Rang de l'image du groupe des unités et polynômes lacunaires*

GABRIELE RANIERI (Caen, Pisa)

1 Introduction

Dans [Amo1] F. Amoroso a introduit la notion de corps proche d'un corps CM (en abrégé : PCM). Soit K un corps de nombres et soit Γ son groupe de $\mathbb{Q}$-automorphismes. Suivant [Amo1], nous dirons que K est un corps PCM s'il existe $\phi \in \mathbb{Z}[\Gamma]$ tel que :

$$\|\phi\|_1 R_\phi < [K : \mathbb{Q}].$$

Ici $\|\phi\|_1$ est la taille de ϕ (i.e. si $\phi = \sum_{\sigma\in\Gamma} \phi_\sigma \sigma$ alors $\|\phi\|_1 = \sum_{\sigma\in\Gamma} |\phi_\sigma|$), $R_\phi = \dim(\mathcal{L}(\mathrm{K}^{*\phi}) \otimes \mathbb{R})$, où $\mathcal{L}$ est le plongement logarithmique et

$$K^{*\phi} = \{\beta \in K^* \text{ t.q. } \exists \alpha \in \mathrm{K}^* \text{ t.q. } \beta = \alpha^\phi\}.$$

Remarquons que si K est un corps CM et j est la conjugaison complexe, alors $R_{1-j}\|1 - j\|_1 = 0$, en particulier tout corps CM est PCM. D'autres exemples remarquables de corps PCM sont donnés par $K = \mathbb{Q}(\alpha)$, où α est un nombre de Salem (voir [Amo2]).

Le problème de caractériser les corps PCM se pose ; nous donnons ici une réponse partielle, en montrant qu'une extension totalement rélle n'est jamais PCM (corollaire 1).

Soit maintenant k un entier positif et soient $d_1,\ldots, d_k \in \mathbb{N}^*$. Dans le cas particulier des extensions abéliennes totalement réelles, le problème de déterminer les éventuels corps PCM se traduit, *via* la correspondance entre caractères et racines de l'unités (voir appendice), dans l'existence de polynômes non nuls $P \in \mathbb{Z}[x_1, \ldots, x_k]$ de degrés partiels $\deg_{x_i}(P) < d_i$ pour tout $1 \leq i \leq k$, tels que :

$$\|P\|_1 R_{\mathbf{d},P} < d_1 \ldots d_k$$

Ici $\mathbf{d} = (d_1, \ldots, d_k)$, $\|P\|_1$ est la somme des modules des coefficients de P et

$$R_{\mathbf{d},P} = |\{\boldsymbol{\omega} \in \mu_{d_1} \times \cdots \times \mu_{d_k} \text{ t. q. } P(\boldsymbol{\omega}) \neq 0\}|$$

*2000 *Mathematics Subject classification* : AA 5221

(où μ_{d_i} est l'ensemble des racines d_i-ièmes de l'unité pour tout $1 \leq i \leq k$).

F. Amoroso avait conjecturé que pour tout $P \neq 0$ dans $\mathbb{Z}[x_1, \ldots, x_k]$, on a :

$$\|P\|_1 R_{\mathbf{d},P} \geq d_1 \cdots d_k.$$

A. Schinzel a ensuite remarqué (communication orale) que même dans le cas très particulier

$$P(x) = \frac{x^n - 1}{\phi_n(x)} \in \mathbb{Z}[x]$$

où n est un entier positif et ϕ_n est le n-ième polynôme cyclotomique (donc, en suivant les notations précédentes, dans ce cas $k = 1$ et $n = d_1$) cette conjecture n'était pas évidente.

Ici nous prouvons une version plus forte de la conjecture de F. Amoroso ; plus précisément (paragraphe 2) en utilisant des techniques élémentaires nous démontrons le :

Théorème 1. *Soit k un entier positif, soit $P \in \mathbb{C}[x_1, \ldots, x_k]$ un polynôme non nul tel que $\deg_{x_i}(P) < d_i$ pour tout $1 \leq i \leq k$ et soit Ω_P le nombre de coefficients $\neq 0$ de P. Alors on a :*

$$\Omega_P \geq \frac{d_1 \ldots d_k}{R_{\mathbf{d},P}}. \tag{1}$$

Il est clair que la conjecture de F. Amoroso découle de (1). En effet si $P \in \mathbb{Z}[x_1, \ldots, x_k]$ alors $||P||_1 \geq \Omega_P$ car tout coefficient de P non nul est de module $\geq$1.

