HAL open science

Degré de définition des endomorphismes d'une variété abélienne

Gaël Rémond

▶ To cite this version:

Gaël Rémond. Degré de définition des endomorphismes d'une variété abélienne. Journal of the European Mathematical Society, 2020, 22 (9), pp.3059-3099. 10.4171/JEMS/981 . hal-03041900

HAL Id: hal-03041900
https://hal.science/hal-03041900v1

Submitted on 5 Dec 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Degré de définition des endomorphismes d'une variété abélienne

Gaël RÉMOND

juin 2018

Abstract. — Given an abelian variety over a field of zero characteristic, we give an optimal explicit upper bound depending only on the dimension for the degree of the smallest extension of the base field over which all endomorphisms of the abelian variety are defined. For each dimension, the bound is achieved over the rationals by twisting a power of a CM elliptic curve. This complements a result of Guralnick and Kedlaya giving the exact value of the least common multiple of all these degrees. We also provide a similar statement for the homomorphisms between two distinct abelian varieties. The proof relies on divisibility bounds obtained by Minkowski's method but, in some cases, we need more precise facts on finite linear groups, including a theorem of Feit whose proof has not been published : we therefore include one based on work by Collins on Jordan's theorem.

1 Introduction

Soit K un corps de caractéristique nulle. Si A et B sont des variétés abéliennes sur K, l'ensemble des extensions L de K telles que $\mathrm{Hom}(A_L, B_L) = \mathrm{Hom}(A_{\overline{K}}, B_{\overline{K}})$ admet un plus petit élément qui est une extension galoisienne finie de K et que nous notons $K_{A,B}$. Dans le cas d'une unique variété A, nous abrégeons $K_{A,A}$ en K_A, le corps de définition des endomorphismes de $A_{\overline{K}}$.

Pour un entier naturel $g \geq 1$, posons $f(g) = 2\alpha(g)6^{g-1}g!$ où $\alpha(g) = 1$ si $g \notin \{2, 4, 6\}$ et $\alpha(2) = 2$, $\alpha(4) = 5$, $\alpha(6) = 7/6$.

Théorème 1.1 *Pour toute variété abélienne non nulle A sur K, nous avons $[K_A : K] \leq f(\dim A)$ et cette majoration est optimale au sens où, pour tout $g \geq 1$, il existe une variété abélienne A sur $K = \mathbb{Q}$ de dimension g telle que $[\mathbb{Q}_A : \mathbb{Q}] = f(g)$ et $A_{\overline{K}} \simeq E^g$ où E est la courbe elliptique CM sur $\overline{\mathbb{Q}}$ d'équation $y^2 = x^3 - 1$ (si $g \neq 2$) ou $y^2 = x^3 - x$ (si $g = 2$).*

Ce résultat était connu pour $g = 1$ (classique) et $g = 2$ d'après [FKRS] (au moins si K est un corps de nombres). La première majoration générale de $[K_A : K]$ remonte à Silverberg en 1992 (voir [Si]) qui donnait même une divisibilité et donc une majoration du ppcm de tous les $[K_A : K]$ (à dimension fixée). Dans un travail récent (voir [GK]), Guralnick et Kedlaya améliorent ceci en déterminant la valeur exacte du ppcm. En fait, leur théorème est même plus général puisque $[K_A : K]$ y est remplacé par le nombre de composantes du groupe de Sato-Tate de A (qui est un multiple de $[K_A : K]$). Ils évoquent aussi le problème de déterminer la valeur de $f(g)$ ci-dessus en suggérant le résultat pour g assez grand.

Nous pouvons donner un énoncé de même facture pour les morphismes entre deux variétés. Pour cela, si g et h sont deux entiers naturels non nuls, notons

$$\mathcal{F}(g,h) = \begin{cases} 3f(g)f(h) & \text{si } 2 \notin \{g,h\}, \\ 2f(g)f(h) & \text{si } \max(g,h) = 2, \\ (3/2)f(g)f(h) & \text{sinon.} \end{cases}$$

Théorème 1.2 *Pour toutes variétés abéliennes non nulles A et B sur K, nous avons $[K_{A,B} : K] \leq \mathcal{F}(\dim A, \dim B)$ et pour tous $g, h \geq 1$ il existe deux variétés abéliennes A et B sur $\mathbb{Q}$ de dimensions respectives g et h telles que $[\mathbb{Q}_{A,B} : \mathbb{Q}] = \mathcal{F}(g,h)$, $A_{\overline{\mathbb{Q}}} \simeq E^g$ et $B_{\overline{\mathbb{Q}}} \simeq E^h$ où E est l'une des deux courbes elliptiques $y^2 = x^3 - 1$ ou $y^2 = x^3 - x$.*

Pour contrôler $K_{A,B}$, il est utile de disposer du fait beaucoup plus élémentaire suivant, où pour une variété abélienne A sur K nous notons μ_A le nombre de racines de l'unité dans le centre de l'algèbre $(\mathrm{End} A_{\overline{K}}) \otimes \mathbb{Q}$.

Proposition 1.3 *Si A et B sont deux variétés abéliennes sur K telles que $K_A = K_B = K$ alors $[K_{A,B} : K] \mid \mathrm{pgcd}(\mu_A, \mu_B)$.*

Si, par exemple, nous nous intéressons aux morphismes vers une variété abélienne fixée B avec $K_B = K$, nous pouvons dire que, pour tout A, le degré $[K_{A,B} : K]$ divise $\mu_A[K_A : K]$. Notre dernier énoncé donne une majoration de cette quantité. Écrivons pour cela $\omega(g) = 6f(g)$ si $g \geq 1$ et $g \notin \{2, 5\}$ puis $\omega(2) = 4f(2)$ et $\omega(5) = 8f(5)$.

Théorème 1.4 *Pour toute variété abélienne non nulle A sur K, nous avons la majoration $\mu_A[K_A : K] \leq \omega(\dim A)$ et pour tout $g \geq 1$ il existe une variété abélienne A sur $\mathbb{Q}$ de dimension g telle que $\mu_A[\mathbb{Q}_A : \mathbb{Q}] = \omega(g)$.*

Ici aussi l'égalité s'obtient à l'aide des deux courbes elliptiques précédentes mais, en dimension 5, une puissance de l'une ne suffit pas, les deux courbes doivent intervenir (voir proposition 2.4).

Les démonstrations de nos trois théorèmes sont semblables, décrivons ici l'approche pour le théorème 1.1. Le début ressemble au paragraphe 5 de [GK] mais nous ne parlons pas de groupe de Sato-Tate. Nous considérons directement l'action de $\mathrm{Gal}(\overline{K}/K)$ sur l'algèbre $\mathfrak{A} = (\mathrm{End} A_{\overline{K}}) \otimes \mathbb{Q}$. Par définition, $\mathrm{Gal}(K_A/K)$ s'identifie à l'image de $\mathrm{Gal}(\overline{K}/K)$ dans les automorphismes de cette $\mathbb{Q}$-algèbre. Il se trouve que, dans la plupart des cas, cette inclusion suffit, c'est-à-dire que nous pouvons nous contenter de borner $[K_A : K]$ par le cardinal maximal d'un sous-groupe fini de $\mathrm{Aut}_{\mathbb{Q}}(\mathfrak{A})$. En réalité, une première série de réductions montrera que nous pouvons supposer que $A_{\overline{K}}$ est isotypique c'est-à-dire que l'algèbre $\mathfrak{A}$ est simple. Notons F son centre qui est un corps de nombres. Nous disposons d'un morphisme naturel $\mathrm{Aut}_{\mathbb{Q}}(\mathfrak{A}) \to \mathrm{Aut}_{\mathbb{Q}}(F)$ et, par le théorème de Skolem-Noether, son noyau $\mathrm{Aut}_F(\mathfrak{A})$ est formé des automorphismes intérieurs donc s'écrit $\mathfrak{A}^\times/F^\times$. Nous nous intéressons donc aux sous-groupe finis d'un tel quotient et posons pour un corps de nombres F et un entier $n \geq 1$

$$\Gamma_F(n) = \mathrm{ppcm}\{\mathrm{Card} G \mid G \subset \mathfrak{A}^\times/F^\times,\ [\mathfrak{A} : F] = n^2\}$$

où $\mathfrak{A}$ parcourt ici les F-algèbres centrales simples de dimension n^2 et G les sous-groupes finis de $\mathfrak{A}^\times/F^\times$. Par ce qui précède, nous avons donc une première majoration $[K_A : K] \leq [F : \mathbb{Q}]\Gamma_F(n)$ (lorsque $A_{\overline{K}}$ est isotypique et $n = [\mathfrak{A} : F]^{1/2}$).

Nous nous appuyons alors sur la méthode de réduction de Minkowski (déjà utilisée dans [GK] et, un peu différemment, dans [Si]) pour déterminer la valeur exacte de $\Gamma_F(n)$. Il s'agit essentiellement d'injecter le groupe G dans un groupe de la forme $\mathrm{PGL}_n(\mathcal{O}_F/\mathfrak{p})$ où $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_F$ soigneusement choisi (on utilise notamment le théorème de Chebotarev). Ce procédé permet de contrôler de façon optimale les diviseurs impairs de $\mathrm{Card} G$ mais pour borner l'exposant de 2 un travail supplémentaire est requis. Cette étape s'inspire de la présentation de la méthode de Minkowski par Guralnick et Lorenz (voir [GL]). Notons que la valeur trouvée pour $\Gamma_F(n)$ est presque la même que celle que nous aurions si nous supposions que G

était le quotient d'un sous-groupe fini de $\mathfrak{A}^\times$: les deux quantités diffèrent seulement d'un facteur 1 ou 2 selon le couple (F, n) (voir théorème 4.2).

En estimant numériquement une borne supérieure pour $\Gamma_F(n)$, nous constatons ensuite que la majoration de $[K_A : K]$ ci-dessus permet de conclure sauf lorsque $A_{\overline{K}}$ est la puissance d'une courbe ellptique à multiplications complexes. Dans ce cas, F est un corps quadratique imaginaire, $n = g$ et $\mathfrak{A} \simeq M_g(F)$. Un argument un peu différent montre que $[K_A : K]$ peut être contrôlé par le cardinal maximal d'un sous-groupe fini de $\mathrm{GL}_g(K)$. Si F n'est pas cyclotomique, la connaissance de $\Gamma_F(g)$ suffit encore pour obtenir la majoration voulue sauf pour un nombre fini de couples (F, g) qui peuvent être traités à part.

En revanche, lorsque F est l'un des deux corps cyclotomiques quadratiques $\mathbb{Q}(\mu_4)$ ou $\mathbb{Q}(\mu_6)$, nous devons être beaucoup plus précis puisque ce sont ces deux situations qui vont donner la valeur de $f(g)$: en effet les endomorphismes de $y^2 = x^3 - x$ et $y^2 = x^3 - 1$ sont respectivement $\mathbb{Z}[\mu_4]$ et $\mathbb{Z}[\mu_6]$. Pour conclure, nous devons connaître exactement le cardinal maximal d'un sous-groupe fini de $\mathrm{GL}_g(\mathbb{Q}(\mu_4))$ et $\mathrm{GL}_g(\mathbb{Q}(\mu_6))$. Or un résultat de Feit (voir [Fe] ou [BDEPS]) répond précisément à cette question, même pour tout corps cyclotomique. Malheureusement, la démonstration de Feit n'a jamais été publiée et de plus son théorème comporte un oubli dans le cas de $\mathrm{GL}_6(\mathbb{Q}(\mu_4))$. Pour ces raisons, il nous a paru opportun de donner ici en appendice une preuve complète du théorème de Feit à l'aide de résultats plus récents. Ceux-ci concernent la fonction de Jordan

$$j(n) = \sup_{G \subset \mathrm{GL}_n(\mathbb{C})} \min_{H \subset G} [G : H]$$

où G parcourt les sous-groupes finis de $\mathrm{GL}_n(\mathbb{C})$ et H les sous-groupes abéliens distingués de G. Jordan a montré en 1878 que $j(n)$ était fini pour tout n. Feit utilisait des résultats (non publiés) de Weisfeiler donnant une majoration de $j(n)$. En utilisant (comme Weisfeiler) la classification des groupes simples finis, Collins (voir [C1] et le théorème 7.2 ci-dessous) a calculé la valeur exacte de $j(n)$ pour tout $n \geq 1$; par exemple $j(n) = (n+1)!$ si $n \geq 71$. Nous déduirons ici le théorème de Feit pour tous les corps cyclotomiques (y compris $\mathbb{Q}$) du travail de Collins.

En particulier, pour tout $g \notin \{2, 4, 6\}$, le cardinal maximal d'un sous-groupe fini de $\mathrm{GL}_g(\mathbb{Q}(\mu_6))$ est $6^g g!$, atteint pour le produit en couronne $\mu_6 \wr \mathfrak{S}_g$ vu comme le sous-groupe des matrices ayant dans chaque colonne un unique élément non nul, choisi dans μ_6. Ce groupe conduit à la borne $f(g)$ de même que trois groupes exceptionnels dans $\mathrm{GL}_2(\mathbb{Q}(\mu_4))$, $\mathrm{GL}_4(\mathbb{Q}(\mu_6))$ et $\mathrm{GL}_6(\mathbb{Q}(\mu_6))$ pour les autres valeurs de g.

Pour terminer la démonstration du théorème 1.1 (optimalité de la majoration), il faut vérifier que nous pouvons renverser l'argument et construire à partir de ces sous-groupes des variétés abéliennes sur $\mathbb{Q}$ avec $[\mathbb{Q}_A : \mathbb{Q}] = f(g)$. Nous tirons parti du fait que ces groupes sont des groupes de pseudo-réflexions pour utiliser (comme dans [BDEPS]) un argument de théorie inverse de Galois et leur associer un 1-cocycle galoisien à valeur dans $\mathrm{GL}_g(F)$ qui à son tour donne naissance à une $\mathbb{Q}$-forme A de E^g où E est une courbe elliptique sur $\mathbb{Q}$ telle que $\mathrm{End} E_{\overline{\mathbb{Q}}} \simeq \mathcal{O}_F$.

Cette étape de construction de $\mathbb{Q}$-formes est présentée dans la partie suivante. Après cela, notre plan suit l'ordre des arguments esquissés ci-dessus à ceci près que nous traitons simultanément nos trois théorèmes principaux.

Notations. Si A est une variété abélienne sur un corps K et L une extension de K, nous notons simplement L_A le corps L_{A_L}. Deux variétés abéliennes sur un corps K sont dites isogènes si $\mathrm{Hom}(A, B)$ contient une isogénie (ce qui est plus restrictif que de demander que $\mathrm{Hom}(A_{\overline{K}}, B_{\overline{K}})$ en contienne une). Pour les racines de l'unité, en plus de la notation μ_A associée ci-dessus à une variété abélienne A, nous notons μ_F le nombre de racines de l'unité d'un corps de nombres F tandis que μ_n désignera

le groupe $\{\xi \in \overline{\mathbb{Q}} \mid \xi^n = 1\}$ pour tout entier $n \geq 1$. Nous écrivons $Z(\cdot)$ pour le centre d'un groupe ou d'un anneau. Le lettre I représente une matrice identité. Lorsque ce n'est pas précisé, la lettre g désigne toujours un entier naturel non nul.

2 Minorations

Nous rappelons qu'une pseudo-réflexion est un endomorphisme d'ordre fini d'un espace vectoriel induisant l'identité sur un hyperplan. Nous commençons par un énoncé de théorie inverse de Galois de nature voisine de ceux utilisés dans [BDEPS]. Lorsque K est un corps quadratique imaginaire, nous appelons *conjugaison* l'unique automorphisme non trivial de K et nous la notons $z \mapsto \overline{z}$ si z est un élément de K ou, par extension, une matrice ou un polynôme à coefficients dans K.

Proposition 2.1 *Soient K un corps quadratique imaginaire et $G \subset \mathrm{GL}_g(K)$ un sous-groupe fini stable par conjugaison et engendré par des pseudo-réflexions. Il existe une extension L de K telle que l'extension $L/\mathbb{Q}$ est galoisienne, le groupe $\mathrm{Gal}(L/\mathbb{Q})$ est isomorphe au produit semi-direct de G par $\mathbb{Z}/2\mathbb{Z}$ (agissant sur G à travers la conjugaison) et $G \simeq \mathrm{Gal}(L/K)$ dans cet isomorphisme.*

Démonstration. Par le théorème de Shephard et Todd (voir le théorème 3.20 page 48 de [LT]), il existe des polynômes homogènes et algébriquement indépendants $F_1, \ldots, F_g \in K[X_1, \ldots, X_g]$ tels que, pour l'action naturelle de G sur $K[X_1, \ldots, X_g]$, la sous-algèbre des éléments G-invariants soit $K[X_1, \ldots, X_g]^G = K[F_1, \ldots, F_g]$. Montrons par récurrence sur $D \geq 0$ qu'il est possible de modifier les F_i de sorte que $\overline{F_i} = F_i$ dès que $\deg F_i \leq D$. Pour $D = 0$ il n'y a rien à faire. Si $D \geq 1$, nous supposons que les F_i de degré $< D$ vérifient $\overline{F_i} = F_i$. Notons $J = \{i \mid \deg F_i = D\}$, $J' = \{i \mid \deg F_i < D\}$ et V le K-espace vectoriel engendré par les F_i, $i \in J$. Si $P \in V$ alors pour $\varphi \in G$ on a $\varphi \cdot \overline{P} = \overline{\overline{\varphi} \cdot P} = \overline{P}$ puisque $\overline{\varphi} \in G$ et P est G-invariant. Ainsi $\overline{P} \in K[F_1, \ldots, F_g]$ et, comme $\deg \overline{P} \leq D$, nous pouvons écrire $\overline{P}$ comme la somme d'un élément $\delta(P)$ de V et d'un polynôme en les F_i, $i \in J'$. Ceci définit une application semi-linéaire $\delta \colon V \to V$ et, modulo des polynômes en les F_i, $i \in J'$ (stables par conjugaison), nous avons $P \equiv \overline{\delta(P)} \equiv \delta(\delta(P))$ ce qui entraîne $\delta(\delta(P)) = P$. Nous pouvons donc voir δ comme définissant une action semi-linéaire de $\mathrm{Gal}(K/\mathbb{Q})$ sur V et donc, d'après un lemme de Silverman (voir le lemme II.5.8.1 de [S1]), il existe une base de V formée de polynômes F_i' avec $\delta(F_i') = F_i'$ $(i \in J)$. Posons $F_i'' = (1/2)(F_i' + \overline{F_i'})$. Alors $F_i' - F_i'' = (1/2)(F_i' - \overline{F_i'}) \equiv (1/2)(F_i' - \delta(F_i')) = 0$ modulo un polynôme en les F_j, $j \in J'$. On en déduit que l'on peut remplacer les F_i $(i \in J)$ par les F_i' puis les F_i'' sans changer $K[F_1, \ldots, F_g]$.

Grâce à cette démonstration par récurrence, nous supposons désormais que nous avons $\overline{F_i} = F_i$ pour $1 \leq i \leq g$. Autrement dit, les F_i appartiennent à $\mathbb{Q}[X_1, \ldots, X_g]$. Notons H le produit semi-direct de l'énoncé. Nous pouvons le voir comme le sous-groupe de $\mathrm{Aut}_{\mathbb{Q}}(K^g)$ engendré par G et la conjugaison. Comme tel, il agit sur $K[X_1, \ldots, X_g]$ (l'algèbre symétrique de K^g) et $K[X_1, \ldots, X_g]^H = K[X_1, \ldots, X_g]^G \cap \mathbb{Q}[X_1, \ldots, X_g] = \mathbb{Q}[F_1, \ldots, F_g]$ par ce qui précède. Nous avons donc une extension galoisienne de groupe H d'un corps de fractions rationnelles : $K(X_1, \ldots, X_g)/\mathbb{Q}(F_1, \ldots, F_g)$. Par le théorème d'irréductibilité de Hilbert (voir chapitre 12 de [FJ]), il existe des éléments $a_i \in \mathbb{Q}$ tels que $K[X_1, \ldots, X_g]/(F_1 - a_1, \ldots, F_g - a_g)$ est une extension galoisienne L de $\mathbb{Q}$ avec $\mathrm{Gal}(L/\mathbb{Q}) \simeq H$. Ce corps L contient $K = K[F_1, \ldots, F_g]/(F_1 - a_1, \ldots, F_g - a_g)$ et $\mathrm{Gal}(L/K) \simeq G$ par spécialisation de l'extension $K(X_1, \ldots, X_g)/K(F_1, \ldots, F_g)$. $\square$

Nous en déduisons une construction de variétés abéliennes comme $\mathbb{Q}$-formes de puissances de courbes elliptiques sur $\mathbb{Q}$.

