/\mathbb{Q}$ une extension cyclique de degré 6 et totalement imaginaire; k_1 est la sous-extension de k cubique cyclique sur $\mathbb{Q}$; k_2 est le sous-corps quadratique de k.
Posons $d = d_p cl_k$, $d_1 = d_p cl_{k_1}$ et $d_2 = d_p cl_{k_2}$.
Alors, sous une des conditions suivantes, k a une p-tour de Hilbert infinie.

i) $p \equiv 2(3)$ *et* $d \geq 4$.

ii) $d_1 = 0$ *et* $d \geq 4$ *(corollaire 5.4).*

iii) $d_2 = 0$ *et* $d \geq 4$.

iv) $d_1 + d_2 \geq 4$.

v) $d_1 \geq 3$ *et* $d \geq 4$.

Démonstration :
Lorsque l'on observe les tables précédentes, on note au total 8 situations pouvant ne pas vérifier les hypothèses de la proposition 5.1 :

- $d = 4$ avec $\chi = \psi_3 + \psi_1 + 2\psi_4$
- $d = 4$ avec $\chi = \psi_3 + \psi_1 + \psi_4 + \psi_5$
- $d = 4$ avec $\chi = \psi_3 + \psi_1 + 2\psi_5$
- $d = 4$ avec $\chi = \psi_3 + 2\psi_1 + \psi_4$
- $d = 4$ avec $\chi = \psi_3 + \psi_1 + \psi_2 + \psi_4$
- $d = 4$ avec $\chi = \psi_3 + \psi_1 + \psi_4$
- $d = 5$ avec $\chi = \psi_3 + \psi_1 + 2\psi_4 + \psi_5$
- $d = 5$ avec $\chi = 2\psi_3 + \psi_1 + \psi_4 + \psi_5$

Il suffit ensuite de remarquer que ces cas n'entrent pas dans les situations du théorème 5.5. □

Exemple numérique 5.6 :
Prenons $k_1 = \mathbb{Q}\sqrt{-14606}$ et k_2 le corps cubique cyclique sur $\mathbb{Q}$, de conducteur $m = 18913$, définit par le polynôme $X^3 + X^2 - 6304X + 190531$; à partir des tables numériques de B. Oriat [O] et de M.-N. Gras [G], on note que $d_5 cl_{k_1} = d_5 cl_{k_2} = 2$.
Ainsi, dans ce cas le corps composé k a une 5-tour de Hilbert infinie (théorème 5.5, *iv*).

§6. Relation entre $a_2(G)$, $r_2(G)$ et d.

6.1. Relation.

On se fixe G un p-groupe fini ; I est l'idéal d'augmentation de $\mathbb{F}_p[G]$.
Partons de la suite exacte

$$0 \longrightarrow I^k \longrightarrow I^{k-1} \longrightarrow \frac{I^{k-1}}{I^k} \longrightarrow 0\ ,\quad k \geq 2,$$

qui devient

$$0 \longrightarrow \frac{H_1(I^{k-1})}{Im\,(H_1(I^k) \longrightarrow H_1(I^{k-1}))} \longrightarrow H_1(\frac{I^{k-1}}{I^k}) \longrightarrow \frac{I^k}{I^{k+1}} \longrightarrow 0\ ,\ \forall k \geq 2.$$

Pour $k = 2$, on obtient

$$0 \longrightarrow R_2(G) \longrightarrow H_1(\frac{I}{I^2}) \longrightarrow \frac{I^2}{I^3} \longrightarrow 0.$$

Ainsi, il vient

$$d_p H_1(\frac{I}{I^2}) = a_2(G) + r_2(G),$$

où $a_2(G) = d_p \frac{I^2}{I^3}$.
Comme G agit trivialement sur $\frac{I}{I^2}$, on a (lemme 3.2)

$$H_1(\frac{I}{I^2}) \simeq \frac{I}{I^2} \otimes \frac{I}{I^2},$$

et ainsi

$$d_p H_1(\frac{I}{I^2}) = d^2,$$

d étant le p-rang de G. On a ainsi obtenu :

Proposition 6.1 :
Soit G un p-groupe fini, alors on a

$$d^2 = a_2(G) + r_2(G).$$

On a alors immédiatement le théorème suivant :

Théorème 6.2 :
Soit p un nombre premier différent de 2, et soit G un p-groupe fini (non cyclique).
Supposons que $r_2(G) = 0$.
Notons par $h_1, \ldots, h_d$, d éléments générateurs de G ($d = d_pG$).
Alors, les relations entre les h_i, du type

$$h^p . \prod_{i<j} [h_i, h_j]^{\alpha_{i,j}} = 1,$$

où $h \in G$, $0 \leq \alpha_{i,j} < p$, avec au moins un élément $\alpha_{i,j}$ non nul, sont à exclure.