Remarquons que la minoration (1) est optimale. En effet si l, m sont entiers positifs tels que l divise m et si on pose :

$$G(x) := 1 + x^l + x^{2l} + \ldots + x^{m-l} = \frac{x^m - 1}{x^l - 1},$$

on a $\deg(G) < m$, $\Omega_G = m/l$ et $R_{m,G} = l$; donc :

$$\Omega_G = \frac{m}{R_{m,G}}.$$

De même si v est un entier positif pair et si on pose :

$$H(x) = 1 - x^{v/2}$$

on a encore $\deg(H) < v$, $\Omega_H = 2$ et $R_{v,H} = v/2$, en particulier :

$$\Omega_H = \frac{v}{R_{v,H}}.$$

Dans le paragraphe 3 , nous généralisons la méthode du théorème 1 au cas de groupes non nécessairement commutatifs pour montrer :

Théorème 2. *Soit G un groupe fini et soit $\phi = \sum_{\sigma\in G}\phi_\sigma\sigma$ un élément non nul de $\mathbb{C}[G]$; notons Ω_ϕ le nombre des coefficients $\neq 0$ de ϕ et $\widetilde{R}_\phi$ le rang de l'application linéaire*

$$T_\phi\colon \mathbb{C}[G] \to \mathbb{C}[G]$$

qui envoie $\psi \in \mathbb{C}[G]$ sur $\psi\phi$. Alors on a :

$$\Omega_\phi \widetilde{R}_\phi \geq |G|.$$

Le théorème 2 permet de répondre en toute généralité à la question de l'existence de corps PCM réels :

Corollaire 1. *Tout corps totalement réel n'est pas PCM.*

Remerciements. Je tiens à remercier B. Anglès et B. Leclerc pour leur aide lors de la réalisation de cet article. Je tiens également à remercier P. Gillibert pour ses intéressantes remarques, et C. Pontreau qui a relu une version préliminaire de ce travail.

2 Preuve du théorème 1

Puisque $\deg_{x_i}(P) < d_i$, pour tout $1 \leq i \leq k$, nous avons :

$$P(\mathbf{x}) = \sum_{h_1=0}^{d_1-1}\cdots\sum_{h_k=0}^{d_k-1} P_{\mathbf{h}}\mathbf{x}^{\mathbf{h}} \in \mathbb{C}[x_1,\ldots,x_k]. \tag{2}$$

Montrons tout d'abord, pour tout $\mathbf{l} \in \mathbb{Z}^k$, l'égalité :

$$P_{\mathbf{l}} = \frac{1}{d}\sum_{\boldsymbol{\omega}\in\mu_{\mathbf{d}}} \overline{\boldsymbol{\omega}^{\mathbf{l}}} P(\boldsymbol{\omega}), \tag{3}$$

où on a posé $d := d_1\cdots d_k$ et $\mu_{\mathbf{d}} = \mu_{d_1}\times\cdots\times\mu_{d_k}$. D'après (2), pour tout $\boldsymbol{\omega} \in \mu_{\mathbf{d}}$, on a :

$$P(\boldsymbol{\omega}) = \sum_{h_1=0}^{d_1-1}\ldots\sum_{h_k=0}^{d_k-1} P_{\mathbf{h}}\boldsymbol{\omega}^{\mathbf{h}}.$$