Proposition 2.2 *Soient K un corps quadratique imaginaire dont l'anneau des entiers $\mathcal{O}_K$ est principal, g et g' des entiers naturels non nuls puis $G \subset \mathrm{GL}_g(K)$ et $G' \subset \mathrm{GL}_{g'}(K)$ deux sous-groupes finis stables par conjugaison et engendrés par des pseudo-réflexions. Nous notons $\pi\colon \mathrm{GL}_g(K) \to \mathrm{PGL}_g(K)$ et $\pi'\colon \mathrm{GL}_{g+g'}(K) \to \mathrm{PGL}_{g+g'}(K)$ les morphismes quotients naturels. Si E est une courbe elliptique sur $\mathbb{Q}$ vérifiant $\mathrm{End}E_{\overline{\mathbb{Q}}} \simeq \mathcal{O}_K$ alors il existe deux variétés abéliennes A et B sur $\mathbb{Q}$ telles que*

(1) $A_{\overline{\mathbb{Q}}} \simeq E^g_{\overline{\mathbb{Q}}}$ *et* $B_{\overline{\mathbb{Q}}} \simeq E^{g'}_{\overline{\mathbb{Q}}}$ *;*
(2) $[\mathbb{Q}_A : \mathbb{Q}] = 2\mathrm{Card}\pi(G)$ *;*
(3) $[\mathbb{Q}_{A,B} : \mathbb{Q}] = 2\mathrm{Card}\pi'(G \times G')$.

Démonstration. La proposition précédente appliquée au groupe G fournit une extension L de K munie d'un isomorphisme $\lambda\colon \mathrm{Gal}(L/K) \to G$ et nous notons $\gamma \in \mathrm{Gal}(L/\mathbb{Q})$ un élément d'ordre 2 tel que $\mathrm{Gal}(L/\mathbb{Q})$ soit le produit semi-direct de $\mathrm{Gal}(L/K)$ par le sous-groupe $\{\mathrm{id}, \gamma\}$. Par construction, cela signifie $\lambda(\gamma\sigma\gamma) = \overline{\lambda(\sigma)}$ pour tout $\sigma \in \mathrm{Gal}(L/K)$. Maintenant la principalité de $\mathcal{O}_K$, en plus d'assurer l'existence de E (voir le théorème II.4.3(b) de [S2]), montre que le sous-$\mathcal{O}_K$-module de type fini $G \cdot \mathcal{O}_K^g$ de K^g est libre et par conséquent qu'il existe $N \in \mathrm{GL}_g(K)$ avec $G \cdot \mathcal{O}_K^g = N \cdot \mathcal{O}_K^g$. Comme G est stable par conjugaison, nous avons aussi $G \cdot \mathcal{O}_K^g = \overline{N} \cdot \mathcal{O}_K^g$. Nous en déduisons $N^{-1}GN \cdot \mathcal{O}_K^g = N^{-1}G(G \cdot \mathcal{O}_K^g) = N^{-1}G \cdot \mathcal{O}_K^g = \mathcal{O}_K^g$ et de même $N^{-1}G\overline{N} \cdot \mathcal{O}_K^g = \mathcal{O}_K^g$ ce qui s'écrit $N^{-1}GN \subset \mathrm{GL}_g(\mathcal{O}_K)$ et $N^{-1}G\overline{N} \subset \mathrm{GL}_g(\mathcal{O}_K)$. Nous savons en outre que les endomorphismes de $E_{\overline{\mathbb{Q}}}$ sont définis sur K (voir le théorème II.2.2(b) de [S2]) donc $\mathrm{End}E_K = \mathrm{End}E_L = \mathrm{End}E_{\overline{\mathbb{Q}}} \simeq \mathcal{O}_K$. Nous fixons un tel isomorphisme, ce qui nous autorise à identifier $\mathrm{GL}_g(\mathcal{O}_K)$ et $\mathrm{GL}_g(\mathrm{End}E_L) = \mathrm{Aut}(E_L^g)$. Définissons alors une application

$$c\colon \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E_L^g)$$

en posant $c(\sigma) = N^{-1}\lambda(\sigma)N$ et $c(\gamma\sigma) = N^{-1}\overline{\lambda(\sigma)}\,\overline{N}$ lorsque $\sigma \in \mathrm{Gal}(L/K)$. Ceci a un sens par le choix de N. Grâce à la formule $\lambda(\gamma\sigma\gamma) = \overline{\lambda(\sigma)}$, nous vérifions que, pour $\sigma, \tau \in \mathrm{Gal}(L/K)$, nous avons : $c(\sigma\tau) = c(\sigma)c(\tau)$, $c(\gamma\sigma\tau) = c(\gamma\sigma)\overline{c(\tau)}$, $c(\gamma\sigma\gamma\tau) = c(\gamma\sigma)\overline{c(\gamma\tau)}$ et $c(\sigma\gamma\tau) = c(\sigma)c(\gamma\tau)$. Comme $\sigma \in \mathrm{Gal}(L/K)$ agit trivialement sur $\mathrm{Aut}(E_L^g)$ tandis que γ agit par conjugaison, ces quatre formules se réduisent au fait que, si σ et τ varient à présent dans $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(L/K) \cup \gamma\mathrm{Gal}(L/K)$, nous avons toujours

$$c(\sigma\tau) = c(\sigma)\sigma(c(\tau)).$$

Autrement dit, c est un 1-cocycle. Un procédé classique lui associe alors une $\mathbb{Q}$-forme de E^g : c'est la construction utilisée au paragraphe 6 de [GK], décrite page 131 de [Se] ou plus en détails pages 18–22 de [Sa]. De manière précise, nous obtenons une variété abélienne A sur $\mathbb{Q}$ munie d'un isomorphisme $\varphi\colon A_L \to E_L^g$ tel que si $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ l'automorphisme $\varphi \circ \sigma(\varphi)^{-1}$ de E_L^g coïncide avec $c(\sigma)$. Si maintenant $\psi \in \mathrm{End}A_L$, nous avons pour $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$

$$\begin{aligned} \sigma(\psi) &= \sigma(\varphi)^{-1} \circ \sigma(\varphi \circ \psi \circ \varphi^{-1}) \circ \sigma(\varphi) \\ &= \varphi^{-1} \circ c(\sigma) \circ \sigma(\varphi \circ \psi \circ \varphi^{-1}) \circ c(\sigma)^{-1} \circ \varphi. \end{aligned}$$

En notant $M = \varphi \circ \psi \circ \varphi^{-1} \in \mathrm{End}E_L^g = M_g(\mathcal{O}_K)$, nous pouvons écrire $\sigma(\psi) = \psi \iff M = c(\sigma)\sigma(M)c(\sigma)^{-1}$. Par suite, σ agit trivialement sur $\mathrm{End}A_L$ si et seulement si cette relation matricielle est vraie pour tout $M \in M_g(\mathcal{O}_K)$. C'est impossible si $\sigma \notin \mathrm{Gal}(L/K)$ car dans ce cas $\sigma(M) = \overline{M}$ et $M = xI$ avec $x \in \mathcal{O}_K \setminus \mathbb{Z}$ conduit à la contradiction $x = \overline{x}$. Lorsque $\sigma \in \mathrm{Gal}(L/K)$ nous trouvons l'égalité $Mc(\sigma) = c(\sigma)M$ qui signifie que $c(\sigma)$ — ou encore $\lambda(\sigma)$ — est central. Tous les endomorphismes de $A_{\overline{\mathbb{Q}}}$ proviennent de A_L donc $\mathbb{Q}_A \subset L$ et l'argument

qui précède montre $\mathrm{Gal}(L/\mathbb{Q}_A) = \{\sigma \in \mathrm{Gal}(L/K) \mid \pi(\lambda(\sigma)) = 1\}$. En particulier, $K \subset \mathbb{Q}_A$ et nous avons un isomorphisme $\mathrm{Gal}(\mathbb{Q}_A/K) \simeq \pi(G)$. L'assertion (2) est donc établie. Pour le reste de l'énoncé, nous constatons que tout ce qui vient d'être fait à partir du groupe G peut tout aussi bien l'être à partir de G' ou du produit $G \times G' \subset \mathrm{GL}_{g+g'}(K)$ qui vérifient les mêmes hypothèses. Mieux, si nous partons de l'extension L'' de K donnée par la proposition 2.1 pour le groupe $G \times G'$, alors la sous-extension de L''/K fixée par l'image de $0 \times G' \subset G \times G'$ dans l'isomorphisme $\mathrm{Gal}(L''/K) \simeq G \times G'$ satisfait la conclusion de la proposition 2.1 pour G. Nous pouvons donc supposer que l'extension L utilisée ci-dessus était choisie ainsi. De même, nous notons L' le sous-corps de L'' fixé par l'image de $G \times 0$. Il n'y a pas non plus de restriction à supposer que l'élément $\gamma \in \mathrm{Gal}(L/\mathbb{Q})$ s'étend en un automorphisme d'ordre 2 de L'' encore noté γ. Notons $N' \in \mathrm{GL}_{g'}(K)$ une matrice telle que $G' \cdot \mathcal{O}_K^{g'} = N' \cdot \mathcal{O}_K^{g'}$. Nous lui associons comme plus haut un 1-cocycle c' et donc une variété abélienne B sur $\mathbb{Q}$ munie d'un isomorphisme $\varphi' \colon B_L \to E_L^{g'}$ tel que $c'(\sigma) = \varphi' \circ \sigma(\varphi')^{-1}$ pour $\sigma \in \mathrm{Gal}(L'/\mathbb{Q})$. Considérons à présent $\sigma \in \mathrm{Gal}(L''/\mathbb{Q})$ et $\psi \in \mathrm{Hom}(A_{L''}, B_{L''})$. Nous calculons

$$\begin{aligned} \sigma(\psi) &= \sigma(\varphi')^{-1} \circ \sigma(\varphi' \circ \psi \circ \varphi^{-1}) \circ \sigma(\varphi) \\ &= (\varphi')^{-1} \circ c'(\sigma_{|L'}) \circ \sigma(\varphi' \circ \psi \circ \varphi^{-1}) \circ c(\sigma_{|L})^{-1} \circ \varphi. \end{aligned}$$

La matrice $M = \varphi' \circ \psi \circ \varphi^{-1}$ appartient à $\mathrm{Hom}(E_{L''}^g, E_{L''}^{g'}) \simeq M_{g',g}(\mathcal{O}_K)$ et $\sigma(\psi) = \psi \iff M = c'(\sigma_{|L'})\sigma(M)c(\sigma_{|L})^{-1}$. Si cette dernière relation vaut pour tout M alors $\sigma_{|K} = \mathrm{id}_K$ car sinon on obtient une contradiction en l'appliquant à $M \neq 0$ et xM avec $x \in \mathcal{O}_K \setminus \mathbb{Z}$. D'autre part, c'est un exercice élémentaire de montrer que si $P \in \mathrm{GL}_g(K)$ et $P' \in \mathrm{GL}_{g'}(K)$ vérifient $MP = P'M$ pour tout $M \in M_{g',g}(K)$ alors il existe $x \in K^\times$ tel que $P = xI$ et $P' = xI'$. Nous en déduisons que σ agit trivialement sur $\mathrm{Hom}(A_{L''}, B_{L''}) = \mathrm{Hom}(A_{\overline{\mathbb{Q}}}, B_{\overline{\mathbb{Q}}})$ si et seulement si σ appartient à l'image de $\mathrm{Ker}\pi' \subset G \times G'$ dans l'isomorphisme $\mathrm{Gal}(L''/\mathbb{Q}) \simeq G \times G'$. Nous en tirons bien $\mathrm{Gal}(\mathbb{Q}_{A,B}/K) \simeq \pi'(G \times G')$ et la proposition est établie. □

Il nous reste à décrire les groupes auxquels nous appliquerons ceci.

Lemme 2.3 *Soit (ℓ, g, n) l'un des triplets suivants d'entiers naturels non nuls :*
(1) $(6, g, 3f(g))$ *pour* $g \neq 2$,
(2) $(6, 2, 3f(2)/2)$,
(3) $(4, g, 2f(g))$ *pour* $1 \leq g \leq 2$.
Alors il existe un sous-groupe de cardinal n de $\mathrm{GL}_g(\mathbb{Q}(\mu_\ell))$ contenant $\mu_\ell I$, stable par conjugaison et engendré par des pseudo-réflexions.

Démonstration. Nous nous basons sur la classification des sous-groupes finis engendrés par des pseudo-réflexions de $\mathrm{GL}_g(\mathbb{C})$ établie par Shephard et Todd : voir [ST] et, en particulier, la table VII page 301 où les groupes sont numérotés. En notant ST_m le groupe de numéro m, ceux dont nous aurons besoin sont $\mathrm{ST}_2(\ell, 1, g)$, ST_8 ($g = 2$), ST_{32} ($g = 4$) et ST_{34} ($g = 6$). La table de Shephard et Todd assure que ces groupes sont engendrés par des pseudo-réflexions, donne leur cardinal ainsi que le cardinal de leur image dans $\mathrm{PGL}_g(\mathbb{C})$. Cette information permet de calculer l'intersection du groupe avec $\mathbb{C}^\times I$ et donc de vérifier qu'il contient $\mu_\ell I$. Notre tâche est donc de contrôler que ces groupes sont à coefficients dans $\mathbb{Q}(\mu_\ell)$ et stables par conjugaison, ce que nous faisons cas par cas. Le groupe $\mathrm{ST}_2(\ell, 1, g) \simeq \mu_\ell \wr \mathfrak{S}_g$ est formé des matrices ayant un unique coefficient non nul par colonne, choisi dans μ_ℓ. Il est donc clairement contenu dans $\mathrm{GL}_g(\mathbb{Q}(\mu_\ell))$ et stable par conjugaison. Son cardinal vaut $\ell^g g!$ et nous en déduisons donc la propriété souhaitée pour les triplets $(6, g, 3f(g))$ si $g \notin \{2, 4, 6\}$, $(6, 2, 3f(2)/2)$ et $(4, 1, 2f(1))$. Le groupe ST_8 est

engendré par (voir page 281 de [ST])

$$S = \frac{i-1}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \qquad \text{et} \qquad T = \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix}.$$

Nous avons $\mathrm{ST}_8 \subset \mathrm{GL}_2(\mathbb{Q}(\mu_4))$, la table prouve $\mu_4 I \subset \mathrm{ST}_8$ et les relations $\overline{T} = T^3 \in \mathrm{ST}_8$, $\overline{S} = iS \in \mathrm{ST}_8$ donnent la stabilité par conjugaison. Comme $\mathrm{Card}\mathrm{ST}_8 = 96 = 2f(2)$, nous avons le résultat pour le triplet $(4, 2, 2f(2))$. De son côté, ST_{32} est engendré par 4 matrices R_1, R_2, R_3, R_4 de $\mathrm{GL}_4(\mathbb{Q}(\mu_6))$ données en (10.5) page 297 de [ST]. Ces matrices sont unitaires et symétriques donc vérifient $\overline{R_h} = R_h^{-1} \in \mathrm{ST}_{32}$ pour $1 \leq h \leq 4$. La table donne $\mu_6 I \subset \mathrm{ST}_{32}$ et $\mathrm{Card}\mathrm{ST}_{32} = 216 \cdot 6! = 3f(4)$ ce qui nous donne la conclusion pour $(6, 4, 3f(4))$. Enfin le triplet $(6, 6, 3f(6))$ se traite de même avec ST_{34} de cardinal $108 \cdot 9! = 3f(6)$ pourvu que nous montrions $\mathrm{ST}_{34} \subset \mathrm{GL}_6(\mathbb{Q}(\mu_6))$ et $\mathrm{ST}_{34} = \overline{\mathrm{ST}_{34}}$. Or, d'après la description page 298 de [ST] du groupe qu'ils notent $[3\ 1; 2]^3$ ou $[2\ 1; 3]^3$ (voir l'égalité au bas de la page 294), ST_{34} est engendré par les réflexions autour des six hyperplans $x_1 = x_2$, $x_2 = x_3$, $x_3 = x_4$, $x_4 = x_5$, $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 0$ et $x_1 = jx_2$ (ici $j^2 + j + 1 = 0$). Les matrices $P_1, \ldots, P_6$ de ces réflexions sont visiblement à coefficients dans $\mathbb{Q}(j)$ et les cinq premières sont même à coefficients dans $\mathbb{Q}$ donc coïncident chacune avec leur conjuguée. Pour la dernière, on vérifie très facilement $\overline{P_6} = P_6 P_1 P_6 \in \mathrm{ST}_{34}$. □

La combinaison de nos deux derniers énoncés entraîne assez directement l'optimalité des théorèmes de l'introduction. Pour une courbe elliptique E sur $\mathbb{Q}$, notons $\mathcal{A}_g(E)$ l'ensemble des variétés abéliennes A sur $\mathbb{Q}$ telles que $A_{\overline{\mathbb{Q}}} \simeq E^g_{\overline{\mathbb{Q}}}$.