Démonstration :
Tout d'abord notons que pour tout s, t, $v \in G$, et $a \in \mathbb{Z}$, on a

$$(st - 1)(v - 1) \equiv (s - 1)(v - 1) + (t - 1)(v - 1) \ \ modulo\ I^3,$$

et

$$(s^a - 1)(t - 1) \equiv a(s - 1)(t - 1) \ \ modulo\ I^3.$$

Ainsi, $\dfrac{I^2}{I^3}$ va être engendré en tant que $\mathbb{F}_p$-espace vectoriel, par les éléments

$$(h_i - 1)(h_j - 1) \ modulo\ I^3,\ i = 1, \ldots, d,\ j = 1, \ldots, d.$$

Ces éléments sont au nombre de

$$d + A_d^2 = d^2 \ ;$$

d correspond au nombre d'éléments du type $(h_i - 1)^2$ et A_d^2 au nombre d'éléments du type $(h_i - 1)(h_j - 1)$, $i \neq j$ (attention, $(h_i - 1)(h_j - 1)$ peut-être différent de $(h_j - 1)(h_i - 1)$).
Ainsi, si $r_2(G) = 0$, alors $d_p \dfrac{I^2}{I^3} = d^2$; cela signifie donc que, modulo I^3, il n'y aucune relation entre les éléments $(h_i - 1)(h_j - 1)$.
Remarquons ensuite l'identité

$$[h_i, h_j]^{\alpha_{i,j}} - 1 \equiv \alpha_{i,j}\left((h_i - 1)(h_j - 1) - (h_j - 1)(h_i - 1)\right) \ modulo\ I^3. \tag{5}$$

Or, à partir de

$$h^p . \prod_{i<j} [h_i, h_j]^{\alpha_{i,j}} = 1,$$

on a

$$\sum_{i<j} \alpha_{i,j}\left((h_i - 1)(h_j - 1) - (h_j - 1)(h_i - 1)\right) \equiv 0 \ modulo\ I^3,$$

ainsi, si $r_2(G) = 0$, tous les éléments $\alpha_{i,j}$ doivent être nuls. □

Il en résulte alors le corollaire suivant :

Corollaire 6.3 :
Soit k un corps de nombres, et soit p un nombre premier différent de 2; notons par k_1 le p-corps de Hilbert de k, et par G le groupe de Galois de L/k, L étant la p-tour de Hilbert de k.
Si $r_2(G)$ est nul et si $d_p cl_k \geq 2$, alors le p-groupe des classes de k_1 est non trivial.

Démonstration :
Supposons que le p-groupe des classes de k_1 est trivial ; alors $L = k_1$ et $G = Gal(L/k) = cl_k$ est abélien.
Soient h_1 et h_2 deux éléments distincts d'un système de générateurs de G (ceux-ci existent car $d_p cl_k \geq 2$). Alors on a

$$[h_1, h_2] = 1,$$

ce qui s'oppose au théorème 6.2. □

Ce résultat s'applique aux corps quadratiques, car on sait dans ce cas, lorsque G est fini, que $r_2(G) = 0$ (cf. §4.1) ; on obtient ainsi

Corollaire 6.4 : Cas quadratique.
Soient p un nombre premier différent de 2, et k un corps quadratique ; k_1 désigne le p-corps de Hilbert de k.
Si $d_p cl_k$ est supérieur ou égal à 2, alors le p-groupe des classes de k_1 est non trivial.

De manière identique, on montre

Corollaire 6.5 :
Soit p un nombre premier différent de 2.
Soit $\underline{k}$ une extension quadratique imaginaire, différent de $\mathbb{Q}(\sqrt{-3})$, de p-groupe des classes trivial et soit k une extension quadratique sur $\underline{k}$; k_1 désigne le p-corps de Hilbert de k.
Si $d_p cl_k \geq 2$, alors le p-groupe des classes de k_1 est non trivial.

Remarque 6.6 :
Lorsque k est un corps quadratique imaginaire, Lemmermeyer ([L], 3.1) a montré que dès que le 2-rang du groupe des classes de k est supérieur ou égal à 3, le 2-groupe des classes de k_1 est non trivial (k_1 désignant le 2-corps de Hilbert de k). De plus, lorsque $cl_k = C_2 \times C_2$, il donne une bonne description des deux premiers étages de la 2-tour de Hilbert en fonction du discriminant de k ([L], Théorème 2).

6.2. Cas cubique.

Dans ce paragraphe, on va donner une version du corollaire 6.4 pour les extensions cubiques cycliques de $\mathbb{Q}$.

Corollaire 6.7 :
Soit $k/\mathbb{Q}$ une extension cubique cyclique, et soit p un nombre premier différent de 3. Notons par k_1 le p-corps de Hilbert de k.
Alors dans les trois situations suivantes, le p-groupe des classes de k_1 est non trivial.

i) p est différent de 2, et $d_p cl_k \geq 3$.

ii) p est congru à 2 modulo 3 ($p \neq 2$) et $d_p cl_k \geq 2$.

iii) $p = 2$, avec $d_2 cl_k \geq 4$.