Il vient :

$$\begin{aligned}
\frac{1}{d}\sum_{\boldsymbol{\omega}\in\mu_{\mathbf{d}}} \overline{\boldsymbol{\omega}^{\mathbf{l}}} P(\boldsymbol{\omega}) &= \frac{1}{d}\sum_{\boldsymbol{\omega}\in\mu_{\mathbf{d}}} \overline{\boldsymbol{\omega}^{\mathbf{l}}} \sum_{h_1=0}^{d_1-1}\cdots\sum_{h_k=0}^{d_k-1} P_{\mathbf{h}}\boldsymbol{\omega}^{\mathbf{h}} \\
&= \frac{1}{d}\sum_{\boldsymbol{\omega}\in\mu_{\mathbf{d}}} \sum_{h_1=0}^{d_1-1}\cdots\sum_{h_k=0}^{d_k-1} P_{\mathbf{h}}\boldsymbol{\omega}^{\mathbf{h}-\mathbf{l}} \\
&= \frac{1}{d}\sum_{h_1=0}^{d_1-1}\cdots\sum_{h_k=0}^{d_k-1}\sum_{\boldsymbol{\omega}\in\mu_{\mathbf{d}}} P_{\mathbf{h}}\boldsymbol{\omega}^{\mathbf{h}-\mathbf{l}}.
\end{aligned} \tag{4}$$

Soit maintenant $\mathbf{h} \in \mathbb{Z}^k$. Si $\mathbf{h} = \mathbf{l}$ on a $\boldsymbol{\omega}^{\mathbf{h}-\mathbf{l}} = 1$ et :

$$\frac{1}{d} \sum_{\boldsymbol{\omega} \in \mu_{\mathbf{d}}} P_{\mathbf{l}} \boldsymbol{\omega}^{\mathbf{l}-\mathbf{l}} = P_{\mathbf{l}}. \tag{5}$$

Par ailleurs si $\mathbf{h} - \mathbf{l} = \mathbf{m} \neq \mathbf{0}$ on a :

$$\frac{1}{d} \sum_{\boldsymbol{\omega} \in \mu_{\mathbf{d}}} P_{\mathbf{h}} \boldsymbol{\omega}^{\mathbf{m}} = 0. \tag{6}$$

Des relations (5) et (6) il vient :

$$\frac{1}{d} \sum_{h_1=0}^{d_1-1} \cdots \sum_{h_k=0}^{d_k-1} \sum_{\boldsymbol{\omega} \in \mu_{\mathbf{d}}} P_{\mathbf{h}} \boldsymbol{\omega}^{\mathbf{h}-\mathbf{l}} = P_{\mathbf{l}}$$

d'où l'égalité (3).

Choisissons maintenant $\mathbf{M} \in \mathbb{Z}^k$ tel que pour tout vecteur $\mathbf{h}$ on ait $|P_{\mathbf{M}}| \geq |P_{\mathbf{h}}|$. Par la relation (3) on a :

$$P_{\mathbf{M}} = \frac{1}{d} \sum_{\boldsymbol{\omega} \in \mu_{\mathbf{d}}} \overline{\boldsymbol{\omega}^{\mathbf{M}}} P(\boldsymbol{\omega}).$$

Donc :

$$|P_{\mathbf{M}}| \leq \frac{1}{d} \sum_{\boldsymbol{\omega} \in \mu_{\mathbf{d}}} |\overline{\boldsymbol{\omega}^{\mathbf{M}}} P(\boldsymbol{\omega})| = \frac{1}{d} \sum_{\boldsymbol{\omega} \in \mu_{\mathbf{d}}} |P(\boldsymbol{\omega})|. \tag{7}$$

En rappelant que, par définition, $R_{\mathbf{d},P}$ est le nombre de $\boldsymbol{\omega} \in \mu_{\mathbf{d}}$ tels que $P(\boldsymbol{\omega})$ est non nul et en observant que

$$|P(\boldsymbol{\omega})| \leq \Omega_P |P_{\mathbf{M}}|$$

(car $|\boldsymbol{\omega}^{\mathbf{h}}| = 1$ pour tous $\boldsymbol{\omega}$ et $\mathbf{h}$), par la relation (7) on obtient :

$$|P_{\mathbf{M}}| \leq \frac{1}{d} \Omega_P |P_{\mathbf{M}}| R_{\mathbf{d},P}. \tag{8}$$

Puisque par hypothèse P est non nul, $P_{\mathbf{M}} \neq 0$ et donc on peut diviser les membres de la relation (8) par $|P_{\mathbf{M}}|$. On obtient alors le résultat souhaité. □

3 Corps totalement réels et algèbres sur groupes finis

Comme déjà annoncé, dans ce paragraphe on montre que tout corps totalement réel n'est pas PCM.