Proposition 2.4 *Soient E et E' les courbes elliptiques sur $\mathbb{Q}$ de modèles de Weierstrass respectifs $y^2 = x^3 - 1$ et $y^2 = x^3 - x$. Soient g et g' deux entiers naturels non nuls.*

(1) *Si $g \neq 2$, il existe $A \in \mathcal{A}_g(E)$ avec $[\mathbb{Q}_A : \mathbb{Q}] = f(g)$ et $\mu_A[\mathbb{Q}_A : \mathbb{Q}] = 6f(g)$.*
(2) *Il existe $A \in \mathcal{A}_2(E')$ avec $[\mathbb{Q}_A : \mathbb{Q}] = f(2)$ et $\mu_A[\mathbb{Q}_A : \mathbb{Q}] = 4f(2)$.*
(3) *Si $\max(g, g') \neq 2$, il existe $A \in \mathcal{A}_g(E)$ et $B \in \mathcal{A}_{g'}(E)$ avec $[\mathbb{Q}_{A,B} : \mathbb{Q}] = \mathcal{F}(g, g')$.*
(4) *Si $\max(g, g') = 2$, il existe $A \in \mathcal{A}_g(E')$ et $B \in \mathcal{A}_{g'}(E')$ avec $[\mathbb{Q}_{A,B} : \mathbb{Q}] = \mathcal{F}(g, g')$.*
(5) *Il existe $C \in \mathcal{F}_4(E)$ telle que si $A = E' \times C$ alors $\mu_A[\mathbb{Q}_A : \mathbb{Q}] = 8f(5)$.*

Démonstration. Il est fort bien connu que $\mathrm{End}E_{\overline{\mathbb{Q}}} \simeq \mathbb{Z}[\mu_6]$ et $\mathrm{End}E'_{\overline{\mathbb{Q}}} \simeq \mathbb{Z}[\mu_4]$ (comme cela se vérifie très facilement à l'aide des automorphismes $(x, y) \mapsto (jx, y)$ de E et $(x, y) \mapsto (-x, iy)$ de E'). (1) Si $G \subset \mathrm{GL}_g(\mathbb{Q}(\mu_6))$ est associé par le lemme 2.3 au triplet $(6, g, 3f(g))$ alors la proposition 2.2 fournit une variété $A \in \mathcal{A}_g(E)$ avec $[\mathbb{Q}_A : \mathbb{Q}] = 2\mathrm{Card}\pi(G) = (1/3)\mathrm{Card}G = f(g)$ en utilisant $\mu_6 I \subset G$. De plus dans ce cas $Z(\mathrm{End}A_{\overline{\mathbb{Q}}}) = Z(M_g(\mathbb{Z}[\mu_6])) = \mathbb{Z}[\mu_6]$ donc $\mu_A = 6$. (2) Le raisonnement est identique avec le sous-groupe de $\mathrm{GL}_2(\mathbb{Q}(\mu_4))$ associé à $(4, 2, 2f(2))$. (3) Supposons d'abord $2 \notin \{g, g'\}$. Nous choisissons $G \subset \mathrm{GL}_g(\mathbb{Q}(\mu_6))$ et $G' \subset \mathrm{GL}_{g'}(\mathbb{Q}(\mu_6))$ associés aux triplets $(6, g, 3f(g))$ et $(6, g', 3f(g'))$. Avec les notations de la proposition 2.2, $\mathrm{Card}\pi(G \times G') = (1/6)\mathrm{Card}(G \times G') = (3/2)f(g)f(g')$ d'où le résultat. Lorsque $g = 2 < g'$, nous utilisons les triplets $(6, 2, (3/2)f(2))$, $(6, g', 3f(g'))$ et symétriquement pour $g > 2 = g'$. (4) Employer $(4, g, 2f(g))$ et $(4, g', 2f(g'))$. (5) On note $G \subset \mathrm{GL}_4(\mathbb{Q}(\mu_6))$ associé à $(6, 4, 3f(4))$. La proposition 2.2 avec $G' = G$ produit deux variétés abéliennes $C, C' \in \mathcal{A}_4(E)$ qui satisfont $[\mathbb{Q}_C : \mathbb{Q}] = [\mathbb{Q}_{C'} : \mathbb{Q}] = f(4)$ et $\mu_C = \mu_{C'} = 6$. On vérifie de plus sur la construction $\mathbb{Q}_C \cap \mathbb{Q}_{C'} = \mathbb{Q}(\mu_6)$ donc, quitte à échanger C et C' si besoin, on peut supposer $\mathbb{Q}_{E'} = \mathbb{Q}(\mu_4) \not\subset \mathbb{Q}_C$. Pour $A = E' \times C$, on a alors $\mu_A = \mu_C \mu_{E'} = 24$ et $\mathbb{Q}_A = \mathbb{Q}_C \mathbb{Q}_{E'}$ donc $\mu_A[\mathbb{Q}_A : \mathbb{Q}] = 48[\mathbb{Q}_C : \mathbb{Q}] = 48f(4) = 8f(5)$. □

3 Réduction du problème

Grâce aux résultats de la partie précédente, il reste seulement à établir les majorations des théorèmes 1.1, 1.2 et 1.4. Ici, nous allons ramener celles-ci à une série d'inégalités où n'interviennent plus de variétés abéliennes (voir le théorème 3.8). Le théorème ci-dessous reprend les estimations à montrer avec une précision technique dans un cas particulier qui sera nécessaire pour raisonner par récurrence. Dans toute cette partie, K désigne un corps de caractéristique nulle et nous notons E_0 la courbe elliptique sur $\overline{K}$ de modèle de Weierstrass $y^2 = x^3 - 1$ (donc telle que $\mathrm{End}E_0 \simeq \mathbb{Z}[\mu_6]$).

Théorème 3.1 *Soient A et B deux variétés abéliennes non nulles sur K de dimensions respectives g et h. Nous avons*
(M1) $[K_A : K] \leq f(g)$;
(M2) $\mu_A[K_A : K] \leq \omega(g)$;
(M3) $\mu_A[K_A : K] \leq (2/3)\omega(4)$ *si* $g = 4$ *et* $\mathrm{Hom}(E_0, A_{\overline{K}}) = 0$;
(M4) $[K_{A,B} : K] \leq \mathcal{F}(g, h)$.

Commençons par remarquer que, dans la détermination des corps K_A et $K_{A,B}$, nous disposons d'une certaine liberté pour varier A et B.

Lemme 3.2 *Soient A, B, C et D des variétés abéliennes sur K telles que C est isogène à A et D à B. Alors $K_A = K_C$ et $K_{A,B} = K_{C,D}$. De plus, il existe une sous-variété abélienne A' de B telle que $A'_{\overline{K}}$ est engendrée par les images des morphismes de* $\mathrm{Hom}(A_{\overline{K}}, B_{\overline{K}})$ *et donc $K_{A,B} = K_{A,A'}$.*

Démonstration. Une isogénie entre A et C induit un isomorphisme $(\mathrm{End}A_{\overline{K}}) \otimes \mathbb{Q} \simeq (\mathrm{End}C_{\overline{K}}) \otimes \mathbb{Q}$ qui respecte l'action de $\mathrm{Gal}(\overline{K}/K)$. Or, par définition, $\mathrm{Gal}(\overline{K}/K_A)$ est le noyau de l'action de $\mathrm{Gal}(\overline{K}/K)$ sur $\mathrm{End}A_{\overline{K}}$ ou, ce qui revient au même, sur $(\mathrm{End}A_{\overline{K}}) \otimes \mathbb{Q}$. Nous avons donc $\mathrm{Gal}(\overline{K}/K_A) = \mathrm{Gal}(\overline{K}/K_C)$ puis $K_A = K_C$. L'égalité $K_{A,B} = K_{C,D}$ résulte de même d'un isomorphisme $\mathrm{Hom}(A_{\overline{K}}, B_{\overline{K}}) \otimes \mathbb{Q} \simeq \mathrm{Hom}(C_{\overline{K}}, D_{\overline{K}}) \otimes \mathbb{Q}$. Pour la dernière assertion, notons A'' la sous-variété abélienne de $B_{\overline{K}}$ engendrée par les images des éléments de $\mathrm{Hom}(A_{\overline{K}}, B_{\overline{K}})$. Comme $\mathrm{Gal}(\overline{K}/K)$ permute ces éléments, son action sur $B_{\overline{K}}$ laisse A'' stable ce qui signifie bien qu'il existe $A' \subset B$ avec $A'_{\overline{K}} = A''$. Enfin l'égalité $\mathrm{Hom}(A_{\overline{K}}, B_{\overline{K}}) = \mathrm{Hom}(A_{\overline{K}}, A'_{\overline{K}})$ fournit $K_{A,B} = K_{A,A'}$. □

Pour raisonner par récurrence, nous aurons besoin des estimations numériques suivantes.

Lemme 3.3 *Soient g, h et s trois entiers naturels non nuls tels que s divise g. Nous avons*
(N1) $3f(g)f(h) \leq f(g + h)$;
(N2) $\omega(g)\omega(h) \leq \omega(g + h)$ *si* $\{g, h\} \neq \{1, 4\}$;
(N3) $4s!f(g/s)^s \leq f(g)$ *si* $s \neq 1$;
(N4) $s!\omega(g/s)^s \leq \omega(g)$ *si* $s \neq 1$, $s \neq g$ *et* $(s, g) \neq (2, 8)$.

Démonstration. (N1) En utilisant la fonction α de l'introduction, notre inégalité se réécrit $\alpha(g)\alpha(h) \leq \binom{g+h}{h}\alpha(g + h)$. Comme $\alpha(g)\alpha(h) \leq 10$ si $(g, h) \neq (4, 4)$, il suffit de vérifier la formule pour ce couple $(4, 4)$ et les 16 couples (g, h) tels que $\binom{g+h}{h} \leq 9$. Un calcul explicite conclut. (N2) En raisonnant de même, on constate que la formule est évidente si $(g, h) \neq (4, 4)$ et $\binom{g+h}{h} \geq 14$ et l'on traite séparément les couples restants. (N3) et (N4) Lorsque $g/s \in \{1, 2, 4\}$, les majorations se vérifient

directement : par exemple, (N4) pour $g = 4s$ s'écrit $240^s s! \leq 2(4s)!$ facilement vrai pour $s \geq 3$. Dans tous les autres cas, nos inégalités découlent de

$$\left(\frac{g}{s}\right)^{s-1} \leq \frac{g!}{s!(g/s)!^s}.$$

Pour vérifier cette formule, on peut interpréter le membre de droite comme l'indice $[\mathfrak{S}_g : G]$ du sous-groupe G du groupe symétrique sur $\{1, \ldots, g\}$ formé des éléments σ qui permutent entre eux les sous-ensembles $\{ig/s + 1, \ldots, (i+1)g/s\}$ pour $0 \leq i \leq s-1$ (autrement dit $\lceil si/g \rceil = \lceil sj/g \rceil \Rightarrow \lceil \sigma(i)s/g \rceil = \lceil \sigma(j)s/g \rceil$ pour tous $1 \leq i, j \leq g$) tandis que le membre de gauche est le cardinal du sous-groupe H engendré par les $s-1$ (g/s)-cycles $(ig/s + 2 \cdots (i+1)g/s + 1)$ pour $0 \leq i \leq s-2$. On constate alors que $G \cap H = \{\mathrm{id}\}$ d'où $\mathrm{Card} H \leq [\mathfrak{S}_g : G]$. □

Nous dirons en abrégé que le théorème 3.1 vaut en dimension au plus n si son énoncé est vrai sous la condition supplémentaire $g \leq n$ (pour tout corps K). Nous traitons tout d'abord une situation produit.

Proposition 3.4 *Soit A une variété abélienne de dimension g sur K isogène à un produit $C \times D$ de deux variétés abéliennes non nulles telles que* $\mathrm{Hom}(C_{\overline{K}}, D_{\overline{K}}) = 0$. *Si le théorème 3.1 vaut en dimension au plus $g-1$ alors il vaut pour A (et toute variété B sur K).*

Démonstration. Par le lemme 3.2, nous pouvons supposer $A = C \times D$. L'hypothèse assure alors $\mathrm{End} A_{\overline{K}} = \mathrm{End} C_{\overline{K}} \times \mathrm{End} D_{\overline{K}}$ donc $K_A \subset K_C K_D$ et $\mu_A = \mu_C \mu_D$. Le théorème 3.1 pour C donne $[K_C : K] \leq f(\dim C)$ et $\mu_C [K_C : K] \leq \omega(\dim C)$ et de même pour D. L'assertion (M1) résulte de (N1) : $[K_A : K] \leq [K_C : K][K_D : K] \leq f(\dim C) f(\dim D) < f(g)$. L'assertion (M3) s'obtient par $\omega(1)\omega(3) \leq (2/3)\omega(4)$ et $\omega(2)^2 \leq (2/3)\omega(4)$. De son côté, (N2) entraîne (M2) pour A sauf si $\{\dim C, \dim D\} = \{1, 4\}$. Dans ce cas, supposons par symétrie que C est une courbe elliptique. Alors $\mu_C \in \{2, 4, 6\}$ et $[K_C : K] \leq 2$. Si $\mu_C \neq 6$, $\mu_C [K_C : K] \leq 8$ fournit $\mu_A [K_A : K] \leq 8\omega(4) = \omega(5)$. Si $\mu_C = 6$ alors $C_{\overline{K}}$ est isogène à E_0 donc $\mathrm{Hom}(E_0, D_{\overline{K}}) = 0$. Ceci entraîne $\mu_D [K_D : K] \leq (2/3)\omega(4)$ par (M3) pour D puis $\mu_A [K_A : K] \leq (2/3)\omega(4)\omega(1) = \omega(5)$. Ainsi A vérifie (M2) dans tous les cas. Considérons maintenant une autre variété abélienne B sur K de dimension h. La seconde partie du lemme 3.2 définit des sous-variétés abéliennes C' et D' de B avec $K_{C,B} = K_{C,C'}$ et $K_{D,B} = K_{D,D'}$. Ceci nous donne $K_{A,B} \subset K_{C,B} K_{D,B} = K_{C,C'} K_{D,D'}$. Notons que $C' \cap D'$ est fini : en effet, si $(C' \cap D')_{\overline{K}}$ contenait une variété abélienne simple Z, alors que le fait que $C'_{\overline{K}}$ soit engendré par les images de $\mathrm{Hom}(C_{\overline{K}}, B_{\overline{K}})$ nous permettrait de définir un morphisme surjectif $C_{\overline{K}} \to Z$ et, de même, $D_{\overline{K}} \to Z$, ce qui conduirait à un morphisme non nul $C_{\overline{K}} \to D_{\overline{K}}$ contrairement à l'hypothèse. Ainsi $\dim C' + \dim D' \leq \dim B$. Si aucune de ces dimensions n'est nulle, nous avons (avec (M4) pour (C, C') et (D, D'), (N1) et la croissance de la fonction f) :

$$\begin{aligned} [K_{A,B} : K] &\leq \mathcal{F}(\dim C, \dim C') \mathcal{F}(\dim D, \dim D') \\ &\leq 9 f(\dim C) f(\dim C') f(\dim D) f(\dim D') \\ &\leq f(g) f(h) \leq \mathcal{F}(g, h). \end{aligned}$$

Il est ensuite facile de voir que ceci vaut encore si C' ou D' est nulle. □

Nous rappelons qu'une variété abélienne A est dite isotypique si elle est isogène à la puissance d'une variété abélienne simple. Il revient au même de demander que $(\mathrm{End} A) \otimes \mathbb{Q}$ soit une $\mathbb{Q}$-algèbre simple (en effet, en général, A est isogène à un produit $\prod_{i=1}^{s} A_i^{n_i}$ où les A_i sont des variétés abéliennes simples et $n_i \geq 1$; A

est isotypique si et seulement si $s = 1$; de son côté, l'algèbre $(\mathrm{End}A) \otimes \mathbb{Q}$ est isomorphe à $\prod_{i=1}^{s} M_{n_i}((\mathrm{End}A_i) \otimes \mathbb{Q})$ qui est simple si et seulement si $s = 1$ puisque les $(\mathrm{End}A_i) \otimes \mathbb{Q}$ sont des corps). Voici la deuxième situation où le théorème 3.1 se réduit à une dimension inférieure.

Proposition 3.5 *Soit A une variété abélienne de dimension g sur K telle que $A_{\overline{K}}$ n'est pas isotypique. Si le théorème 3.1 vaut en dimension au plus $g-1$ alors il vaut pour A.*

Démonstration. Écrivons l'algèbre semi-simple $(\mathrm{End}A_{\overline{K}}) \otimes \mathbb{Q}$ comme un produit $\prod_{i=1}^{s} \mathfrak{A}_i$ d'algèbres simples sur $\mathbb{Q}$. Les éléments de la forme $(0, \ldots, 0, 1, 0, \ldots, 0)$ de ce produit forment l'unique famille $(\chi_1, \ldots, \chi_s)$ d'idempotents centraux vérifiant $\chi_1 + \cdots + \chi_s = 1$ (puisque le centre de $\mathfrak{A}_i$ est un corps de nombres ayant pour seuls idempotents 0 et 1). Par suite, l'action de $\mathrm{Gal}(\overline{K}/K)$ sur $(\mathrm{End}A_{\overline{K}}) \otimes \mathbb{Q}$ permute ces χ_i et définit donc un morphisme $\mathrm{Gal}(\overline{K}/K) \to \mathfrak{S}_s$. Fixons un entier naturel non nul N tel que $N\chi_i \in \mathrm{End}A_{\overline{K}}$ pour tout i. L'image de $N\chi_i$ est une sous-variété abélienne C_i de $A_{\overline{K}}$ telle que $(\mathrm{End}C_i) \otimes \mathbb{Q} \simeq \mathfrak{A}_i$; elle est donc isotypique. Nous savons aussi que $A_{\overline{K}}$ est isogène au produit des C_i et $\mathrm{Hom}(C_i, C_j) = 0$ si $i \neq j$. Notre hypothèse entraîne $s \neq 1$. Si l'action de $\mathrm{Gal}(\overline{K}/K)$ n'est pas transitive sur $\{\chi_1, \ldots, \chi_s\}$, il existe une partition non triviale $\{1, \ldots, s\} = J \cup J'$ avec $\sum_{i \in J} \chi_i$ et $\sum_{j \in J'} \chi_j$ fixes donc $N \sum_{i \in J} \chi_i, N \sum_{j \in J'} \chi_j \in \mathrm{End}A$ et les images C et D de ces éléments vérifient les hypothèses de la proposition 3.4 qui nous donne le résultat. Nous pouvons donc supposer que l'action est transitive. Les variétés abéliennes C_i sont conjuguées par l'action de Galois. En particulier, elles ont toutes même dimension donc s divise g et $\dim C_i = g/s$. Nous voyons aussi qu'aucune des C_i ne contient une courbe elliptique CM : en effet si E est une telle courbe (sur $\overline{K}$) alors ses conjuguées sous $\mathrm{Gal}(\overline{K}/K)$ sont des courbes CM de même type CM donc lui sont isogènes ; par suite si $i \neq j$ et si C_i contenait E alors C_j contiendrait une courbe isogène à E ce qui contredirait $\mathrm{Hom}(C_i, C_j) = 0$. Notons à présent $\mathrm{Gal}(\overline{K}/L)$ le noyau de $\mathrm{Gal}(\overline{K}/K) \to \mathfrak{S}_s$ où L est une extension de K avec $[L : K] \leq s!$. Par construction, il existe des sous-variétés D_i de A_L telles que $(D_i)_{\overline{K}} = C_i$ et A_L est isogène au produit des D_i. Par le théorème 3.1 pour les D_i (sur L) nous avons $[L_{D_i} : L] \leq f(g/s)$ et $\mu_{D_i}[L_{D_i} : L] \leq \omega(g/s)$ pour tout i. En fait, la remarque sur les courbes elliptiques CM montre que si $g/s = 1$ alors $[L_{D_i} : L] = 1$ et $\mu_{D_i} = 2$ tandis que si $g/s = 4$ par (M3) nous avons $\mu_{D_i}[L_{D_i} : L] \leq (2/3)\omega(4)$. Maintenant K_A contient L et est contenu dans le compositum des L_{D_i} donc $[K_A : K] \leq s![K_A : L] \leq s! \prod_{i=1}^{s} [L_{D_i} : L] \leq s! f(g/s)^s < f(g)$ par (N3). De plus $\mu_A = \prod_{i=1}^{s} \mu_{D_i}$ donc $\mu_A[K_A : K] \leq s!\omega(g/s)^s \leq \omega(g)$ lorsque $s \neq g$ et $(s, g) \neq (2, 8)$. Si $s = g$ nous trouvons $\mu_A[K_A : K] \leq s!2^s \leq \omega(s)$. Si $(s, g) = (2, 8)$ il vient $\mu_A[K_A : K] \leq 2!(2\omega(4)/3)^2 < \omega(8)$. L'assertion (M2) vaut donc dans tous les cas pour A. De son côté, (M3) découle de $2\omega(2)^2 < (2/3)\omega(4)$ (si $s = 2$) et $4!2^4 < (2/3)\omega(4)$ (si $s = 4$). Passons à (M4) avec B de dimension h. Par le lemme 3.2, B_L contient pour tout i une variété abélienne D'_i avec $L_{D_i, B_L} = L_{D_i, D'_i}$. Comme dans la démonstration précédente, on vérifie que la somme des $h_i = \dim D'_i$ n'excède pas h. Quitte à réordonner les indices, nous supposons $h_i = 0 \iff i > t$ pour $0 \leq t \leq s$. Alors

$$[K_{A,B} : K] \leq s! \prod_{i=1}^{t} [L_{D_i, D'_i} : L] \leq s! \prod_{i=1}^{t} \mathcal{F}(g/s, h_i) \leq s! 3^t f(g/s)^t \prod_{i=1}^{t} f(h_i).$$

Par itération de (N1) ce dernier produit vaut au plus $3^{1-t} f(h)$ donc en appliquant (N3) nous trouvons $[K_{A,B} : K] \leq (3/4) f(g) f(h) < \mathcal{F}(g, h)$ (au lieu d'introduire t il aurait aussi été possible de montrer que les h_i étaient tous égaux). $\square$

Établissons à présent le résultat auxiliaire cité dans l'introduction.