Démonstration:
Supposons que le p-groupe des classes de k_1 est trivial (i.e que $k_1 = L$ est la p-tour de Hilbert de k). Notons par Δ le groupe de Galois de $k/\mathbb{Q}$, et par G celui de k_1/k; on rappelle l'existence de trois caractères $\mathbb{C}_p[\Delta]$-irréductibles ψ_0, ψ_1 et $\psi_2 = \psi_1^2$ (paragraphe 5.1).
On sait que $\chi\left[\dfrac{E_k}{(E_k)^p}\right] = \psi_1 + \psi_2$.

Cas où p est différent de 2:
i) Si le p-rang du groupe des classes de k est égal à 3, le caractère du p-groupe des classes de k peut se décomposer de deux façons:

- $\chi\left[\dfrac{cl_k}{(cl_k)^p}\right] = 3\psi_1$; dans ce cas, on note par le théorème 3.1 que $\chi[R_2(G)] \leq 4\psi_1 + \psi_2$, et que $\chi[R_2(G)] \leq 3\psi_2$, ainsi $r_2(G) \leq 1$.

Il est facile de noter ici que $a_2(G)$ vaut 6, ainsi $a_2(G) + r_2(G) < d^2$; par conséquent le p-groupe des classes de k_1 est non trivial.

- $\chi\left[\dfrac{cl_k}{(cl_k)^p}\right] = 2\psi_1 + \psi_2$; dans ce cas, on a:

$\chi[R_2(G)] \leq 3\psi_1 + 2\psi_2$ et $\chi[R_2(G)] \leq \psi_2 + 2\psi_0$, ainsi $r_2(G) \leq 1$.

Comme $a_2(G)$ vaut 6, la conclusion est donc identique à celle du point précédent.

ii) Si le p-rang du groupe des classes de k est égal à 2 avec p congru à 2 *modulo* 3, alors le caractère de $\dfrac{cl_k}{(cl_k)^p}$ est égal à $\psi_1 + \psi_2$.
De ceci, on a:
$\chi[R_2(G)] \leq 2\psi_1 + 2\psi_2$, et $\chi[R_2(G)] \leq \psi_0$; par conséquent, $r_2(G) = 0$ et l'égalié $a_2(G) + r_2(G) = d^2$ n'est pas vérifiée.

Cas $p = 2$:
Tout d'abord, supposons que $G = (C_2)^{d_2} \times G'$ avec G' d'exposant supérieur ou égal à 4.
Ensuite, en utilisant l'inégalité de Safarevic, on note que si le 2-rang du groupe des classes de k est supérieur ou égal à 6, alors la 2-tour de Hilbert de k est non finie.
Si le 2-rang du groupe des classes de k est égal à 4, alors le caractère de $\dfrac{cl_k}{(cl_k)^2}$ est égal à $2\psi_1 + 2\psi_2$.
Dans ce cas, on obtient en utilisant le théorème 3.1:
$\chi[R_2(G)] \leq 3\psi_1 + 3\psi_2 + \psi_0$ et $\chi[R_2(G)] \leq \psi_1 + \psi_2 + 4\psi_0 + \alpha\psi_1 + (d_2 - \alpha)\psi_2$, $\alpha = 0, 1,$ ou 2, $\alpha \leq d_2$.
Par conséquent, $r_2(G)$ est inférieur à $3 + d_2$.
On note de plus que $a_2(G)$ est égal à $10 - d_2$; ainsi $a_2(G) + r_2(G)$ est inférieur à 13. □

6.3. Conclusions.

Pour terminer, remarquons deux résultats intéressants.

6.3.1. Conclusion I.

Dans un premier point, nous allons interpréter la condition $r_2(G) = 0$ en terme de relations du groupe G.
Soient donc G un p-groupe fini et I est l'idéal d'augmentation de $\mathbb{F}_p[G]$.
Soit

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1,$$

une résolution minimale de G, et soit $\{x_1, \cdots, x_r\} \subset R$ un système de relations de G. Notons par I_F l'idéal d'augmentation de $\mathbb{F}_p[[F]]$. On rappelle le filtration de Zassenhaus $(F_n)_{n\geq 1}$ de F:

$$x \in F_n \Longleftrightarrow x - 1 \in {I_F}^n.$$

Posons alors:

$$r'_n = |\{x_i \in F_n, x_i \notin F_{n+1}\}|.$$

Théorème 6.8:

$$r_2(G) = 0 \Longrightarrow r'_2 = 0.$$

Démonstration:
Soit $\{h_1, \ldots, h_d\}$ un système minimal de générateurs de F ($d = d_pG$).
On sait alors que tout élément $x_k \in R$ peut s'écrire sous la forme