Lemme 1. *Soit K un corps de nombres et soit Γ son groupe de $\mathbb{Q}$-automorphismes ; notons L la clotûre galoisienne de K et posons $G := \mathrm{Gal}(\mathrm{L}/\mathbb{Q})$. Alors, en utilisant les notations du paragraphe 1, pour tout $\phi \in \mathbb{Z}[\Gamma]$ il existe $\psi \in \mathbb{Z}[G]$ tel que :*

$$\frac{\|\psi\|_1 R_\psi}{[L:\mathbb{Q}]} \leq \frac{\|\phi\|_1 R_\phi}{[K:\mathbb{Q}]}.$$

Preuve. Soit $\phi = \sum_{\sigma\in\Gamma} \phi_\sigma\sigma \in \mathbb{Z}[\Gamma]$. Pour tout $\sigma \in \Gamma$ choisissons un élément $\widetilde{\sigma} \in G$ tel que $\widetilde{\sigma}$ coïncide avec σ sur K. Notons $\widetilde{\phi}$ l'élément :

$$\widetilde{\phi} = \sum_{\sigma\in\Gamma} \phi_\sigma\widetilde{\sigma} \in \mathbb{Z}[G].$$

Soit maintenant H_K =Gal(L/K) et posons $N = \sum_{\sigma\in H_K} \sigma$ et $\psi = \widetilde{\phi}N$. Il est alors évident, par construction, que $R_\psi = R_\phi$. De plus, puisque $\|\phi\|_1 = \|\widetilde{\phi}\|_1$ et $\|N\|_1 = |H_K| = [L : K]$, nous obtenons :

$$\begin{aligned}\|\psi\|_1 &\leq \sum_{\sigma\in H_K} \|\widetilde{\phi}\sigma\|_1 \\ &= \|\phi\|_1[L : K].\end{aligned}$$

Donc, en observant que $[L : \mathbb{Q}] = [K : \mathbb{Q}][L : K]$ et que $R_\psi = R_\phi$, on en déduit :

$$\begin{aligned}\frac{\|\psi\|_1 R_\psi}{[L : \mathbb{Q}]} &\leq \frac{\|\phi\|_1 R_\phi[L : K]}{[L : K][K : \mathbb{Q}]} \\ &= \frac{\|\phi\|_1 R_\phi}{[K : \mathbb{Q}]}.\end{aligned}$$

□

Lemme 2. *Soit $K/\mathbb{Q}$ une extension galoisienne finie de $\mathbb{Q}$ totalement réelle de groupe de Galois G. Alors, en utilisant les notations du premier paragraphe, pour tout $\phi = \sum_{\sigma\in G} \phi_\sigma\sigma \in \mathbb{Z}[G]$ on a : $R_\phi = \widetilde{R}_\phi$.*

Preuve. Puisque K est, par hypothèse, un corps totalement réel, les places infinies de K sont exactement les éléments de G. Donc, pour tout $\alpha \in K^*$, nous avons :

$$\mathcal{L}(\alpha) = (\log|\alpha|_v)_{v|\infty} = (\log|\alpha^\sigma|)_{\sigma\in G}.$$

0 Soit L_ϕ l'endomorphisme linéaire de $\mathcal{L}(K^*) \otimes \mathbb{R}$ définie par :

$$L_\phi((\log|\alpha^\sigma|)_\sigma \otimes c) = (\log|\alpha^{\sigma\phi}|)_\sigma \otimes c$$

pour tout $\alpha \in K^*$ et $c \in \mathbb{R}$. Puisque l'image de L_ϕ coïncide avec l'espace $\mathcal{L}(K^{*\phi}) \otimes \mathbb{R}$, le rang de L_ϕ est égal à R_ϕ.