Démonstration de la proposition 1.3. Traitons tout d'abord le cas où A et B sont simples. Si $A_{\overline{K}}$ et $B_{\overline{K}}$ (qui restent simples) ne sont pas isogènes, $K_{A,B} = K$. Sinon fixons une isogénie $\varphi\colon A_{\overline{K}} \to B_{\overline{K}}$, notons D le corps gauche $(\mathrm{End}A) \otimes \mathbb{Q}$ et F son centre. L'application $\psi \mapsto \varphi \circ \psi \circ \varphi^{-1}$ donne un isomorphisme $D \to (\mathrm{End}B) \otimes \mathbb{Q}$, ce qui montre en particulier $\mu_A = \mu_B = \mu_F$. Si maintenant $\sigma \in \mathrm{Gal}(\overline{K}/K)$, l'hypothèse $K_A = K_B = K$ entraîne $\sigma(\psi) = \psi$ et $\sigma(\varphi \circ \psi \circ \varphi^{-1}) = \varphi \circ \psi \circ \varphi^{-1}$ pour tout $\psi \in D$. Par suite, $\varphi^{-1} \circ \sigma(\varphi) \in D^\times$ commute à tout ψ donc $\varphi^{-1} \circ \sigma(\varphi) \in F^\times$. De plus, si $\tau \in \mathrm{Gal}(\overline{K}/K)$, $\varphi^{-1} \circ (\sigma\tau)(\varphi) = \varphi^{-1} \circ \sigma(\varphi) \circ \sigma(\varphi^{-1} \circ \tau(\varphi)) = \varphi^{-1} \circ \sigma(\varphi) \circ \varphi^{-1} \circ \tau(\varphi)$ puisque σ agit trivialement sur D. Ainsi $\sigma \mapsto \varphi^{-1} \circ \sigma(\varphi)$ définit un morphisme de groupes $\mathrm{Gal}(\overline{K}/K) \to F^\times$ dont le noyau est $\mathrm{Gal}(\overline{K}/K_{A,B})$. En d'autres termes, le groupe fini $\mathrm{Gal}(K_{A,B}/K)$ s'injecte dans $F^\times$ donc dans le sous-groupe des racines de l'unité et nous en déduisons bien $[K_{A,B} : K] \mid \mu_F = \mathrm{pgcd}(\mu_A, \mu_B)$. Passons au cas général. Par isogénies (lemme 3.2), nous pouvons supposer $A = \prod_{i=1}^s A_i^{n_i}$ et $B = \prod_{i=1}^s B_i^{m_i}$ où les A_i et B_i sont des variétés abéliennes simples et les n_i, m_i des entiers naturels de façon que les A_i sont deux à deux non isogènes et $(A_i)_{\overline{K}}$ est isogène à $(B_i)_{\overline{K}}$ pour tout $1 \leq i \leq s$. Alors $\prod_{n_i m_i \neq 0} \mu_{A_i} \mid \mathrm{pgcd}(\mu_A, \mu_B)$ et $K_{A,B} = \prod_{n_i m_i \neq 0} K_{A_i, B_i}$ et le résultat découle du cas simple déjà traité. □

Revenons maintenant au théorème 3.1. Grâce aux propositions 3.4 et 3.5, il nous reste à examiner le cas où $A_{\overline{K}}$ est isotypique. Nous allons devoir traiter séparément le sous-cas plus délicat où $A_{\overline{K}}$ contient une courbe elliptique CM. En dehors de celui-ci, la méthode de Minkowski nous suffira c'est-à-dire que nous pourrons utiliser l'énoncé suivant qui fait seulement intervenir la fonction $\Gamma_F(\cdot)$ définie dans l'introduction. Remarquons ici que, si $F_1 \subset F$ sont des corps de nombres et g, h des entiers naturels non nuls, nous avons $\Gamma_{F_1}(g) \mid \Gamma_F(gh)$: en effet, si $\mathfrak{A}$ est une F_1-algèbre centrale simple de dimension g^2 alors $M_h(\mathfrak{A} \otimes F)$ est une F-algèbre centrale simple de dimension g^2h^2 et tout sous-groupe fini $G \subset \mathfrak{A}^\times/F_1^\times$ s'injecte (diagonalement) dans $\mathrm{GL}_h(\mathfrak{A} \otimes F)/F^\times$.

Proposition 3.6 *Soit A une variété abélienne de dimension g sur K telle que $A_{\overline{K}}$ est isotypique mais ne contient pas de courbe elliptique CM. Alors l'une des deux assertions suivantes est vraie.*

(1) *On a $\mu_A[K_A : K] \leq 2\Gamma_{\mathbb{Q}}(g)$.*
(2) *Il existe un corps CM F tel que $4 \leq [F : \mathbb{Q}] \mid 2g$ et $\mu_A[K_A : K] \leq \mu_F[F : \mathbb{Q}]\Gamma_F(2g/[F : \mathbb{Q}])$.*

Démonstration. Notons $\mathfrak{A}$ l'algèbre simple $(\mathrm{End}A_{\overline{K}}) \otimes \mathbb{Q}$, F_1 son centre et $d^2 = [\mathfrak{A} : F_1]$. L'action galoisienne sur $\mathfrak{A}$ identifie $\mathrm{Gal}(K_A/K)$ à un sous-groupe fini de $\mathrm{Aut}_{\mathbb{Q}}(\mathfrak{A})$. Comme tout automorphisme de la $\mathbb{Q}$-algèbre $\mathfrak{A}$ laisse stable son centre, nous avons une suite exacte

$$0 \longrightarrow \mathrm{Aut}_{F_1}(\mathfrak{A}) \longrightarrow \mathrm{Aut}_{\mathbb{Q}}(\mathfrak{A}) \longrightarrow \mathrm{Aut}_{\mathbb{Q}}(F_1).$$

Par le théorème de Skolem-Noether (voir page 222 de [Ja]), tout automorphisme de la F_1-algèbre centrale simple $\mathfrak{A}$ est intérieur c'est-à-dire que le morphisme de groupes $\mathfrak{A}^\times \to \mathrm{Aut}_{F_1}(\mathfrak{A})$, $x \mapsto (y \mapsto xyx^{-1})$ est surjectif. Son noyau étant $F_1^\times$, nous avons $\mathrm{Aut}_{F_1}(\mathfrak{A}) \simeq \mathfrak{A}^\times/F_1^\times$. Nous pouvons donc écrire une suite exacte

$$0 \longrightarrow G \longrightarrow \mathrm{Gal}(K_A/K) \longrightarrow G' \longrightarrow 0$$

où $G \subset \mathfrak{A}^\times/F_1^\times$ et $G' \subset \mathrm{Aut}_{\mathbb{Q}}(F_1)$ sont deux groupes finis. Nous en déduisons $[K_A : K] = (\mathrm{Card}G')(\mathrm{Card}G) \leq [F_1 : \mathbb{Q}]\Gamma_{F_1}(d)$. Par ailleurs $\mu_A = \mu_{F_1}$. Maintenant, grâce à la classification d'Albert, nous savons que F_1 est soit un corps totalement réel soit un corps CM et les relations de divisibilité en caractéristique nulle données page 202 de [Mu] et étendues immédiatement au cas isotypique montrent $[F_1 : \mathbb{Q}]d \mid g$ si

F_1 est réel et $[F_1 : \mathbb{Q}]d \mid 2g$ sinon. Distinguons alors plusieurs cas. Si $F_1 = \mathbb{Q}$, nous avons $\mu_A = 2$, $[K_A : K] \leq \Gamma_{\mathbb{Q}}(d)$ et $d \mid g$ et donc l'assertion (1) est satisfaite. Si F_1 est un corps totalement réel différent de $\mathbb{Q}$, nous posons $F = F_1(i)$ ($i^2 = -1$). Il s'agit d'un corps CM, de degré $2[F_1 : \mathbb{Q}] \geq 4$ et $[F : \mathbb{Q}] = 2[F_1 : \mathbb{Q}] \mid 2g/d \mid 2g$. Par suite, $\mu_A[K_A : K] = 2[K_A : K] \leq 2[F_1 : \mathbb{Q}]\Gamma_{F_1}(d) \leq [F : \mathbb{Q}]\Gamma_F(2g/[F : \mathbb{Q}])$ donc l'assertion (2) vaut. Supposons à présent que F_1 soit un corps CM. Si $[F_1 : \mathbb{Q}] \neq 2$, l'assertion (2) est immédiatement vérifiée avec $F = F_1$. Lorsque F_1 est un corps quadratique imaginaire, nous avons $d \mid g$ d'après la relation de divisibilité générale. Toutefois le cas $d = g$ ($[\mathfrak{A} : \mathbb{Q}] = 2g^2$) n'est possible que lorsque $A_{\overline{K}}$ est isogène à la puissance g-ème d'une courbe elliptique CM, ce que nous avons exclu. Ainsi $d \neq g$ donc $2g/d \geq 4$ et nous pouvons choisir un corps CM F contenant F_1 de degré $2g/d$ (il suffit d'adjoindre à F_1 un corps totalement réel de degré g/d). Alors $\mu_A[K_A : K] \leq \mu_{F_1}[F_1 : \mathbb{Q}]\Gamma_{F_1}(d) \leq \mu_F[F : \mathbb{Q}]\Gamma_F(d) = \mu_F[F : \mathbb{Q}]\Gamma_F(2g/[F : \mathbb{Q}])$ montre que nous avons encore (2). $\square$

Considérons finalement la situation où $A_{\overline{K}}$ est isogène à la puissance d'une courbe elliptique CM. Ici la méthode de Minkowski ne nous permettra pas de conclure et nous devons introduire un invariant plus fin que Γ. Nous posons pour cela lorsque F est un corps de nombres et g un entier

$$\Xi_F(g) = \mu_F^{-1} \sup\{\mathrm{Card} G \mid G \text{ sous-groupe fini de } \mathrm{GL}_g(F)\}.$$

Nous pouvons limiter la définition aux groupes G qui contiennent les matrices centrales ξI où ξ est une racine de l'unité. Dans ce cas, $\mu_F^{-1}\mathrm{Card} G$ est le cardinal de l'image de G dans $\mathrm{PGL}_g(F) = M_g(F)^\times/F^\times$ donc $\Xi_F(g) \mid \Gamma_F(g)$. Voyons que, dans le cas restant, nous pouvons faire apparaître Ξ_F au lieu de Γ_F quitte à faire intervenir le nombre de classes h_F du corps F.

Proposition 3.7 *Soient E une courbe elliptique CM sur $\overline{K}$, $F = (\mathrm{End} E) \otimes \mathbb{Q}$, g et h deux entiers naturels non nuls et A et B deux variétés abéliennes sur K telles que $A_{\overline{K}}$ et $B_{\overline{K}}$ sont respectivement isogènes à E^g et E^h. Alors nous avons*

(1) $\mu_A = \mu_B = \mu_F \in \{2, 4, 6\}$;

(2) $[K_A : K] \leq 2\min(\Gamma_F(g), h_F\Xi_F(g))$;

(3) $[K_{A,B} : K] \leq 2\mu_F \min(\Gamma_F(g)\Gamma_F(h), h_F\Xi_F(g)\Xi_F(h))$.

Démonstration. L'assertion (1) est élémentaire. L'inégalité $[K_A : K] \leq 2\Gamma_F(g)$ qui figure dans (2) s'obtient exactement comme dans la démonstration précédente avec $\mathfrak{A} \simeq M_g(F)$: le sous-groupe de $\mathrm{Gal}(K_A/K)$ qui agit trivialement sur le centre de $(\mathrm{End} A_{\overline{K}}) \otimes \mathbb{Q}$ s'injecte dans $\mathrm{PGL}_g(F)$ donc est de cardinal au plus $\Gamma_F(g)$. Nous pouvons l'écrire $\mathrm{Gal}(K_A/K')$ où K' est une extension de degré 1 ou 2 de K, d'où l'inégalité. Remarquons maintenant que $\mathrm{Gal}(\overline{K}/K')$ agit aussi trivialement sur le centre de $(\mathrm{End} B_{\overline{K}}) \otimes \mathbb{Q}$: en effet, nous avons deux applications canoniques

$$Z((\mathrm{End} A_{\overline{K}}) \otimes \mathbb{Q}) \longleftarrow Z((\mathrm{End} A_{\overline{K}} \times B_{\overline{K}}) \otimes \mathbb{Q}) \longrightarrow Z((\mathrm{End} B_{\overline{K}}) \otimes \mathbb{Q})$$

qui respectent l'action de Galois et qui, dans notre situation isotypique, sont des isomorphismes. Par suite, $K' \subset K_B$ et $[K_B : K'] \leq \Gamma_F(h)$. Par la proposition 1.3 sur K', il vient $[K'_{A,B} : K'] \leq \mu_F[K'_A : K'][K'_B : K'] = \mu_F[K_A : K'][K_B : K'] \leq \mu_F\Gamma_F(g)\Gamma_F(h)$ d'où l'inégalité $[K_{A,B} : K] \leq 2\mu_F\Gamma_F(g)\Gamma_F(h)$ qui apparaît dans (3). Venons-en aux relations avec Ξ. D'après le théorème II.4.3 de [S2], nous savons qu'il existe un corps de nombres L_0 de degré $2h_F$ et une courbe elliptique $\widetilde{E}$ sur L_0 telle que $(\mathrm{End}\widetilde{E}) \otimes \mathbb{Q} \simeq F$. Les deux courbes elliptiques E et $\widetilde{E}_{\overline{K}}$ sont alors isogènes. Nous disposons donc d'une isogénie $\varphi\colon A_{\overline{K}} \to \widetilde{E}^g_{\overline{K}}$. Notons $L = KL_0$. L'application

$$\begin{array}{rcl} c\colon \mathrm{Gal}(\overline{K}/L) & \longrightarrow & \mathrm{End}(\widetilde{E}^g_{\overline{K}}) \otimes \mathbb{Q} = \mathrm{End}(\widetilde{E}^g) \otimes \mathbb{Q} \simeq M_g(F) \\ \sigma & \longmapsto & \varphi \circ \sigma(\varphi)^{-1} \end{array}$$

est un morphisme de groupes car

$$c(\sigma\tau) = \varphi \circ \sigma(\varphi)^{-1} \circ \sigma(\varphi) \circ \sigma(\tau(\varphi))^{-1} = c(\sigma) \circ \sigma(c(\tau)) = c(\sigma) \circ c(\tau),$$

l'automorphisme σ agissant trivialement sur $\mathrm{End}(\widetilde{E}^g)$. Notons G l'image de c. C'est un sous-groupe de $\mathrm{GL}_g(F)$ qui est fini (puisque φ provient d'une extension finie de L). Si $\psi \in \mathrm{End}A_{\overline{K}}$, nous calculons

$$\begin{aligned} \varphi \circ \sigma(\psi) \circ \varphi^{-1} &= \varphi \circ \sigma(\varphi^{-1}) \circ \sigma(\varphi \circ \psi \circ \varphi^{-1}) \circ \sigma(\varphi) \circ \varphi^{-1} \\ &= c(\sigma) \circ (\varphi \circ \psi \circ \varphi^{-1}) \circ c(\sigma)^{-1} \end{aligned}$$

pour tout $\sigma \in \mathrm{Gal}(\overline{K}/L)$. Un tel σ agit donc trivialement sur $\mathrm{End}A_{\overline{K}}$ si $c(\sigma)$ commute aux éléments de $\varphi \circ ((\mathrm{End}A_{\overline{K}}) \otimes \mathbb{Q}) \circ \varphi^{-1} = \mathrm{End}(\widetilde{E}^g) \otimes \mathbb{Q}$. Ceci nous donne $\mathrm{Gal}(L_A/L) \simeq G/G \cap F^\times$. Comme G est fini, $G \cap F^\times = G \cap H$ où H est le groupe des racines de l'unité de $F^\times$ (vu ici comme groupe de matrices scalaires). Alors $\mathrm{Gal}(L_A/L) \simeq GH/H$ et GH est un sous-groupe fini de $\mathrm{GL}_g(F)$ donc $[L_A : L] = \mu_F^{-1}\mathrm{Card}GH \leq \Xi_F(g)$. Nous en déduisons bien $[K_A : K] \leq [L_A : L][L : K] \leq 2h_F\Xi_F(g)$ ce qui établit (2). Comme nous avons aussi $[L_B : L] \leq \Xi_F(h)$, il vient $[K_{A,B} : K] \leq [L : K][L_{A,B} : L] \leq [L_0 : \mathbb{Q}]\mu_A[L_A : L][L_B : L] \leq 2\mu_F h_F \Xi_F(g)\Xi_F(h)$ d'où (3). □

Nous pouvons finalement énoncer les majorations de Γ et Ξ qui entraîneront le théorème 3.1.

Théorème 3.8 *Soient g un entier naturel non nul et F un corps de nombres CM tel que $[F : \mathbb{Q}] \mid 2g$.*

(1) $2\Gamma_{\mathbb{Q}}(g) \leq f(g)$;
(2) $\mu_F[F : \mathbb{Q}]\Gamma_F(2g/[F : \mathbb{Q}]) \leq f(g)$ *si* $[F : \mathbb{Q}] \neq 2$;
(3) $2\min(\Gamma_F(g), h_F\Xi_F(g)) \leq f(g)$ *si* $[F : \mathbb{Q}] = 2$;
(4) $8\Xi_F(g) \leq 3f(g)$ *si* $F = \mathbb{Q}(\mu_4)$ *et* $g \geq 3$;
(5) $4\Xi_F(2) \leq f(2)$ *si* $F = \mathbb{Q}(\mu_6)$.

Ces estimations seront démontrées dans les parties 5 et 6. Ici nous en déduisons nos résultats principaux.