$$x_k = \prod_i {h_i}^{p.\alpha_i} . \prod_{i<j} [h_i, h_j]^{\alpha_{i,j}} . b, \tag{6}$$

où $b \in F_3$, $0 \leq \alpha_i < p$, et $0 \leq \alpha_{i,j} < p$ (cf. [K1], §7, proposition 7.23, page 71).
Notons que pour $p \geq 3$, ${h_i}^p - 1 \in F_3$.
Si l'on regarde alors $x_k - 1$ dans $\mathbb{F}_p[G]$, on obtient avec (5) (cf. démonstration du théorème 6.2) et (6)

- Pour $p \neq 2$: $\sum_{i,j} \alpha_{i,j} ((h_i - 1)(h_j - 1) - (h_j - 1)(h_i - 1)) \equiv 0\ (I^3)$,
- Pour $p = 2$: $\sum_i \alpha_i (h_i - 1)^2 + \sum_{i,j} \alpha_{i,j} ((h_i - 1)(h_j - 1) - (h_j - 1)(h_i - 1)) \equiv 0\ (I^3)$,

où ici, les éléments h_i sont vus comme éléments de G.
Si $r_2(G) = 0$, alors $a_2(G) = d^2$, cela signifie donc qu'il n'y a aucune relation entre les éléments $(h_i - 1)(h_j - 1)$ (cf. démonstration du théorème 6.2); ainsi $\alpha_{i,j} = 0$ et de plus, pour $p = 2$, $\alpha_i = 0$. □

6.3.2. Conclusion II.

Ici, G est encore un p-groupe fini; oublions la proposition 6.1.
On définit, pour $k \geq 1$, $a_k(G)$ par

$$a_k(G) = d_p(\frac{I^k}{I^{k+1}}).$$

Soit $P(t)$ le polynôme suivant construit à partir de G:

$$P(t) = 1 + dt + a_2(G)t^2 + a_3(G)t^3 + \cdots$$

Alors en fait, Schoof a montré le résultat suivant ([Sc]):
Parce que G est fini, on a

$$\sum_{k\geq 2} r_k(G)t^k - dt + 1 \geq \frac{1}{P(t)}, \quad \forall t \in]0;1[. \tag{7}$$

Au voisinage de 0, nous avons

$$\frac{1}{P(t)} = 1 - dt + t^2(d^2 - a_2(G)) + t^2\varepsilon(t).$$

Ainsi (7) devient au voisinage de 0

$$1 - dt + r_2(G)t^2 + t^2\varepsilon'(t) \geq 1 - dt + t^2\left(d^2 - a_2(G)\right) + t^2\varepsilon(t).$$

On voit que si $r_2(G)$ est nul, alors l'inégalité est contredite au voisinage de 0 dès que d^2 est strictement supérieur à $a_2(G)$; on retrouve alors la proposition 6.3.

Références

[G] M.-N. Gras, Méthodes et algorithmes pour le calcul du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$, J. reine angew. Math., 277 (1975), 89-116.

[K1] H. Koch, Galoissche Theorie der p-Erweiterungen, VEB Deutscher Verlag der Wissenschaften, Berlin, 1970.

[K2] H. Koch, Zum Satz von Golod-Schafarewitsch, Math. Nachr., 42 (1969), 321-333.

[L] F. Lemmermeyer, Construction of Hilbert Class Field II, preprint, 1994.

[M] C. Maire, Extensions T-ramifiées modérées, S-décomposées, Thèse, Faculté des Sciences de Besançon, 1995.

[O] B. Oriat, Groupes des classes d'idéaux des corps quadratiques imaginaires $\mathbb{Q}(\sqrt{d})$, $-24572 < d < 0$, Publ. Math. Fac. Sci. Besançon, Fascicule 2 (1988).

[R] P. Roquette, On class field towers, dans "J.-W.-S. Cassels et A. Fröhlich, Algebraic number theory", Academic Press London, 1967.

[Sc] R. Schoof, Infinite class field towers of quadratic fields, J. reine angew. Math., 372 (1986), 209-220.

[Se1] J.-P. Serre, Représentations linéaires des groupes finis, Hermann, Paris, 1967.

[Se2] J.-P. Serre, Corps locaux, Hermann, Paris, 1968.

[T] J.-T. Tate, Global class field theory, dans "J.-W.-S. Cassels et A. Fröhlich, Algebraic number theory", Academic Press London, 1967.

[V] E.B. Vinberg, On the dimension theorem of associative algebras, Izv. Ak. Nauk. SSSR, 29 (1965), 209-214 (russian).

Christian Maire
Laboratoire de Mathématiques
URA 741 au CNRS
Université de Besançon
16, route de Gray
F-25030 Besançon cedex