Rappelons maintenant que ϕ est un élément de $\mathbb{Z}[G]$. La multiplication à droite par ϕ est donc un endomorphisme linéaire de $\mathbb{Q}[G]$ et, par simples arguments d'algèbre linéaire, on obtient que la dimension du noyau de tel endomorphisme est égale à $\dim(\ker(T_\phi))$ (on a utilisé la notation du théorème 2 où est défini T_ϕ comme l'endomorphisme linéaire de $\mathbb{C}[G]$ qui agit sur les éléments de $\mathbb{C}[G]$ en multipliant à droite par ϕ). Par ailleurs, une famille d'éléments de $\mathbb{Z}[G]$ étant $\mathbb{Z}$ libre si et seulement si elle est $\mathbb{Q}$ libre, nous obtenons que $\dim(\ker(T_\phi))$

est égal au rang du sous-module de $\mathbb{Z}[G]$ des éléments λ tels que $\lambda\phi = 0$. Notons maintenant $n = \dim(\ker(T_\phi))$ et soit C un ensemble de cardinalité maximale d'éléments $\lambda_i = \sum_{\sigma\in G} \lambda_{i,\sigma}\sigma \in \mathbb{Z}[G]$ indépendants sur $\mathbb{Z}$ tels que $\lambda_i\phi = 0$ pour tout $1 \leq i \leq n$. Remarquons alors que $\mathfrak{L}(K^{*\phi}) \otimes \mathbb{R}$ et

$$V := \{\mathbf{x} \in \mathfrak{L}(K^*) \otimes \mathbb{R} \text{ t. q. } \sum_{\sigma\in G} \lambda_{i,\sigma} x_\sigma = 0 \ \forall i\}$$

coïncident. En effet pour tout $\alpha \in K^*$ nous avons $(\log|\alpha^{\lambda_i\phi}|) = 0$ pour tout $1 \leq i \leq n$. Donc V contient $\mathfrak{L}(K^{*\phi}) \otimes \mathbb{R}$. L'autre inclusion découle de la maximalité du cardinal de C. Par ailleurs, puisque les éléments λ_i sont indépendants pour tout $1 \leq i \leq n$ et $n = \dim(\ker(T_\phi))$, on obtient :

$$R_\phi = \dim(\mathfrak{L}(K^{*\phi}) \otimes \mathbb{R}) = \dim(V) = |G| - \dim(\ker(T_\phi)) = \widetilde{R_\phi}.$$

□

Le lemme 2 nous dit que le rang R_ϕ de $\mathfrak{L}(K^\phi) \otimes \mathbb{R}$ est égal au rang $\widetilde{R}_\phi$ de l'endomorphisme T_ϕ de $\mathbb{C}[G]$ qui envoie $\psi \in \mathbb{C}[G]$ sur $\psi\phi$. On notera donc également dans la suite R_ϕ le rang de T_ϕ.

Le lemme suivant est le dernier résultat nécessaire pour la preuve du théorème 2.

Lemme 3. *Soient n, r entiers positifs et soient $U_1, \ldots, U_n$ matrices unitaires d'ordre $r \times r$ à coefficients dans $\mathbb{C}$. De plus soient $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ et posons $M = \sum_{i=1}^n \lambda_i U_i$. Alors on a :*

$$|Tr(M)| \leq \left(\sum_{i=1}^n |\lambda_i|\right) R(M)$$

où $Tr(M)$ est la trace de M et $R(M)$ son rang.

Preuve. Puisque la trace de M est égal à la somme de ses valeurs propres et le rang de M est égal au nombre de ses valeurs propres non nuls (toute valeur propre est comptée avec sa multiplicité algébrique), si μ est une valeur propre de module maximum on a :

$$|Tr(M)| \leq |\mu| R(M).$$

Il suffit donc montrer l'inégalité :

$$|\mu| \leq \sum_{i=1}^n |\lambda_i|.$$

Par hypothèse pour tout $1 \leq i \leq n$ les matrices U_i sont unitaires. Donc, en considérant la norme $\|.\|$ induite par le produit scalaire standard de $\mathbb{C}^r$, on a, pour tout $v \in \mathbb{C}^r$

$$\|U_i(v)\| = \|v\|.$$

Soit maintenant w un vecteur propre de M de norme 1 associé au valeur propre μ. On obtient :

$$\begin{aligned}|\mu| &= \|M(w)\| \\ &= \|\sum_{i=1}^{n} \lambda_i U_i(w)\| \\ &\leq \sum_{i=1}^{n} \|\lambda_i U_i(w)\| \\ &= \sum_{i=1}^{n} |\lambda_i|.\end{aligned}$$

□

Avant de terminer ce paragraphe avec la preuve du théorème 2 et du corollaire 1, rappelons quelques propriétés des $\mathbb{C}$-algèbres sur groupes finis.