Lemme 3.9 *Le théorème 3.8 entraîne le théorème 3.1.*

Démonstration. Nous établissons le théorème 3.1 par récurrence sur g. Les propositions 3.4 et 3.5 montrent que nous pouvons supposer $A_{\overline{K}}$ isotypique. Plaçons-nous d'abord dans le cas où $A_{\overline{K}}$ ne contient pas de courbe elliptique CM. La proposition 3.6 combinée aux assertions (1) et (2) du théorème 3.8 fournit $\mu_A[K_A : K] \leq f(g)$ ce qui entraîne facilement (M1), (M2) et (M3). D'autre part, le lemme 3.2 nous assure de l'existence d'une sous-variété abélienne A' de B telle que $K_{A,B} = K_{A,A'}$ et de plus $A'_{\overline{K}}$, engendrée par des images de $A_{\overline{K}}$, est aussi isotypique et ne contient pas de courbe CM. Nous pouvons donc lui appliquer la proposition 3.6 et obtenir $\mu_{A'}[K_{A'} : K] \leq f(\dim A') \leq f(h)$ par croissance de f. Alors $[K_{A,B} : K] = [K_{A,A'} : K] \leq \mu_A[K_A : K][K_{A'} : K] \leq f(g)f(h) \leq \mathcal{F}(g,h)$ et (M4) est établi. Nous pouvons à présent supposer que $A_{\overline{K}}$ est isogène à la puissance d'une courbe elliptique CM. La variété $A'_{\overline{K}}$ fournie par le lemme 3.2 est aussi isogène à une puissance de cette courbe elliptique. Nous pouvons donc appliquer la proposition 3.7 en y remplaçant h par $\dim A'$ (si A' est nulle, (M4) est tautologique et nous ne considérons que A). L'assertion (2) de cette proposition combinée à l'assertion (3) du théorème 3.8 donne exactement (M1). Nous en déduisons (M2) sauf dans le cas où $\mu_F = 6$ et $g = 2$ (c'est le seul cas où $\mu_F f(g) > \omega(g)$). Dans ce cas particulier, $F = \mathbb{Q}(\mu_6)$ donc l'assertion (5) du théorème 3.8 montre $2[K_A : K] \leq f(2)$ (car $h_F = 1$) d'où

$\mu_A[K_A : K] \leq 3f(2) < 4f(2) = \omega(2)$ et (M2) vaut encore. Sous l'hypothèse de (M3), nous avons nécessairement $\mu_F \leq 4$ donc $\mu_A[K_A : K] \leq 4f(4) = (2/3)\omega(4)$ comme prévu. Pour (M4) enfin (lorsque $h' = \dim A' \neq 0$), nous distinguons suivant les valeurs de μ_F. Lorsque $\mu_F = 2$, nous utilisons $\Xi_F(\cdot) \leq \Gamma_F(\cdot)$ pour écrire

$$\min(\Gamma_F(g)\Gamma_F(h'), h_F\Xi_F(g)\Xi_F(h')) \leq \min(\Gamma_F(g), h_F\Xi_F(g)) \min(\Gamma_F(h'), h_F\Xi_F(h'))$$

et donc l'assertion (3) de la proposition 3.7 jointe à l'assertion (3) du théorème 3.8 nous fournit

$$[K_{A,B} : K] = [K_{A,A'} : K] \leq f(g)f(h') \leq f(g)f(h) \leq \mathcal{F}(g,h).$$

Si au contraire μ_F vaut 4 ou 6, nous avons respectivement $F = \mathbb{Q}(\mu_4)$ ou $F = \mathbb{Q}(\mu_6)$ donc $h_F = 1$ dans les deux cas. Les assertions (3) de la proposition 3.7 et du théorème 3.8 s'écrivent donc ici $[K_{A,B} : K] \leq 2\mu_F\Xi_F(g)\Xi_F(h')$, $2\Xi_F(g) \leq f(g)$ et $2\Xi_F(h') \leq f(h')$. Si $2 \notin \{g, h'\}$, nous trouvons $[K_{A,B} : K] \leq (\mu_F/2)f(g)f(h') \leq 3f(g)f(h') = \mathcal{F}(g,h')$. Si $\mu_F = 6$ et $2 \in \{g, h'\}$ nous utilisons l'assertion (5) du théorème 3.8 au lieu de (3) pour gagner un facteur 2 et avoir encore $[K_{A,B} : K] \leq (3/2)f(g)f(h') \leq \mathcal{F}(g,h')$. Si $\mu_F = 4$ et $\max(g,h') = 2$, l'inégalité précédente était $[K_{A,B} : K] \leq 2f(g)f(h') = \mathcal{F}(g,h')$. Enfin, lorsque $\mu_F = 4$ et $\min(g,h') = 2 < \max(g,h')$, nous utilisons (4) pour ce maximum afin de gagner un facteur 3/4 qui conduit à $[K_{A,B} : K] \leq (3/2)f(g)f(h') = \mathcal{F}(g,h')$. Ainsi nous avons $[K_{A,B} : K] \leq \mathcal{F}(g,h')$ dans tous les cas et nous obtenons (M4) en remarquant que $\mathcal{F}(g,h') \leq \mathcal{F}(g,h)$: c'est clair si $h' = h$ et sinon cela découle de $6f(h') \leq f(h)$, conséquence de (N1). □

Le reste du texte est donc consacré à la démonstration du théorème 3.8 (où les variétés abéliennes ont disparu). Nous commençons dans la partie suivante par un calcul exact de Γ.

4 Méthode de Minkowski

Dorénavant, K désigne un corps de nombres et g un entier naturel non nul. Nous allons donner des expressions exactes pour $\Gamma_K(g)$ et cinq autres quantités associées au couple (K, g) que nous introduisons maintenant. Pour cela, notons $\mathcal{C}_g(K)$ l'ensemble des K-algèbres centrales simples de dimension g^2 et, lorsque G est un groupe, $\mathcal{G}(G)$ l'ensemble de ses sous-groupes finis. Nous posons alors

$$\Gamma_K(g) = \mathrm{ppcm}\{\mathrm{Card}G \mid G \in \mathcal{G}(\mathfrak{A}^\times/K^\times),\ \mathfrak{A} \in \mathcal{C}_g(K)\},$$

$$\Gamma'_K(g) = \mu_K^{-1}\mathrm{ppcm}\{\mathrm{Card}G \mid G \in \mathcal{G}(\mathfrak{A}^\times),\ \mathfrak{A} \in \mathcal{C}_g(K)\},$$

$$\Delta_K(g) = \mathrm{ppcm}\{\mathrm{Card}G \mid G \in \mathcal{G}(\mathrm{PGL}_g(K))\},$$

$$\Delta'_K(g) = \mu_K^{-1}\mathrm{ppcm}\{\mathrm{Card}G \mid G \in \mathcal{G}(\mathrm{GL}_g(K))\},$$

$$\Theta_K(g) = \sup_{N\geq 1} \mathrm{pgcd}\{\mathrm{Card}\mathrm{PGL}_g(\mathcal{O}_K/\mathfrak{p}) \mid N_{K/\mathbb{Q}}(\mathfrak{p}) \geq N\},$$

$$\Theta'_K(g) = \mu_K^{-1} \sup_{N\geq 1} \mathrm{pgcd}\{\mathrm{Card}\mathrm{GL}_g(\mathcal{O}_K/\mathfrak{p}) \mid N_{K/\mathbb{Q}}(\mathfrak{p}) \geq N\}$$

où, dans les deux derniers cas, $\mathfrak{p}$ parcourt les idéaux premiers de $\mathcal{O}_K$ de norme au moins N. Les valeurs qui nous intéressent ici sont $\Gamma_K(g)$ et $\Delta'_K(g)$ (comme majorant de $\Xi_K(g)$), $\Gamma'_K(g)$ et $\Delta_K(g)$ leur sont étroitement liés tandis que $\Theta_K(g)$ et $\Theta'_K(g)$ servent au calcul, suivant le principe de la méthode de Minkowski (réduction modulo $\mathfrak{p}$, voir lemme 4.6). Nous verrons qu'en fait ces six quantités ne diffèrent qu'au plus par des puissances de 2.

Le théorème initial de Minkowski en 1887 donne la valeur de $\Delta'_{\mathbb{Q}}(g)$ (voir le théorème 1 de [GL]) tandis qu'un résultat ultérieur de Schur en 1905 détermine plus généralement $\Delta'_K(g)$ et $\Gamma'_K(g)$. Rappelons les notations nécessaires pour l'énoncer (voir le paragraphe 5.3 de [GL]). Pour un nombre premier ℓ, nous notons $\mu_{\ell^\infty} = \bigcup_{m\geq 1}\mu_{\ell^m}$ le groupe des racines de l'unité de $\overline{\mathbb{Q}}$ d'ordre une puissance de ℓ. Nous introduisons alors le corps $K^{(\ell)} = K \cap \mathbb{Q}(\mu_{\ell^\infty})$ et les entiers $m(K,\ell) = \min\{m \geq 1 \mid K^{(\ell)} \subset \mathbb{Q}(\mu_{\ell^m}),\ \ell^m \neq 2\}$, $t(K,\ell) = [\mathbb{Q}(\mu_{\ell^{m(K,\ell)}}) : K^{(\ell)}]$ (notre convention diffère légèrement de celle de [GL] lorsque $\ell = 2$ et $K^{(2)} = \mathbb{Q}$ mais on vérifie que cela ne change pas l'expression qui suit). La borne de Schur s'écrit

$$S(g,K) = 2^{g-[g/t(K,2)]} \prod_{\ell \text{ premier}} \ell^{m(K,\ell)[g/t(K,\ell)]} \left(\left[\frac{g}{t(K,\ell)}\right]!\right)_\ell$$

où, ici et dans toute la suite, $[x]$ désigne la partie entière d'un réel et $n_\ell = \ell^{v_\ell(n)}$ la ℓ-partie d'un entier naturel n.

Théorème 4.1 *Nous avons* $\Gamma'_K(g) = \Delta'_K(g) = \mu_K^{-1}S(g,K)$.

Pour déduire ceci du résultat de Schur (le théorème 14 de [GL]), il convient de plonger $\mathfrak{A} \in \mathcal{C}_g(K)$ dans $\mathfrak{A}\otimes_K \mathbb{C} \simeq M_g(\mathbb{C})$ donc $\mathfrak{A}^\times$ dans $\mathrm{GL}_g(\mathbb{C})$ et de constater que la trace d'un élément de $\mathfrak{A} \subset M_g(\mathbb{C})$ coïncide avec sa trace réduite dans l'algèbre $\mathfrak{A}/K$ donc appartient à K. Nous ne détaillons pas ceci car nous allons en fait redémontrer le théorème 4.1 au cours du calcul de $\Gamma_K(g)$ et $\Delta_K(g)$. Comme nous l'avons dit, nous employons pour cela la méthode de Minkowski dans l'esprit de la partie 5 de [GL], en la complétant en $\ell = 2$.

Le résultat principal de cette partie est le suivant.

Théorème 4.2 *Si le corps* $K^{(2)}$ *n'est pas totalement réel, alors* $\Gamma_K(g) = \Gamma'_K(g) = \Delta_K(g) = \Delta'_K(g) = \Theta_K(g) = \Theta'_K(g)$. *S'il est totalement réel,* $\Theta_K(g) = \Theta'_K(g) = 2^{[g/2]}\Delta'_K(g) = 2^{[g/2]}\Gamma'_K(g)$ *et, pour* g *impair,* $\Gamma_K(g) = \Delta_K(g) = \Gamma'_K(g)$ *tandis que, pour* g *pair,* $\Gamma_K(g) = \Delta_K(g) = 2\Gamma'_K(g)$.

Nous démontrons maintenant simultanément les théorèmes 4.1 et 4.2 à l'aide d'une série de résultats intermédiaires dont le premier est très élémentaire.

Lemme 4.3 *Nous avons* $\Delta'_K(g) \mid \Gamma'_K(g) \mid \Gamma_K(g)$ *et* $\Delta'_K(g) \mid \Delta_K(g) \mid \Gamma_K(g)$.

Démonstration. Les divisibilités $\Delta \mid \Gamma$ et $\Delta' \mid \Gamma'$ traduisent simplement le fait que $M_g(K)$ est une K-algèbre centrale simple, $M_g(K)^\times = \mathrm{GL}_g(K)$ et $\mathrm{GL}_g(K)/K^\times = \mathrm{PGL}_g(K)$. Pour voir $\Gamma' \mid \Gamma$, on note que tout $G \in \mathcal{G}(\mathfrak{A}^\times)$ ($\mathfrak{A} \in \mathcal{C}_g(K)$) est contenu dans un groupe fini $G' \in \mathcal{G}(\mathfrak{A}^\times)$ tel que $G' \cap K^\times$ est égal au groupe des racines de l'unité de K de cardinal μ_K (il suffit de choisir G' engendré par G et ce groupe de racines qui est central). Nous pouvons donc ajouter librement cette condition dans la définition de $\Gamma'_K(g)$ et ainsi $\Gamma'_K(g)$ est le ppcm des $\mu_K^{-1}\mathrm{Card}G' = \mathrm{Card}(G'/G' \cap K^\times)$ pour les tels G'. Comme $G'/G' \cap K^\times \in \mathcal{G}(\mathfrak{A}^\times/K^\times)$, nous avons bien $\Gamma'_K(g) \mid \Gamma_K(g)$ et de même $\Delta'_K(g) \mid \Delta_K(g)$ en nous limitant à $\mathfrak{A} = M_g(K)$. □

Nous aurons besoin des précisions suivantes sur les corps $K^{(\ell)}$ (voir aussi page 11 de [GL]).

Lemme 4.4 *Soit* ℓ *un nombre premier.*

(1) *Si* $\ell \neq 2$ *alors* $t(K,\ell) \mid \ell - 1$.

(2) *Si* $\ell = 2$ *alors* $t(K,\ell) \mid 2$. *Si* $t(K,2) = 2$ *et si* ζ *est une racine de l'unité d'ordre* $2^{m(K,2)}$ *alors* $K^{(2)}$ *est l'un des deux corps* $\mathbb{Q}(\zeta+\zeta^{-1})$ *ou* $\mathbb{Q}(\zeta-\zeta^{-1})$.

Démonstration. Il s'agit d'un exercice de théorie de Galois : si $m = m(K, \ell)$, le corps $K^{(\ell)}$ est un sous-corps de $\mathbb{Q}(\mu_{\ell^m})$ non contenu dans $\mathbb{Q}(\mu_{\ell^{m-1}})$ donc le sous-groupe $G = \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^m})/K^{(\ell)})$ de $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^m})/\mathbb{Q})$ ne contient pas $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^m})/\mathbb{Q}(\mu_{\ell^{m-1}}))$. Dans l'isomorphisme $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^m})/\mathbb{Q}) \simeq (\mathbb{Z}/\ell^m\mathbb{Z})^\times$ cela signifie que G ne contient pas le noyau de $(\mathbb{Z}/\ell^m\mathbb{Z})^\times \to (\mathbb{Z}/\ell^{m-1}\mathbb{Z})^\times$. Lorsque ℓ est impair, tous ces groupes sont cycliques : G s'identifie à un sous-groupe de $\mathbb{Z}/\ell^{m-1}(\ell-1)\mathbb{Z}$ qui (si $m \neq 1$) ne contient pas l'unique sous-groupe de cardinal ℓ. Cela entraîne bien $t(K, \ell) = \mathrm{Card}G \mid \ell-1$ (y compris si $m = 1$). Lorsque $\ell = 2$, notre convention entraîne $m \geq 2$. Si $m = 2$ alors $K^{(2)}$ vaut soit $\mathbb{Q}(\mu_4)$ et $t(K, 2) = 1$ soit $\mathbb{Q}$ et $t(K, 2) = 2$, $K^{(2)} = \mathbb{Q}(\zeta + \zeta^{-1})$ car $\zeta + \zeta^{-1} = 0$. Supposons donc $m \geq 3$. Alors $(\mathbb{Z}/2^m\mathbb{Z})^\times \simeq \mathbb{Z}/2^{m-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et, dans cet isomorphisme, le noyau ci-dessus correspond à $2^{m-3}\mathbb{Z}/2^{m-2}\mathbb{Z} \times \{0\}$. Ceci force G à être l'un des trois groupes $\{(0, 0)\}$, $\{(0, 0), (0, 1)\}$ ou $\{(0, 0), (2^{m-3}, 1)\}$. Dans le premier cas, $t(K, 2) = 1$. Dans les deux autres $t(K, 2) = 2$ et, en revenant dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$, G est engendré par -1 ou $2^{m-1} - 1$. Le corps $K^{(2)}$ est donc le sous-corps de $\mathbb{Q}(\zeta)$ fixé par $\zeta \mapsto \zeta^{-1}$ ou $\zeta \mapsto \zeta^{2^{m-1}-1} = -\zeta^{-1}$ d'où le résultat. □

Nous donnons ensuite des minorations de $\Delta_K(g)$ et $\Delta'_K(g)$ en exhibant des ℓ-groupes de gros cardinal pour tout ℓ.

Lemme 4.5 *Nous avons toujours $\mu_K^{-1}S(g, K) \mid \Delta'_K(g)$. Lorsque g est pair et $K^{(2)}$ totalement réel, nous avons de plus $2\mu_K^{-1}S(g, K) \mid \Delta_K(g)$.*

Démonstration. Soit ℓ un nombre premier et notons $m = m(K, \ell)$, $t = t(K, \ell)$ puis $h = [g/t]$. Le produit $V = \mathbb{Q}(\mu_{\ell^m})^h \times (K^{(\ell)})^{g-ht}$ est un $K^{(\ell)}$-espace vectoriel de dimension g. Considérons le groupe H d'automorphismes de V engendré par :

- les permutations des h premiers facteurs,
- la multiplication du premier facteur par un élément de μ_{ℓ^m},
- l'action de $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^m})/K^{(\ell)})$ sur le premier facteur,
- la multiplication par -1 sur l'un des $g - ht$ derniers facteurs.

Nous obtenons ainsi un groupe de cardinal $\mathrm{Card}H = h!(t\ell^m)^h 2^{g-ht}$ que nous pouvons voir comme sous-groupe de $\mathrm{GL}(V) \simeq \mathrm{GL}_g(K^{(\ell)}) \subset \mathrm{GL}_g(K)$. Par conséquent $h!(t\ell^m)^h 2^{g-ht} \mid \mu_K\Delta'_K(g)$. Ceci donne la première partie de l'énoncé car on vérifie sur la définition que la ℓ-partie $S(g, K)_\ell$ divise cette quantité $h!(t\ell^m)^h 2^{g-ht}$ (c'est immédiat si $\ell \neq 2$, si $\ell = 2$ on peut écrire $t = 2^{t-1}$ par le lemme précédent).

Pour la seconde partie, nous ne considérons que $\ell = 2$ et conservons les notations abrégées m et t. Notons ζ un générateur de μ_{ℓ^m}. Par le lemme précédent, l'hypothèse que $K^{(\ell)}$ est totalement réel entraîne $t = 2$ et $K^{(2)} = \mathbb{Q}(\zeta + \zeta^{-1})$. Nous avons construit un groupe fini H de $K^{(2)}$-endomorphismes de $\mathbb{Q}(\zeta)^h$. Introduisons à présent le groupe infini G engendré par H et la multiplication par $1 + \zeta$ c'est-à-dire $(x_1, \ldots, x_h) \mapsto ((1 + \zeta)x_1, \ldots, (1 + \zeta)x_h)$ pour $(x_1, \ldots, x_h) \in \mathbb{Q}(\zeta)^h$. Une permutation des facteurs ou la multiplication sur l'un des facteurs par ζ commute à cette opération tandis que son commutant avec l'action de $\mathrm{Gal}(\mathbb{Q}(\zeta)/K^{(2)})$ fait apparaître un élément de H puisque $\overline{1 + \zeta} = 1 + \zeta^{-1} = (1 + \zeta)\zeta^{-1}$. Ainsi tout élément de G s'écrit de façon unique comme la multiplication par $(1 + \zeta)^n$ (pour $n \in \mathbb{Z}$) suivie par un élément de H. Par ailleurs, $(1 + \zeta)^2 = \zeta^2 + 2\zeta + 1 = \zeta(\zeta + 2 + \zeta^{-1})$ où $\zeta + 2 + \zeta^{-1} \in K^{(2)}$. Nous en déduisons que dans $\mathrm{GL}_g(K^{(2)})$ on a $H \cap (K^{(2)})^\times = \{\pm 1\}$ et $G \cap (K^{(2)})^\times = \pm(\zeta + 2 + \zeta^{-1})^{\mathbb{Z}}$. Par suite l'image de G dans $\mathrm{PGL}_g(K^{(2)})$ est un sous-groupe fini de cardinal $\mathrm{Card}H$ (il contient comme sous-groupe d'indice 2 l'image de H, elle-même de cardinal $2^{-1}\mathrm{Card}H$). Avec $\mathrm{PGL}_g(K^{(2)}) \subset \mathrm{PGL}_g(K)$, nous trouvons $\mathrm{Card}H \mid \Delta_K(g)$ donc $S(g, K)_2 \mid \Delta_K(g)$ par le calcul fait plus haut. Enfin $2 \mid \mu_K$ donne bien $2S(g, K)_2 \mid \mu_K\Delta_K(g)$ puis $2S(g, K) \mid \mu_K\Delta_K(g)$ (car $S(g, K) \mid \mu_K\Delta'_K(g) \mid \mu_K\Delta_K(g)$). □

Voici maintenant l'étape de réduction.

Lemme 4.6 *Nous avons* $\Gamma_K(g) \mid \Theta_K(g)$ *et* $\Gamma'_K(g) \mid \Theta'_K(g)$.

Démonstration. Soient $\mathfrak{A} \in \mathcal{C}_g(K)$ et $G \in \mathcal{G}(\mathfrak{A}^\times/K^\times)$. Notons S un système de représentants de G dans $\mathfrak{A}^\times$. Choisissons aussi un ordre maximal $\mathcal{O}$ de $\mathfrak{A}$. Pour un entier naturel non nul n, on note $\mathcal{O}_n = \mathcal{O}[1/n]$ et $\mathcal{O}_{K,n} = \mathcal{O}_K[1/n]$. On a $\mathcal{O} \cap K = \mathcal{O}_K$ donc $\mathcal{O}_n \cap K = \mathcal{O}_{K,n}$. En utilisant la finitude de S, nous pouvons choisir l'entier n de sorte que

(1) le discriminant de la K-algèbre $\mathfrak{A}$ (un idéal de $\mathcal{O}_K$) contient n,
(2) $\mathcal{O}_{K,n}$ est principal,
(3) $S \subset \mathcal{O}_n$ et $S^{-1} \subset \mathcal{O}_n$,
(4) pour tout $s \in S$ tel que $s \notin K$, il existe une base $e_1, \ldots, e_{g^2}$ de $\mathcal{O}_n$ sur $\mathcal{O}_{K,n}$ avec $e_1 = 1$ et $e_2^*(s) \in \mathcal{O}_{K,n}^\times$

(pour (4) on choisit la base pour que $e_2^*(s)$ soit non nul puis on multiplie n par un entier bien choisi pour qu'il soit inversible).

Considérons maintenant un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ ne contenant pas n. La propriété (1) entraîne $\mathcal{O}/\mathfrak{p}\mathcal{O} \simeq M_g(\mathcal{O}_K/\mathfrak{p})$: en effet, le complété $\mathfrak{A}_\mathfrak{p}$ est isomorphe à $M_g(K_\mathfrak{p})$ d'après [Re, (25.7)] ; $\mathcal{O}_\mathfrak{p}$ en est un ordre maximal (par [Re, (11.6)]) donc isomorphe à $M_g(\mathcal{O}_{K_\mathfrak{p}})$ par [Re, (17.3)] ; on conclut avec $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} \simeq \mathcal{O}/\mathfrak{p}\mathcal{O}$ et $\mathcal{O}_{K_\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}} \simeq \mathcal{O}_K/\mathfrak{p}$. Désignons à présent par H le sous-groupe de $\mathcal{O}_n^\times$ engendré par S et $\mathcal{O}_{K,n}^\times$. Par le choix de S, le quotient $H/\mathcal{O}_{K,n}^\times$ est isomorphe à G. Par ailleurs, la réduction

$$\mathcal{O}_n \longrightarrow \mathcal{O}_n/\mathfrak{p}\mathcal{O}_n \simeq \mathcal{O}/\mathfrak{p}\mathcal{O} \simeq M_g(\mathcal{O}_K/\mathfrak{p})$$

nous donne un morphisme de groupes $H \to \mathrm{GL}_g(\mathcal{O}_K/\mathfrak{p})$ puis, en composant, un morphisme $\varphi\colon H \to \mathrm{PGL}_g(\mathcal{O}_K/\mathfrak{p})$. Nous avons bien sûr $\mathcal{O}_{K,n}^\times \subset \mathrm{Ker}\varphi$ donc φ induit un morphisme $G \to \mathrm{PGL}_g(\mathcal{O}_K/\mathfrak{p})$. Il nous reste à voir que ce morphisme est injectif, autrement dit $\mathrm{Ker}\varphi = \mathcal{O}_{K,n}^\times$. Considérons pour cela un élément $x \in \mathrm{Ker}\varphi \backslash \mathcal{O}_{K,n}^\times$. Par définition de H, on peut écrire $x = sy$ avec $s \in S$ et $y \in \mathcal{O}_{K,n}^\times$. Comme $x \notin \mathcal{O}_{K,n}^\times$, on a $s \notin K$ (on a $\mathcal{O}_n^\times \cap K = \mathcal{O}_{K,n}^\times$). L'hypothèse $x \in \mathrm{Ker}\varphi$ montre qu'il existe $z \in \mathcal{O}_K$ tel que $x - z \in \mathfrak{p}\mathcal{O}_n$ soit $s - zy^{-1} \in \mathfrak{p}\mathcal{O}_n$. En particulier, pour la base associée à s par la propriété (4) on a $e_2^*(s) = e_2^*(s - zy^{-1}e_1) = e_2^*(s - zy^{-1}) \in \mathfrak{p}\mathcal{O}_{K,n}$, ce qui contredit $e_2^*(s) \in \mathcal{O}_{K,n}^\times$.

Nous avons montré que pour tout $G \in \mathcal{G}(\mathfrak{A}^\times/K^\times)$ il existe $n \geq 1$ tel que si $n \notin \mathfrak{p}$ alors nous avons une injection $G \hookrightarrow \mathrm{PGL}_g(\mathcal{O}_K/\mathfrak{p})$. Ainsi $\mathrm{Card}G \mid \Theta_K(g)$ puis, en variant $\mathfrak{A}$ et G, nous trouvons bien $\Gamma_K(g) \mid \Theta_K(g)$. La seconde divisibilité s'établit de la même manière : à partir d'un sous-groupe $G \in \mathcal{G}(\mathfrak{A}^\times)$, on choisit n tel que (1)–(4) valent pour $S = G$. On obtient alors directement un morphisme $G \to \mathrm{GL}_g(\mathcal{O}_K/\mathfrak{p})$ pour $n \notin \mathfrak{p}$ et s'il n'était pas injectif nous aurions $g - 1 \in \mathfrak{p}\mathcal{O}_n$ pour un élément $g \in G \setminus \{1\}$. Si $g \notin K$, on conclut comme ci-dessus. Si $g \in K \setminus \{1\}$, pour éviter $g - 1 \in \mathfrak{p}\mathcal{O}_{K,n}$, il suffit de multiplier préalablement n par un entier convenable de sorte que $g - 1 \in \mathcal{O}_{K,n}^\times$. □

Il s'agit à présent de calculer $\Theta_K(g)$ et $\Theta'_K(g)$. Nous commençons par un lemme élémentaire qui permet d'estimer le cardinal du groupe linéaire sur un corps fini à l'aide de congruences vérifiées par le cardinal du corps.

Lemme 4.7 *Soient* ℓ *un nombre premier,* $g \geq 1$ *un entier,* k *un corps fini de cardinal* q *premier à* ℓ *et* t *un diviseur de* $\ell - 1$. *On note* $T = (\mathrm{Card}\mathrm{GL}_g(k))_\ell$.

(1) *Si* $\ell \neq 2$ *et s'il existe* $m \geq 1$ *tel que* q *est d'ordre* $t\ell$ *dans* $(\mathbb{Z}/\ell^{m+1}\mathbb{Z})^\times$ *alors* $T = \ell^{m[g/t]}[g/t]!_\ell$.
(2) *Si* $\ell = 2$ *et s'il existe un entier* $m \geq 2$ *tel que* $q \equiv 2^m + 1[2^{m+1}]$ *alors* $T = 2^{mg}g!_2$.
(3) *Si* $\ell = 2$ *et s'il existe un entier* $m \geq 2$ *tel que* $q \equiv 2^m - 1[2^{m+1}]$ *alors* $T = 2^{g+(m-1)[g/2]}g!_2$.

Démonstration. On rappelle

$$\mathrm{Card}\mathrm{GL}_g(k) = \prod_{i=0}^{g-1}(q^g - q^i) \qquad \text{donc} \qquad T = \prod_{i=1}^{g}(q^i - 1)_\ell.$$

(1) Puisque $(\mathbb{Z}/\ell^n\mathbb{Z})^\times \simeq \mathbb{Z}/\ell^{n-1}\mathbb{Z} \times \mathbb{Z}/(\ell-1)\mathbb{Z}$ pour tout $n \geq 1$, l'hypothèse entraîne que q est d'ordre $t\ell^{\max(0,n-m)}$ dans ce groupe. On en déduit $(q^i-1)_\ell = 1$ si t ne divise pas i et $(q^i-1)_\ell = \ell^m(i/t)_\ell$ dans le cas contraire. Ceci donne bien la valeur annoncée de T par produit. (2) Ici $q \equiv 1[4]$ donc l'image de q appartient à $\mathrm{Ker}((\mathbb{Z}/2^n\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times) \simeq \mathbb{Z}/2^{n-2}\mathbb{Z}$ pour tout $n \geq 2$ et son ordre dans ce groupe est donc $2^{\max(0,n-m)}$ (puisqu'il vaut clairement 2 lorsque $n = m+1$). Comme ci-dessus, cela fournit $(q^i-1)_2 = 2^m i_2$ pour tout i puis le résultat pour T. (3) Maintenant $q \equiv 3[4]$ ce qui donne $(q^i-1)_2 = 2$ si i est impair. Lorsque i est pair, $q^i = (-q)^i$ et comme $-q \equiv 2^m + 1[2^{m+1}]$ le cas précédent fournit $(q^i-1)_2 = 2^m i_2$ et la conclusion en découle. □

Pour trouver des corps résiduels de la forme $\mathcal{O}_K/\mathfrak{p}$ dont le cardinal vérifie les congruences souhaitées, nous utiliserons le théorème de Chebotarev sous la forme suivante.

Lemme 4.8 *Soient K un corps de nombres, L une extension abélienne finie de $\mathbb{Q}$ et $\sigma \in \mathrm{Gal}(L/L\cap K)$. Alors il existe une infinité de nombres premiers p tels que*

(1) *il existe un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ vérifiant $\mathrm{Card}\mathcal{O}_K/\mathfrak{p} = p$,*

(2) *le morphisme de Frobenius associé à p dans l'extension $L/\mathbb{Q}$ coïncide avec σ.*

Démonstration. Notons M une extension galoisienne finie de $\mathbb{Q}$ contenant K et L. L'application de restriction $\mathrm{Gal}(M/K) \to \mathrm{Gal}(L/L\cap K)$ est surjective donc nous pouvons choisir un antécédent τ de σ. Le théorème de Chebotarev (voir théorème 6.3.1 de [FJ]) dans l'extension $M/\mathbb{Q}$ entraîne alors que, pour une infinité de nombres premiers p (non ramifiés dans $M/\mathbb{Q}$), il existe un idéal $\mathfrak{q}$ de $\mathcal{O}_M$ au-dessus de p tel que $\mathrm{Frob}_\mathfrak{q} = \tau$. En notant $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$, nous avons bien $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z}$ car si $x \in \mathcal{O}_K$, $x - x^p = \tau(x) - x^p \in \mathfrak{p}$ tandis que $\mathrm{Frob}_{\mathfrak{q}\cap\mathcal{O}_L} = \tau_{|L} = \sigma$. □

Ces deux lemmes permettent de conclure le calcul de $\Theta_K(g)$ et $\Theta'_K(g)$.

Proposition 4.9 *Si le corps $K^{(2)}$ n'est pas totalement réel alors $\Theta_K(g) = \Theta'_K(g) = \mu_K^{-1}S(g,K)$. S'il est totalement réel, $\Theta_K(g) = \Theta'_K(g) = \mu_K^{-1}S(g,K)2^{[g/2]}$.*

Démonstration. Fixons tout d'abord un nombre premier impair ℓ. Nous notons $m = m(K,\ell)$, $t = t(K,\ell)$ et $L = \mathbb{Q}(\mu_{\ell^{m+1}})$. Remarquons que $(\mu_K)_\ell = \ell^m$ si $t = 1$ et $(\mu_K)_\ell = 1$ si $t \neq 1$ (car si $\ell \mid \mu_K$ alors $\mathbb{Q}(\mu_\ell) \subset K^{(\ell)} \subset L$ donc $t \mid [L : \mathbb{Q}(\mu_\ell)] = \ell^m$ et $t = 1$ par le lemme 4.4) et que cela s'écrit aussi $(\mu_K)_\ell = S(1,K)_\ell$. Appliquons maintenant le lemme 4.8 à un générateur σ du groupe cyclique $\mathrm{Gal}(L/L\cap K)$ de cardinal $t\ell = [L : K^{(\ell)}]$. Pour chacun des p dans l'ensemble infini obtenu, la condition (2) montre que p est d'ordre $t\ell$ dans $(\mathbb{Z}/\ell^{m+1}\mathbb{Z})^\times$ (pour l'identification du Frobenius dans l'isomorphisme $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/\ell^{m+1}\mathbb{Z})^\times$ voir par exemple le corollaire 2 page 86 de [CF]). Alors la condition (1) jointe au lemme 4.7 nous assure $(\mathrm{Card}\mathrm{GL}_g(\mathcal{O}_K/\mathfrak{p}))_\ell = S(g,K)_\ell$ pour un idéal $\mathfrak{p}$ premier au-dessus de p. Ceci étant vrai pour une infinité de $\mathfrak{p}$, nous avons $(\mu_K\Theta'_K(g))_\ell \mid S(g,K)_\ell$. D'un autre côté, les lemmes 4.3, 4.5 et 4.6 fournissent $S(g,K) \mid \mu_K\Delta'_K(g) \mid \mu_K\Gamma'_K(g) \mid \mu_K\Theta'_K(g)$ donc il y a égalité $(\mu_K\Theta'_K(g))_\ell = S(g,K)_\ell$. De plus, pour les $\mathfrak{p}$ choisis, $(\mathrm{Card}\mathrm{PGL}_g(\mathcal{O}_K/\mathfrak{p}))_\ell = (\mathrm{Card}\mathrm{GL}_g(\mathcal{O}_K/\mathfrak{p}))_\ell(\mathrm{Card}\mathrm{GL}_1(\mathcal{O}_K/\mathfrak{p}))_\ell^{-1} = S(g,K)_\ell S(1,K)_\ell^{-1} = (\mu_K)_\ell^{-1}S(g,K)_\ell$ donc $\Theta_K(g) \mid (\mu_K)_\ell^{-1}S(g,K)_\ell$ et à nouveau les divisibilités des lemmes 4.3, 4.5 et 4.6 entraînent l'égalité.

Considérons à présent le nombre premier $\ell = 2$. Nous écrivons encore $m = m(K,2)$ et $t = t(K,2)$. De façon analogue au cas précédent, nous avons $(\mu_K)_2 = 2$ si $t = 2$ et $(\mu_K)_2 = 2^m$ si $t = 1$ donc $(\mu_K)_2 = S(1,K)_2$. Distinguons selon la nature de $K^{(2)}$. Si $t = 1$, notons ξ une racine de l'unité d'ordre 2^{m+1} de sorte que $K^{(2)} = \mathbb{Q}(\xi^2)$. Nous appliquons le lemme 4.8 à $L = \mathbb{Q}(\xi)$ et au générateur σ de $\mathrm{Gal}(L/K^{(2)})$, qui est caractérisé par $\sigma(\xi) = -\xi = \xi^{2^m+1}$. De cette façon, un p fourni par ce lemme vérifie $p \equiv 2^m + 1[2^{m+1}]$ et le lemme 4.7 conduit à $(\mathrm{Card}\mathrm{GL}_g(\mathcal{O}_K/\mathfrak{p}))_2 = 2^{mg}g!_2 = S(g,K)_2$ pour une infinité de premiers $\mathfrak{p}$ de $\mathcal{O}_K$. On conclut alors, exactement comme dans le cas où ℓ est impair, que $(\mu_K\Theta_K(g))_2 = (\mu_K\Theta'_K(g))_2 = S(g,K)_2$.

Lorsque $t = 2$ et que $K^{(2)}$ n'est pas totalement réel, nous avons $K^{(2)} = \mathbb{Q}(\zeta - \zeta^{-1})$ pour une racine ζ de l'unité d'ordre 2^m. Nous utilisons ici le lemme 4.8 avec $L = \mathbb{Q}(\zeta)$ et $\sigma \in \mathrm{Gal}(L/K^{(2)})$ donné par $\sigma(\zeta) = -\zeta^{-1} = \zeta^{2^{m-1}-1}$. Le raisonnement est identique avec $p \equiv 2^{m-1} - 1[2^m]$ qui donne par le lemme 4.7 (ici $m \geq 3$) la valeur $2^{g+(m-2)[g/2]}g!_2 = 2^{g-[g/2]+m[g/2]}[g/2]!_2 = S(g,K)_2$. On conclut de la même manière.

Étudions enfin le cas où $K^{(2)}$ est totalement réel. Ici $t = 2$, $m \geq 2$ et $K^{(2)} = \mathbb{Q}(\xi^2 + \xi^{-2})$ si ξ désigne comme plus haut un générateur de $\mu_{2^{m+1}}$. Nous choisissons $L = \mathbb{Q}(\xi)$ et $\sigma \in \mathrm{Gal}(L/K^{(2)})$ décrit par $\sigma(\xi) = -\xi^{-1} = \xi^{2^m-1}$. L'application des lemmes 4.7 et 4.8 avec la congruence $p \equiv 2^m - 1[2^{m+1}]$ fournit ici $(\mathrm{Card}\mathrm{GL}_g(\mathcal{O}_K/\mathfrak{p}))_2 = 2^{g+(m-1)[g/2]}g!_2 = 2^{g+m[g/2]}[g/2]!_2 = 2^{[g/2]}S(g,K)_2$. Ceci permet encore de conclure que $(\mu_K\Theta_K(g))_2$ et $(\mu_K\Theta'_K(g))_2$ divisent $2^{[g/2]}S(g,K)_2$ mais les divisibilités des lemmes 4.3, 4.5 et 4.6 ne suffisent pas pour atteindre l'égalité en raison du facteur supplémentaire $2^{[g/2]}$. Nous devons ici calculer directement Θ et Θ'. Considérons pour cela un nombre premier impair arbitraire et le Frobenius Frob_p associé dans $K^{(2)} = \mathbb{Q}(\zeta+\zeta^{-1})$ où $\zeta = \xi^2$. Comme $\mathrm{Frob}_p(\zeta+\zeta^{-1}) = \zeta^p+\zeta^{-p}$ puis $(\mathrm{Frob}_p)^n(\zeta + \zeta^{-1}) = \zeta^{p^n} + \zeta^{-p^n}$, l'ordre f de Frob_p est le plus petit entier n tel que $\zeta^{p^n} + \zeta^{-p^n} = \zeta + \zeta^{-1} \iff \zeta^{p^n} = \zeta$ ou $\zeta^{p^n} = \zeta^{-1} \iff p^n \equiv 1[2^m]$ ou $p^n \equiv -1[2^m]$. En particulier, $p^f \equiv \pm 1[2^m]$. Comme pour tout idéal $\mathfrak{q}$ de $\mathcal{O}_{K^{(2)}}$ au-dessus de p le corps résiduel $\mathcal{O}_{K^{(2)}}/\mathfrak{q}$ est de cardinal p^f nous en déduisons qu'à plus forte raison le cardinal q du corps résiduel $\mathcal{O}_K/\mathfrak{p}$ de tout idéal de $\mathcal{O}_K$ au-dessus de p vérifie $q \equiv \pm 1[2^m]$. Il existe donc un entier $n \geq m$ tel que $q \equiv 2^n + 1[2^{n+1}]$ ou $q \equiv 2^n - 1[2^{n+1}]$. Par le lemme 4.7, $(\mathrm{Card}\mathrm{GL}_g(\mathcal{O}_K/\mathfrak{p}))_2$ vaut $2^{ng}g!_2$ ou $2^{g+(n-1)[g/2]}g!_2$ et donc est toujours un multiple de $2^{g+(m-1)[g/2]}g!_2 = 2^{[g/2]}S(g,K)_2$. Ceci vaut pour tout idéal $\mathfrak{p}$ de $\mathcal{O}_K$ avec $2 \notin \mathfrak{p}$ donc $\mu_K\Theta'_K(g)$ est aussi un multiple de cette quantité d'où $(\mu_K\Theta'_K(g))_2 = 2^{[g/2]}S(g,K)_2$. Pour $(\mathrm{Card}\mathrm{PGL}_g(\mathcal{O}_K/\mathfrak{p}))_2$, nous trouvons la valeur $2^{n(g-1)}g!_2$ ou $2^{g-1+(n-1)[g/2]}g!_2$ toujours multiple de $2^{g-1+(m-1)[g/2]}g!_2 = 2^{[g/2]}(\mu_K)_2^{-1}S(g,K)_2$ et l'on conclut à nouveau $(\mu_K\Theta_K(g))_2 = 2^{[g/2]}S(g,K)_2$. □

Cette proposition et les lemmes 4.3, 4.5 et 4.6 nous montrent que si $K^{(2)}$ n'est pas totalement réel alors $\Theta \mid \Delta' \mid \Gamma', \Delta \mid \Gamma \mid \Theta = \Theta' = \mu^{-1}S$ donc les théorèmes 4.1 et 4.2 sont établis dans ce cas. Si $K^{(2)}$ est totalement réel, ils le sont à une puissance de 2 près. Dans le cas restant, le lemme 4.6 ne suffit pas et nous devons revenir au procédé de réduction de sa démonstration et extraire une information supplémentaire. Nous montrerons que les 2-groupes obtenus par réduction satisfont une condition de trace et nous utiliserons le résultat suivant.