Soit G un groupe fini, soit $\mathrm{Irr(G)}$ l'ensemble des caractères irréductibles de G et considérons la $\mathbb{C}$-algèbre $\mathbb{C}[G]$. La théorie des représentations (voir [Isa], Chapter 1) nous dit que

$$\mathbb{C}[G] = \bigoplus_{\chi \in \mathrm{Irr(G)}} I_\chi^{\chi(1)} \tag{9}$$

où I_χ est un espace vectoriel sur $\mathbb{C}$ de dimension $\chi(1)$ et un idéal à droite de $\mathbb{C}[G]$.

Soit maintenant $\phi \in \mathbb{C}[G]$, considérons l'endomorphisme T_ϕ précédemment défini (par exemple voir l'énoncé du théorème 2 dans le premier paragraphe). Puisque pour tout caractère χ l'ensemble I_χ est un idéal à droite, la restriction $T_{\chi,\phi}$ de T_ϕ à I_χ est une application de I_χ dans I_χ. De plus si R_ϕ désigne le rang de T_ϕ et $R_{\chi,\phi}$ celui de $T_{\chi,\phi}$, par (9) on a :

$$R_\phi = \sum_{\chi \in \mathrm{Irr(G)}} \chi(1) R_{\chi,\phi}. \tag{10}$$

Preuve du théorème 2 . Soit $\phi = \sum_{\sigma \in G} \phi_\sigma \sigma$ un élément non nul de $\mathbb{C}[G]$, posons

$$\|\phi\|_1 = \sum_{\sigma \in G} |\phi_\sigma|.$$

Pour tout $\sigma \in G$ on a $\|\phi\|_1 = \|\phi\sigma\|_1$, $R_\phi = R_{\phi\sigma}$ et $\Omega_\phi = \Omega_{\phi\sigma}$ (rappelons que nous avons changé notre notation après le lemme 2 en posant $\widetilde{R}_\phi = R_\phi$). Nous pouvons donc supposer $|\phi_1| \geq |\phi_\sigma|$ pour tout $\sigma \in G$. Par conséquent

$$\|\phi\|_1 \leq \Omega_\phi |\phi_1|.$$

Définissons maintenant le nombre complexe

$$\beta_\phi = \sum_{\chi \in \mathrm{Irr(G)}} \chi(1) \sum_{\sigma \in G} \phi_\sigma \chi(\sigma).$$

Démontrons tout d'abord que :

$$|\beta_\phi| \leq ||\phi||_1 R_\phi.$$

Soit $\chi \in \mathrm{Irr(G)}$ et fixons une base B_χ de I_χ. Pour tout $\psi \in \mathbb{C}[G]$ nous pouvons associer à l'application linéaire $T_{\chi,\psi} \in \mathrm{End(I_\chi)}$ qui envoi $\alpha \in I_\chi$ sur $\alpha\psi$, la matrice $M_{\chi,\psi}$ de $T_{\chi,\psi}$ dans la base B_χ. En particulier pour tout $\sigma \in G$ les matrices $M_{\chi,\sigma}$ sont bien définies. De plus

$$M_{\chi,\phi} = \sum_{\sigma \in G} \phi_\sigma M_{\chi,\sigma}.$$

Par définition de caractère, $\chi(\sigma)$ est la trace de la matrice $M_{\chi,\sigma}$; en outre les matrices $M_{\chi,\sigma}$ sont unitaires car $T_{\chi,\sigma}$ est d'ordre fini. On peut donc appliquer le lemme 3 à la matrice $M_{\chi,\phi}$, ce qui nous donne :

$$|\sum_{\sigma \in G} \phi_\sigma \chi(\sigma)| = |Tr(M_{\chi,\phi})| \leq ||\phi||_1 R_{\chi,\phi}.$$

Par cette relation et par (10) on a :

$$|\beta_\phi| \leq \sum_{\chi \in \mathrm{Irr(G)}} \chi(1) \left| \sum_{\sigma \in G} \phi_\sigma \chi(\sigma) \right| \leq \|\phi\|_1 R_\phi. \tag{11}$$