Lemme 4.10 *Soient $m \geq 2$ un entier, $p > g^2$ un nombre premier tel que $p \equiv 2^m - 1[2^{m+1}]$ et G un 2-sous-groupe de $\mathrm{GL}_g(\mathbb{F}_p)$.*

(1) *Si pour tout $x \in G$ on a $\mathrm{Tr}(x) = \mathrm{Tr}(x^{-1})$ alors $\mathrm{Card}G \mid 2^{g+(m-1)[g/2]}[g/2]!_2$.*

(2) *Si g est pair et si pour tout $x \in G$ on a $\mathrm{Tr}(x)^2 = \mathrm{Tr}(x^{-1})^2$ alors $\mathrm{Card}G \mid 2^{g+1+(m-1)[g/2]}[g/2]!_2$.*

Démonstration. (1) Ce fait peut se déduire de la démonstration de la proposition 18 de [GL]. Nous donnons une variante (sans forme quadratique) de leur preuve, qui sert aussi de préparation à la démonstration de la seconde assertion. La congruence sur p fournit $(p^2-1)_2 = 2^{m+1}$ et nous appelons Υ le sous-groupe de $\mathbb{F}_{p^2}^\times$ de cardinal 2^{m+1}. Commençons par décrire un 2-sous-groupe de Sylow de $\mathrm{GL}_g(\mathbb{F}_p)$ lorsque $g = 2h$ est pair. Nous notons Σ un 2-sous-groupe de Sylow de $\mathfrak{S}_h$ et considérons le sous-groupe U d'automorphismes $\mathbb{F}_p$-linéaires de $\mathbb{F}_{p^2}^h$ engendré par :

– l'action des éléments de Σ sur les facteurs,
– l'action de $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ sur l'un des facteurs,
– la multiplication de l'un des facteurs par un élément de Υ.

Cette construction (tout à fait semblable à celle faite pour le lemme 4.5) fournit un groupe U de cardinal $(\mathrm{Card}\Sigma)(2^{m+2})^h = 2^{g+mh}h!_2 = 2^{g+(m-1)h}g!_2$. Par le lemme 4.7, il s'agit bien d'un 2-Sylow de $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^2}^h) \simeq \mathrm{GL}_g(\mathbb{F}_p)$. Tous les 2-Sylow étant conjugués, nous pouvons supposer que G est contenu dans U et le résultat à montrer est que son indice $[U : G]$ vaut au moins 2^h. Notons à présent H le sous-groupe Υ^h de U. Nous allons établir $[H : H \cap G] \geq 2^h$ ce qui donnera bien $[U : G] \geq 2^h$.

Comme la trace sur $\mathbb{F}_p$ d'un élément $a \in \mathbb{F}_{p^2}$ vaut $a + a^p$, notre hypothèse entraîne

$$\sum_{i=1}^h \zeta_i + \zeta_i^p = \sum_{i=1}^h \zeta_i^{-1} + \zeta_i^{-p}$$

pour tout élément $x = (\zeta_1, \ldots, \zeta_h) \in G \cap H$. Notons $\pi_i \colon H \to \Upsilon$ la i-ème projection et V_i la représentation de dimension 1 de $G \cap H$ dans $\mathbb{F}_{p^2}$ décrite par le morphisme de groupes $\pi_{i|G\cap H}$. La formule précédente nous dit que les deux représentations de $G \cap H$

$$\bigoplus_{i=1}^h V_i \oplus V_i^{\otimes p} \qquad \text{et} \qquad \bigoplus_{i=1}^h V_i^{\otimes -1} \oplus V_i^{\otimes -p}$$

ont le même caractère. Sachant que leur dimension commune g est $< p$, elles sont isomorphes (les relations d'orthogonalité des caractères de Schur montrent que les deux multiplicités dans ces représentations d'une représentation irréductible donnée coïncident modulo p donc sont égales). Par suite, pour chaque $i \in \{1, \ldots, h\}$ il existe $j = \sigma(i) \in \{1, \ldots, h\}$ tel que $V_i \otimes V_j$ ou $V_i \otimes V_j^{\otimes p}$ est la représentation triviale. D'après $p^2 \equiv 1[2^{m+1}]$, nous avons $V_i^{\otimes p} \otimes V_j \simeq (V_i \otimes V_j^{\otimes p})^{\otimes p}$ donc la condition est symétrique en i et j ce qui fait qu'en procédant de proche en proche nous pouvons supposer que σ est une involution. Notons Γ le sous-groupe de $\mathrm{Hom}(H, \Upsilon)$ des morphismes triviaux sur $G \cap H$. Alors, pour tout $i \in \{1, \ldots, h\}$, nous avons $\pi_i \pi_{\sigma(i)} \in \Gamma$ ou $\pi_i \pi_{\sigma(i)}^p \in \Gamma$. Lorsque $\sigma(i) = i$ l'élément obtenu (π_i^2 ou $\pi_i^{p+1} = \pi_i^{2^m}$) est d'ordre au moins 2 ; lorsque $\sigma(i) \neq i$, il est d'ordre 2^{m+1}. Par conséquent, le sous-groupe de Γ engendré par ces éléments est de cardinal au moins $2^{n_1+(m+1)n_2}$ où n_1 est le nombre de points fixes et n_2 le nombre de 2-cycles. Comme $n_1 + 2n_2 = h$, $n_1 + (m+1)n_2 \geq n_1 + 3n_2 \geq h$ donc $\mathrm{Card}\Gamma \geq 2^h$. Vu la définition de Γ, nous avons $\mathrm{Card}\Gamma = [H : H \cap G]$ ce qui établit le résultat souhaité (lorsque g est pair).

Lorsque g est impair, la valeur donnée par le lemme 4.7 montre qu'un sous-groupe de Sylow de $\mathrm{GL}_g(\mathbb{F}_p)$ s'obtient comme l'ensemble des matrices $y = \begin{pmatrix} x & 0 \\ 0 & \varepsilon \end{pmatrix}$ où x parcourt un 2-Sylow de $\mathrm{GL}_{g-1}(\mathbb{F}_p)$ et $\varepsilon = \pm 1$. Si $y \in G$ alors $\mathrm{Tr}(x) = \mathrm{Tr}(x^{-1})$ donc on peut utiliser le résultat pour $g-1$ avec $G' = \{x \mid \exists \varepsilon \begin{pmatrix} x & 0 \\ 0 & \varepsilon \end{pmatrix} \in G\}$. Cela nous donne $\mathrm{Card}G \mid 2\mathrm{Card}G' \mid 2^{1+(g-1)+(m-1)(g-1)/2}(((g-1)/2)!)_2 = 2^{g+(m-1)[g/2]}[g/2]!_2$ comme prévu.

(2) Nous reprenons toutes les notations de (1) : h, U, H, Γ, π_i, V_i. La première différence est que nous devons seulement montrer $[H : H \cap G] = \mathrm{Card}\Gamma \geq 2^{h-1}$, la

seconde que l'égalité des traces et la condition $p > g^2$ donnent ici

$$\left(\bigoplus_{i=1}^{h} V_i \oplus V_i^{\otimes p}\right)^{\otimes 2} \simeq \left(\bigoplus_{i=1}^{h} V_i^{\otimes -1} \oplus V_i^{\otimes -p}\right)^{\otimes 2}.$$

En développant, nous voyons en particulier que pour tout couple (i,j) d'éléments de $\{1,\dots,h\}$ il existe un couple (k,ℓ) tel que l'un des éléments $\pi_i\pi_j\pi_k\pi_\ell$, $\pi_i\pi_j\pi_k^p\pi_\ell$, $\pi_i\pi_j\pi_k\pi_\ell^p$, $\pi_i\pi_j\pi_k^p\pi_\ell^p$ appartient à Γ. Nous allons maintenant construire par un procédé itératif une permutation $\sigma \in \mathfrak{S}_h$ et une partie $E \subset \{1,\dots,h\}$ contenant h vérifiant la propriété suivante : pour tout $i \in E$, si Δ_i désigne le sous-groupe de $\mathrm{Hom}(H,\Upsilon)$ engendré par $\pi_{\sigma(1)},\dots,\pi_{\sigma(i)}$, alors $\mathrm{Card}\Gamma \cap \Delta_i \geq 2^{i-1}$. Le cas $i = h$ sera le résultat souhaité. Nous posons $\sigma(1) = 1$; ceci suffit pour définir Δ_1 et la propriété requise $\mathrm{Card}\Gamma \cap \Delta_1 \geq 1$ est tautologique. Nous pouvons décider $1 \in E$. Par récurrence, nous supposons avoir construit $\sigma(1),\dots,\sigma(i)$ et $E \cap \{1,\dots,i\}$ avec $i \in E$ et donc $\mathrm{Card}\Gamma \cap \Delta_i \geq 2^{i-1}$. Si $i = h$ c'est terminé, sinon choisissons arbitrairement j hors de $\{\sigma(1),\dots,\sigma(i)\}$, posons $\sigma(i+1) = j$ et considérons l'assertion ci-dessus pour le couple $(1,j)$. Elle nous fournit un couple (k,ℓ) et un élément $\gamma = \pi_1\pi_j\pi_k^?\pi_\ell^? \in \Gamma$. Distinguons plusieurs cas. Si $\{k,\ell\} \subset \{\sigma(1),\dots,\sigma(i+1)\}$ alors l'exposant de π_j dans γ vaut 1, 2, 3, p, $p+1$ ou $2p$ (en distinguant selon que l'on a ou pas $k = j$, $\ell = j$). Vu la congruence vérifiée par p, cet exposant n'est jamais divisible par 2^{m+1}. Nous avons donc un élément γ de $\Gamma \cap \Delta_{i+1}$ qui n'appartient pas à Δ_i d'où $\mathrm{Card}\Gamma\cap\Delta_{i+1} \geq 2\mathrm{Card}\Gamma\cap\Delta_i \geq 2^i$. Nous pouvons ainsi placer $i+1$ dans E et continuer la construction. Examinons ensuite le cas où $k \notin \{\sigma(1),\dots,\sigma(i+1)\}$ et $\ell \in \{\sigma(1),\dots,\sigma(i+1),k\}$. Ici nous posons $\sigma(i+2) = k$. Dans l'élément γ, l'exposant de π_j ou π_k est impair donc son image dans Δ_{i+2}/Δ_i est d'ordre 2^{m+1}. Par suite, $\mathrm{Card}\Gamma \cap \Delta_{i+2} \geq 2^{m+1}\mathrm{Card}\Gamma \cap \Delta_i \geq 2^{m+i} \geq 2^{i+2} \geq 2^{i+1}$ et nous pouvons décréter $i+2 \in E$. Enfin, par symétrie entre k et ℓ, il reste seulement à traiter le cas où $k \neq \ell$ et $\{k,\ell\} \cap \{\sigma(1),\dots,\sigma(i)\} = \emptyset$. Ici $1,j,k,\ell$ sont deux à deux distincts donc tous les exposants de γ sont impairs. Nous posons $\sigma(i+2) = k$ et $\sigma(i+3) = \ell$ et donc notre élément γ est d'ordre 2^{m+1} dans Δ_{i+3}/Δ_i. Comme précédemment, cela donne $\mathrm{Card}\Gamma\cap\Delta_{i+3} \geq 2^{i+2}$ et nous autorise à ranger $i+3$ dans E. Ceci montre qu'il est toujours possible de continuer la construction et termine la démonstration. □

Voici notre dernier énoncé qui utilise un procédé de réduction modifié et conclut la démonstration des théorèmes 4.1 et 4.2.

Proposition 4.11 *Si $K^{(2)}$ est un corps totalement réel, nous avons $(\mu_K)_2 = 2$ et $2\Gamma'_K(g)_2 \mid S(g,K)_2$ pour tout g. Si de plus g est impair, $2\Gamma_K(g)_2 \mid S(g,K)_2$ tandis que si g est pair $\Gamma_K(g)_2 \mid S(g,K)_2$.*

Démonstration. Nous commençons par $\Gamma_K(g)$. Considérons donc une algèbre $\mathfrak{A} \in \mathcal{C}_g(K)$ et un sous-groupe $G \in \mathcal{G}(\mathfrak{A}^\times/K^\times)$. L'objectif étant de montrer que $(\mathrm{Card}G)_2$ divise une quantité prescrite, nous pouvons remplacer G par l'un de ses 2-Sylow, autrement dit supposer que G est un 2-groupe. Fixons temporairement un isomorphisme $\mathfrak{A} \otimes \overline{K} \simeq M_g(\overline{K})$. La trace et le déterminant usuels sur $M_g(\overline{K})$ induisent sur $\mathfrak{A}$ la trace réduite et la norme réduite de cette K-algèbre (voir [Re, (9.3)]) donc sont à valeurs dans K sur $\mathfrak{A}$. Le groupe G se retrouve plongé dans $\mathrm{PGL}_g(\overline{K})$ et son image réciproque dans $\mathrm{SL}_g(\overline{K})$ est un groupe fini dont nous notons $\widetilde{G}$ un 2-Sylow. Soit à présent $h \in \mathfrak{A}^\times$ dont l'image dans $\mathfrak{A}^\times/K^\times$ appartient à G. Par construction, il existe $z \in \overline{K}^\times$ et $\eta \in \widetilde{G}$ tels que $h = z\eta$. Il existe un entier c tel que $\eta^{2^c} = 1$ donc $z^{2^c} \in K$. D'autre part $z^g = \det(z\eta) = \det(h) \in K$ donc, en posant $2^a = \mathrm{pgcd}(2^c, g)$, nous avons $z^{2^a} \in K$ donc $\mathrm{Tr}(\eta)^{2^a} = z^{-2^a}\mathrm{Tr}(h)^{2^a} \in K$. Comme $\mathrm{Tr}(\eta) \in \mathbb{Q}(\mu_{2^c})$, nous avons même $\mathrm{Tr}(\eta)^{2^a} \in K^{(2)}$. Dans $\mathbb{Q}(\mu_{2^c})$, les éléments $\mathrm{Tr}(\eta)$ et $\mathrm{Tr}(\eta^{-1})$ sont conjugués donc l'hypothèse que $K^{(2)}$ est totalement réel entraîne

$\mathrm{Tr}(\eta)^{2^a} = \mathrm{Tr}(\eta^{-1})^{2^a}$. Nous en déduisons qu'ou bien $\mathrm{Tr}(h) = \mathrm{Tr}(h^{-1}) = 0$ ou bien ces deux traces sont non nulles et l'élément $\mathrm{Tr}(h)^{-1}\mathrm{Tr}(h^{-1})h^2$ de $\mathfrak{A}^\times$ est d'ordre une puissance de 2 et de déterminant 1 : en effet $\mathrm{Tr}(h)^{-1}\mathrm{Tr}(h^{-1})h^2 = \mathrm{Tr}(\eta)^{-1}\mathrm{Tr}(\eta^{-1})\eta^2$ et $(\mathrm{Tr}(\eta)^{-1}\mathrm{Tr}(\eta^{-1})\eta^2)^{2^c} = 1$, $\det(\mathrm{Tr}(\eta)^{-1}\mathrm{Tr}(\eta^{-1})\eta^2) = \mathrm{Tr}(\eta)^{-g}\mathrm{Tr}(\eta^{-1})^g = 1$. Nous reprenons maintenant la construction faite dans la démonstration du lemme 4.6. Nous en gardons les notations S, $\mathcal{O}$, n, $\mathcal{O}_n$, $\mathcal{O}_{K,n}$, H. En utilisant le lemme 4.8 comme dans la démonstration de la proposition 4.9, nous pouvons choisir un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ de norme un nombre premier p tel que $p \equiv 2^m - 1[2^{m+1}]$ où nous notons $m = m(K,2) \geq 2$. Nous pouvons également exiger $n \notin \mathfrak{p}$ et $p > g^2$. La construction montre alors que l'image de H dans $\mathrm{GL}_g(\mathcal{O}_K/\mathfrak{p})$ est un sous-groupe H_1 dont l'image dans $\mathrm{PGL}_g(\mathcal{O}_K/\mathfrak{p})$ est isomorphe à G. Notons H_2 un 2-Sylow de H_1. Nous avons $\mathrm{Card}H_2 = 2\mathrm{Card}G$ car $H_2 \cap (\mathcal{O}_K/\mathfrak{p})^\times = \{1,-1\}$ d'après $(p-1)_2 = 2$. Considérons maintenant un élément x de H_2 et un antécédent $h \in H$ de x. L'application de réduction $M_g(\mathcal{O}_{K_\mathfrak{p}}) \to M_g(\mathcal{O}_K/\mathfrak{p})$ respecte traces et déterminants et ceux-ci sur $\mathfrak{A}$ peuvent se calculer dans $M_g(\mathcal{O}_{K_\mathfrak{p}})$. Par suite, $\mathrm{Tr}(x)$ est l'image dans $\mathcal{O}_{K,n}/\mathfrak{p} \simeq \mathcal{O}_K/\mathfrak{p}$ de $\mathrm{Tr}(h) \in \mathcal{O}_{K,n}$ et de même pour $\mathrm{Tr}(x^{-1})$. Ainsi si $\mathrm{Tr}(h) = \mathrm{Tr}(h^{-1}) = 0$ alors $\mathrm{Tr}(x) = \mathrm{Tr}(x^{-1}) = 0$. Dans le cas contraire, $\mathrm{Tr}(h)^{-1}\mathrm{Tr}(h^{-1})h^2$ est d'ordre une puissance de 2 et de déterminant 1. Mais $h \in H$ fournit $\det(h) \in \mathcal{O}_{K,n}^\times$ donc $(\mathrm{Tr}(h)^{-1}\mathrm{Tr}(h^{-1}))^g \in \mathcal{O}_{K,n}^\times$ puis $\mathrm{Tr}(h)^{-1}\mathrm{Tr}(h^{-1}) \in \mathcal{O}_{K,n}^\times$ d'où $\mathrm{Tr}(h)^{-1}\mathrm{Tr}(h^{-1})h^2 \in H$. Notons y l'image dans H_1 de cet élément. C'est encore un élément d'ordre une puissance de 2 et de déterminant 1 et $\mathrm{Tr}(x)y = \mathrm{Tr}(x^{-1})x^2$. Si nous excluons le cas $\mathrm{Tr}(x) = \mathrm{Tr}(x^{-1}) = 0$ alors ces deux traces sont non nulles, y et x commutent et $\mathrm{Tr}(x)^{-1}\mathrm{Tr}(x^{-1}) = yx^{-2}$ est d'ordre une puissance de 2 dans $(\mathcal{O}_K/\mathfrak{p})^\times$ d'où $\mathrm{Tr}(x)^{-1}\mathrm{Tr}(x^{-1}) \in \{-1,1\}$. Nous avons donc $\mathrm{Tr}(x)^2 = \mathrm{Tr}(x^{-1})^2$ pour tout $x \in H_2$. De plus $\det(x)$ étant aussi d'ordre une puissance de 2, on a $\det(x)^2 = 1$ d'où $\mathrm{Tr}(x)^g = \det(\mathrm{Tr}(x)y) = \det(\mathrm{Tr}(x^{-1})x^2) = \mathrm{Tr}(x^{-1})^g$ ce qui entraîne $\mathrm{Tr}(x)^{\mathrm{pgcd}(g,2)} = \mathrm{Tr}(x^{-1})^{\mathrm{pgcd}(g,2)}$. Nous sommes donc en position d'appliquer le lemme 4.10 au groupe H_2 : si g est impair, nous avons $\mathrm{Card}H_2 \mid S(g,K)_2$ par l'assertion (1) tandis que si g est pair l'assertion (2) fournit $\mathrm{Card}H_2 \mid 2S(g,K)_2$. En passant à $\mathrm{Card}G = 2^{-1}\mathrm{Card}H_2$, nous en déduisons bien les divisibilités cherchées pour $\Gamma_K(g)$.