Calculons maintenant la valeur de β_ϕ à l'aide des lois d'orthogonalité entre les colonnes des tables des caractères (voir [Isa], (2.13) Theorem et (2.14) Corollary)

$$\begin{aligned} \beta_\phi &= \sum_{\chi \in \mathrm{Irr(G)}} \chi(1) \sum_{\sigma \in G} \phi_\sigma \chi(\sigma) \\ &= \sum_{\sigma \in G} \phi_\sigma \sum_{\chi \in \mathrm{Irr(G)}} \chi(\sigma)\chi(1) \\ &= \phi_1 |G|. \end{aligned}$$

On en déduit :

$$||\phi||_1 R_\phi \geq |\phi_1||G|$$

et, puisque $\Omega_\phi |\phi_1| \geq \|\phi\|_1$ et $\phi_1 \neq 0$ car ϕ est non nul, on obtient le théorème. □

Preuve du corollaire 1 . Soit K un corps totalement réel. Puisque par le lemme 1 si un corps est PCM alors sa clotûre galoisienne est PCM, on peut supposer l'extension $K/\mathbb{Q}$ galoisienne. Notons alors G le groupe de Galois de $K/\mathbb{Q}$ et soit ϕ un élément non nul de $\mathbb{Z}[G]$. Par le lemme 2 la dimension R_ϕ de $\mathcal{L}(K^\phi) \otimes \mathbb{R}$ est égale au rang de l'endomorphisme de $\mathbb{C}[G]$ qui envoi $\psi \in \mathbb{C}[G]$ sur $\psi\phi$. Par ailleurs par la remarque précédente et le théorème 2 on a :

$$\Omega_\phi R_\phi \geq |G|.$$

Puisque les coefficients de ϕ sont entiers nous avons $\Omega_\phi \leq \|\phi\|_1$. De plus $|G| = [K : \mathbb{Q}]$ car $K/\mathbb{Q}$ est une extension de galoisienne. Donc :

$$\|\phi\|_1 R_\phi \geq [K : \mathbb{Q}]$$

et K n'est pas PCM. □

4 Appendice

Soit G un groupe abélien fini et soient d_1,..., d_k entier positifs tels que G est isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$ (après on idèntifiera G avec le groupe $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$ et $\{0, 1, \ldots, d_i - 1\}$ avec $\mathbb{Z}/d_i\mathbb{Z}$ pour $1 \leq i \leq k$). Soit $F\colon \mathbb{C}[G] \to \mathbb{C}[x_1, \ldots, x_k]$ l'application qui envoi

$$\phi = \sum_{\mathbf{h} \in G} \phi_{\mathbf{h}} \mathbf{h} \in \mathbb{C}[G]$$

dans :

$$F(\phi) = \sum_{h_1=0}^{d_1-1} \cdots \sum_{h_k=0}^{d_k-1} \phi_{\mathbf{h}} \mathbf{X}^{\mathbf{h}}.$$

Il est bien évident que F définit une correspondance biunivoque entre les éléments de $\mathbb{C}[G]$ et les polynômes $Q \in \mathbb{C}[x_1, \ldots, x_k]$ tels que $\deg_{x_i}(Q) < d_i$ pour tout $1 \leq i \leq k$.

Fixons maintenant $\phi \in \mathbb{C}[G]$ et notons $P(x_1, \ldots, x_k) := F(\phi)$. Par définition de F il suit immédiatement que $\Omega_\phi = \Omega_P$. Nous voulons montrer que même R_ϕ est égal $R_{\mathbf{d},P}$.

Soit $\chi \in \mathrm{Irr(G)}$. Puisque G est abélien, $\mathrm{Irr(G)}$ est un groupe isomorphe à G et $\chi(1) = 1$. De plus $R_{\chi,\phi} = 0$ si et seulement si

$$\sum_{\mathbf{h} \in G} P_{\mathbf{h}} \chi(\mathbf{h}) = 0$$

(voir [Was], p. 100). On a donc :

$$R_\phi = \left| \{\chi \in \mathrm{Irr(G)} \text{ t.q. } \sum_{\mathbf{h} \in \mathrm{G}} \mathrm{P}_{\mathbf{h}} \chi(\mathbf{h}) \neq 0\} \right|. \tag{12}$$

Soit maintenant $\boldsymbol{\omega} = (\omega_1, \ldots, \omega_k) \in \mu_{d_1} \times \cdots \times \mu_{d_k}$. Il est bien évident que la fonction

$$\chi_{\boldsymbol{\omega}} \colon G \to \mathbb{C}^*$$

laquelle envoie $\mathbf{h} = (h_1, \ldots, h_k)$ sur $\prod_{i=1}^k \omega_i^{h_i}$ est un caractère irréductible de G. De plus on obtient

$$\sum_{\mathbf{h} \in G} P_{\mathbf{h}} \chi_{\boldsymbol{\omega}}(\mathbf{h}) = \sum_{\mathbf{h} \in G} P_{\mathbf{h}} \boldsymbol{\omega}^{\mathbf{h}}$$

et donc $R_{\chi\boldsymbol{\omega},\phi} = 0$ si et seulement si $P(\boldsymbol{\omega}) = 0$. D'ailleurs si $\chi \in \mathrm{Irr(G)}$ alors

$$\boldsymbol{\omega_\chi} := (\chi(1, 0 \ldots, 0), \ldots, \chi(0, 0, \ldots, 1))$$

appartient à $\mu_{d_1} \times \cdots \times \mu_{d_k}$. De plus par construction :

$$\sum_{\mathbf{h}\in G} P_{\mathbf{h}} \boldsymbol{\omega_\chi}^{\mathbf{h}} = \sum_{\mathbf{h}\in G} P_{\mathbf{h}} \chi(\mathbf{h}).$$

Puisque $\mathrm{Irr(G)}$ est isomorphe à G qui à son tour est isomorphe à $\mu_{d_1} \times \cdots \times \mu_{d_k}$ la correspondance que nous venons de définir entre les caractères irréductibles de G et les éléments de $\mu_{d_1} \times \cdots \times \mu_{d_k}$ est biunivoque. On a alors :

$$|\{\chi \in \mathrm{Irr(G)\ t.q.}\ \sum_{\mathbf{h}\in \mathrm{G}} \mathrm{P_h}\chi(\mathbf{h}) \neq 0\}| = |\{\boldsymbol{\omega} \in \mu_{\mathrm{d_1}} \times \cdots \times \mu_{\mathrm{d_k}}\ \mathrm{P}(\boldsymbol{\omega}) \neq 0\}|$$

et, par (12) et par définition de $R_{\mathbf{d},P}$, on obtient :

$$R_\phi = R_{\mathbf{d},P}.$$

En conclusion on a donc montré qu'il est possible de définir une correspondance biunivoque entre les éléments ϕ de $\mathbb{C}[G]$ (où G est isomorphe au groupe $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$) et les polynômes P de $\mathbb{C}[x_1, \ldots, x_k]$ tels que $\deg_{x_i}(P) < d_i$ pour tout $1 \leq i \leq k$. De plus si P correspond à ϕ nous avons que $\Omega_\phi = \Omega_P$ et $R_\phi = R_{\mathbf{d},P}$.

Références

[Amo1] F. AMOROSO, Groupes des classes de corps « proches » d'un corps CM. Preprint (2005).

[Amo2] F. AMOROSO, Une minoration pour l'exposant du groupe des classes d'un corps engendré par un nombre de Salem, J. of Number Theory, à paraître.

[Isa] I. M. ISAACS, Character theory of finite groups. 1st ed. PI 69. New York, NY : Academic Press. 303 p. 1976.

[Was] L. C. WASHINGHTON, Introduction to cyclotomic fields. 2nd ed. GTM 84. New York, NY : Springer. xiv, 487 p. 1997.

Gabriele Ranieri
Laboratoire de mathématiques
Nicolas Oresme, CNRS UMR 6139
Université de Caen, BP 5186
14032 Caen Cedex, FRANCE.

Dipartimento di matematica
Leonida Tonelli,
Largo Bruno Pontecorvo, 5
56127 Pisa, ITALIA.
E-mail : ranieri@math.unicaen.fr, ranieri@mail.dm.unipi.it