Pour $\Gamma'_K(g)$, nous considérons cette fois $G \in \mathcal{G}(\mathfrak{A}^\times)$ un 2-groupe. Avec $S = G$, tout élément s de S vérifie directement l'égalité $\mathrm{Tr}(s) = \mathrm{Tr}(s^{-1})$ donc nous pouvons appliquer l'assertion (1) du lemme 4.10 (pour tout g) à l'image de G dans $\mathrm{GL}_g(\mathcal{O}_K/\mathfrak{p})$, isomorphe à G. Il vient $\mathrm{Card}G \mid S(g,K)_2$ qui fournit bien *in fine* $2\Gamma'_K(g) \mid S(g,K)_2$. □

Guralnick et Lorenz montrent dans la partie 5 de [GL] comment la méthode de Minkowski permet de retrouver le résultat de Schur avec toutefois la restriction que si $t(K,2) = 2$ alors $K^{(2)}$ doit être totalement réel (voir leur proposition 18). La démarche suivie ci-dessus, basée sur des congruences différentes, permet de lever cette restriction. En effet, la démonstration de la proposition 4.9 montre que, dans tous les cas où $K^{(2)}$ n'est pas réel, il existe des p pour lesquels le groupe linéaire n'est pas trop gros et donc il n'est pas nécessaire de faire intervenir des formes quadratiques : par exemple, si $K^{(2)} = \mathbb{Q}(\mu_{2^m})$, Guralnick et Lorenz utilisent $p \equiv 2^m - 1[2^{m+1}]$ pour assurer la stabilité par conjugaison alors que nous pouvons prendre $p \equiv 2^m + 1[2^{m+1}]$ qui donne un groupe linéaire plus petit (car p est totalement décomposé dans $K^{(2)}$) ; pour cette même raison, nous pouvons conclure dans le cas exclu par [GL] en employant aussi un premier totalement décomposé.

5 Estimations numériques

Dans cette partie, nous entamons la démonstration du théorème 3.8 en traitant les cas qui se déduisent de majorations directes des quantités Γ et Γ' de la partie précédente.

Notre premier résultat nous permettra de traiter facilement les grandes valeurs de g.

Proposition 5.1 *Si q est un nombre premier impair tel que $q \leq g$ alors*

$$\log \frac{S(g,\mathbb{Q})}{g!} \leq g \sum_{p<q} \frac{\log p}{(p-1)^2} + \left(\sum_{2<p<q} 1 \right) \log g + g \left(\frac{q}{(q-1)^2} \log q + \frac{1}{q-1} \right)$$

où, dans les sommes, p parcourt les nombres premiers vérifiant la condition indiquée.

Démonstration. D'après la formule pour la valuation p-adique d'une factorielle, nous avons

$$\log \frac{S(g,\mathbb{Q})}{g!} = g \log 2 + \sum_{p>2} \left(\sum_{i \geq 0} \left[\frac{g}{(p-1)p^i} \right] - \left[\frac{g}{p^{i+1}} \right] \right) \log p.$$

Pour un nombre premier p fixé tel que $2 < p < q$ et un entier $i \geq 0$, notons $z_i = g(p-1)^{-1}p^{-i-1}$ et $y_i = z_i - [z_i]$ sa partie fractionnaire. Alors

$$\begin{aligned} \left[\frac{g}{(p-1)p^i} \right] - \left[\frac{g}{p^{i+1}} \right] &= [pz_i] - [(p-1)z_i] \\ &= [p[z_i] + py_i] - [(p-1)[z_i] + (p-1)y_i] \\ &= [z_i] + [py_i] - [(p-1)y_i] \\ &= z_i + [py_i] - [(p-1)y_i] - y_i. \end{aligned}$$

Si $y_i < 1/p$, nous avons $[py_i] = 0$ donc cette quantité est majorée par z_i. Sinon, comme on a toujours $[py_i] \leq [(p-1)y_i] + 1$, nous la majorons par $z_i + 1 - y_i \leq z_i + (p-1)p^{-1}$. En sommant la série géométrique z_i, il vient

$$\sum_{i \geq 0} \left[\frac{g}{(p-1)p^i} \right] - \left[\frac{g}{p^{i+1}} \right] \leq \frac{g}{(p-1)^2} + \frac{p-1}{p} \mathrm{Card} \left\{ i \geq 0 \mid y_i \geq \frac{1}{p} \right\}.$$

Puisque $y_i \geq p^{-1} \Rightarrow z_i \geq p^{-1} \iff i \leq \log(g/(p-1))/\log p$, nous avons

$$\frac{p-1}{p} \mathrm{Card} \left\{ i \geq 0 \mid y_i \geq \frac{1}{p} \right\} \log p \leq \frac{p-1}{p} \log \frac{pg}{p-1} \leq \log g,$$

en utilisant $\log(p/(p-1)) \leq 1/(p-1)$ et $g \geq q \geq e$. En substituant dans la formule initiale, nous voyons apparaître exactement les deux premiers termes de la majoration souhaitée et il nous reste à montrer

$$\sum_{p \geq q} \left(\sum_{i \geq 0} \left[\frac{g}{(p-1)p^i} \right] - \left[\frac{g}{p^{i+1}} \right] \right) \log p \leq \frac{gq}{(q-1)^2} \log q + \frac{g}{q-1}.$$

Pour tout entier naturel n, notons n_+ le plus petit nombre premier p tel que $p > n$. Alors le membre de gauche ci-dessus se peut réécrire

$$\sum_{i \geq 0} \left[\frac{g}{(q-1)q^i} \right] \log q + \sum_{i \geq 0} \sum_{p \geq q} \left(\left[\frac{g}{(p_+ - 1)p_+^i} \right] \log p_+ - \left[\frac{g}{p^{i+1}} \right] \log p \right).$$

Dans le premier terme, nous enlevons simplement la partie entière. Dans le second, nous notons que $p_+ \geq p+1$ entraîne $(p_+-1)p_+^i \geq p^{i+1}$. Ceci montre que notre expression est majorée par

$$\sum_{i\geq 0} \frac{g}{(q-1)q^i} \log q + \sum_{p\geq q} \sum_{i\geq 0} \left[\frac{g}{(p_+-1)p_+^i} \right] \log \frac{p_+}{p}.$$

En oubliant encore la partie entière et en sommant sur i, nous voyons apparaître le majorant

$$\frac{gq}{(q-1)^2} \log q + \sum_{p\geq q} \frac{gp_+}{(p_+-1)^2} \log \frac{p_+}{p}.$$

Or

$$\begin{aligned} \sum_{p\geq q} \frac{p_+}{(p_+-1)^2} \log \frac{p_+}{p} &= \sum_{p\geq q} \frac{p_+}{(p_+-1)^2} \sum_{n=p+1}^{p_+} \log \frac{n}{n-1} \\ &\leq \sum_{p\geq q} \sum_{n=p+1}^{p_+} \frac{n}{(n-1)^2} \log \frac{n}{n-1} \end{aligned}$$

car la fonction $x(1-x)^{-2}$ décroît pour $x>1$. La double somme obtenue vaut

$$\sum_{n\geq q+1} \frac{n}{(n-1)^2} \log \frac{n}{n-1} \leq \sum_{n\geq q+1} \frac{n}{(n-1)^3} \leq \sum_{n\geq q+1} \frac{1}{(n-1)(n-2)} = \frac{1}{q-1}$$

et, en regroupant nos estimations, nous trouvons bien la formule cherchée. □

Ce calcul améliore des majorations dues à Silverberg (voir [Si]) et à Katznelson (voir [Ka]). Après calculs informatiques, notre estimation prend la forme suivante.

Corollaire 5.2 *Si $g \geq 182$ nous avons*

$$\log \frac{S(g,\mathbb{Q})}{g!} \leq g \log \frac{11}{3}.$$

Si $g \geq 1$,

$$\log \frac{S(g,\mathbb{Q})}{g!} \leq g \log \frac{22}{5}.$$

Démonstration. Nous vérifions ceci par calcul direct si $1 \leq g \leq 8999$. Lorsque $g \geq 9000$, nous employons la proposition précédente avec $q=97$. En utilisant

$$\frac{\log g}{g} \leq \frac{\log 9000}{9000},$$

il vient

$$\frac{1}{g} \log \frac{S(g,\mathbb{Q})}{g!} \leq \sum_{p\leq 89} \frac{\log p}{(p-1)^2} + \frac{23}{9000} \log 9000 + \frac{97}{96^2} \log 97 + \frac{1}{96}$$

et le calcul montre que le membre de droite est majoré par $\log(11/3)$. □

La valeur $\log(11/3)$ est un seuil arbitraire, choisi suffisamment petit pour les calculs qui suivent.

Grâce à ce corollaire et à quelques calculs supplémentaires, nous obtenons le résultat suivant pour les corps quadratiques imaginaires.

Proposition 5.3 *Lorsque K est un corps quadratique imaginaire non cyclotomique et $g \geq 1$, nous avons toujours* $\min(2\Gamma_K(g), 2h_K\Gamma'_K(g)) \leq (9/2)f(g)$. *En outre, nous avons même* $\min(2\Gamma_K(g), 2h_K\Gamma'_K(g)) \leq f(g)$ *sauf pour les dix couples* $(K, g) = (\mathbb{Q}(\sqrt{-D}), g)$ *donnés par les valeurs*

g	6	6	6	12	12	12	12	20	24	24
D	2	7	11	2	7	19	23	2	2	7

Démonstration. Le fait que K ne soit pas cyclotomique entraîne $\mu_K = 2$. D'autre part, la seule façon d'avoir $K^{(2)}$ non totalement réel est d'avoir $K^{(2)} = K$ c'est-à-dire $K \subset \mathbb{Q}(\mu_{2^\infty})$ et ceci force $K = \mathbb{Q}(\sqrt{-2})$. Dans les autres cas, $K^{(2)} = \mathbb{Q}$. Rappelons que le nombre de classes de $\mathbb{Q}(\sqrt{-2})$ vaut 1. En combinant ces renseignements avec les théorèmes 4.1 et 4.2, nous constatons que $\min(2\Gamma_K(g), 2h_K\Gamma'_K(g))$ vaut $2S(g, K)$ lorsque g est pair et $h_K \geq 2$ et vaut $S(g, K)$ dans les autres cas. Maintenant, lorsque K est fixé, il existe au plus un nombre premier p tel que $K \subset \mathbb{Q}(\mu_{p^\infty})$ (et donc $K^{(p)} = K$). Si p est impair, l'unique sous-corps quadratique de $\mathbb{Q}(\mu_{p^\infty})$ est $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}) \subset \mathbb{Q}(\mu_p)$ et il est imaginaire si et seulement si $p \equiv 3[4]$. Dans ce cas $K = \mathbb{Q}(\sqrt{-p})$, on a $m(K, p) = 1$ et $t(K, p) = (p-1)/2$. Pour $K = \mathbb{Q}(\sqrt{-2})$, on a $m(K, 2) = 3$ et $t(K, 2) = 2$. En revenant à la définition de $S(g, K)$, nous trouvons :

- $S(g, K) = S(g, \mathbb{Q})2^{[g/2]}$ si $K = \mathbb{Q}(\sqrt{-2})$;
- $S(g, K) = S(g, \mathbb{Q}) \exp\left(\sum_{i \geq 0}\left(\left[\frac{2g}{(p-1)p^i}\right] - \left[\frac{g}{(p-1)p^i}\right]\right)\log p\right)$ si $K = \mathbb{Q}(\sqrt{-p})$ pour $p \equiv 3[4]$;
- $S(g, K) = S(g, \mathbb{Q})$ dans tous les autres cas.

Pour tout nombre premier p et tout entier $i \geq 0$, nous avons $2g(p-1)^{-1}p^{-i-1} \leq g(p-1)^{-1}p^{-i}$ ce qui permet d'écrire

$$\sum_{i \geq 0}\left[\frac{2g}{(p-1)p^i}\right] - \left[\frac{g}{(p-1)p^i}\right] \leq \left[\frac{2g}{p-1}\right] - \left[\frac{g}{p-1}\right] + \left[\frac{2g}{p(p-1)}\right]$$

que nous majorons généralement par $2g/(p-1)$. Remarquons encore que $(\log p)/(p-1)$ est une fonction décroissante de p et $2^{1/2} \leq 11^{1/5}$. Tout ceci montre que si $K \neq \mathbb{Q}(\sqrt{-7})$ alors $S(g, K) \leq S(g, \mathbb{Q})11^{g/5}$. Pour $K = \mathbb{Q}(\sqrt{-7})$, nous utilisons

$$\left[\frac{g}{3}\right] - \left[\frac{g}{6}\right] + \left[\frac{g}{21}\right] \leq g\left(\frac{1}{3} - \frac{1}{6} + \frac{1}{21}\right) + 1 = g\left(\frac{3}{14} + \frac{1}{g}\right).$$

Comme $(3/14 + 1/182)\log 7 \leq (\log 11)/5$, nous avons $S(g, K) \leq S(g, \mathbb{Q})11^{g/5}$ pour tout K si $g \geq 182$. Avec le corollaire 5.2, cela entraîne

$$2S(g, K) \leq 2\left(\frac{11}{3}11^{1/5}\right)^g g! \leq \frac{1}{3}\left(\frac{11}{3}11^{1/5}6^{1/182}\right)^g g! \leq \frac{1}{3}6^g g! = f(g)$$

et démontre l'énoncé pour $g \geq 182$. Supposons maintenant $g \leq 181$ mais que K n'est pas l'un des cinq corps $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$ ou $\mathbb{Q}(\sqrt{-23})$. D'après ce qui précède, ou bien $S(g, K) = S(g, \mathbb{Q})$ ou bien il existe $p \equiv 3[4]$ avec $K = \mathbb{Q}(\sqrt{-p})$. Vu les corps exclus, $p \geq 31$ et $S(g, K) \leq S(g, \mathbb{Q})p^{[2g/(p-1)]}$. Si $g \leq 14 < (p-1)/2$, il vient encore $S(g, K) = S(g, \mathbb{Q})$ tandis que si $g \geq 15$, nous majorons $p^{[2g/(p-1)]} \leq 31^{g/15}$. En notant $\alpha_g = 1$ si $g \leq 14$ et $\alpha_g = 31^{g/15}$ si $g \geq 15$ ainsi que $\beta_g = 1$ si g est impair et $\beta_g = 2$ si g est pair, nous avons donc

$$\min(2\Gamma_K(g), 2h_K\Gamma'_K(g)) \leq \beta_g S(g, K) \leq \alpha_g\beta_g S(g, \mathbb{Q})$$

et un calcul sur machine montre que $\alpha_g\beta_g S(g, \mathbb{Q}) \leq f(g)$ pour tout $g \leq 181$. Pour conclure nous évaluons aussi (pour $g \leq 181$) $S(g, \mathbb{Q}(\sqrt{-D}))$ où $D = 2, 7, 11, 19$

$(h = 1)$ et $\beta_g S(g, \mathbb{Q}(\sqrt{-23}))$ $(h \geq 2)$ ce qui conduit à la borne $(9/2)f(g)$ et à la liste d'exceptions de l'énoncé. $\square$

Passons au cas des corps de nombres de degré au moins 4.

Proposition 5.4 *Si K est un corps de nombres tel que $4 \leq [K : \mathbb{Q}] \mid 2g$, on a*

$$[K : \mathbb{Q}]\mu_K \Gamma_K(2g/[K : \mathbb{Q}]) \leq \frac{f(g)}{1 + [g/12]}.$$

Démonstration. Considérons tout d'abord le cas où $g \leq 3$. Les hypothèses entraînent $g \geq 2$ et $[K : \mathbb{Q}] = 2g$. Comme $\Gamma_K(1) = 1$, nous devons majorer $2g\mu_K$. Or si $[K : \mathbb{Q}] = 4$ nous avons $\mu_K \leq 12$ (12 est le plus grand entier n tel que $\varphi(n) \leq 4$) et de même $\mu_K \leq 18$ si $[K : \mathbb{Q}] = 6$. Le résultat devient alors trivial. Supposons maintenant $g \geq 4$. Grâce aux théorèmes 4.1 et 4.2, majorons $\mu_K \Gamma_K(n) \leq 2S(n, K)$ où nous notons désormais $n = 2g/[K : \mathbb{Q}]$. Évaluons la valuation p-adique de $S(n, K)/S(n, \mathbb{Q})$. Si p est un nombre premier impair, elle vaut

$$m(K,p)\left[\frac{n}{t(K,p)}\right] - \sum_{i \geq 0}\left[\frac{n}{(p-1)p^i}\right] - \left[\frac{n}{t(K,p)p^{i+1}}\right]$$

$$\leq n\frac{m(K,p)}{t(K,p)} \leq n\frac{p^{m(K,p)-1}}{t(K,p)} = n\frac{[K^{(p)} : \mathbb{Q}]}{p-1}$$

(on rappelle $t(K,p) = [\mathbb{Q}(\mu_{p^{m(K,p)}}) : K^{(p)}]$). Pour $p = 2$, la valuation vaut

$$(m(K,2) - t(K,2))\left[\frac{n}{t(K,2)}\right] \leq n\frac{m(K,2)-1}{t(K,2)} \leq n\frac{2^{m(K,2)-2}}{t(K,2)} = n\frac{[K^{(2)} : \mathbb{Q}]}{2}.$$

Nous en déduisons

$$\frac{S(n,K)}{S(n,\mathbb{Q})} \leq \prod_{p \mid K^{(p)} \neq \mathbb{Q}} \sqrt{3}^{n[K^{(p)} : \mathbb{Q}]}.$$

De plus

$$\sum_{p \mid K^{(p)} \neq \mathbb{Q}} [K^{(p)} : \mathbb{Q}] \leq \prod_{p \mid K^{(p)} \neq \mathbb{Q}} [K^{(p)} : \mathbb{Q}] = [L : \mathbb{Q}] \leq [K : \mathbb{Q}]$$

où L est le compositum de tous les $K^{(p)}$, l'égalité venant du fait que l'intersection de $\mathbb{Q}(\mu_{p^\infty})$ avec le compositum de tous les $\mathbb{Q}(\mu_{\ell^\infty})$ $(\ell \neq p)$ est $\mathbb{Q}$. En combinant, nous avons $S(n, K) \leq S(n, \mathbb{Q})3^g$. En majorant $S(n, \mathbb{Q}) \leq 5^n n!$ (voir corollaire 5.2), nous voyons que $[K : \mathbb{Q}]\mu_K \Gamma_K(n)$ vaut au plus

$$2 \times 3^g 5^n n![K : \mathbb{Q}] = 4g \times 3^g 5^n (n-1)! \leq 4g \times 3^g 5^{g/2}([g/2] - 1)!$$

puisque par hypothèse $n \leq g/2$ donc $n \leq [g/2]$. Il est alors élémentaire de vérifier que la quantité obtenue n'excède pas $f(g)/(1 + [g/12])$ (par exemple pour $g \geq 8$ il suffit d'employer $(g-1)! \geq [g/2]^{g/2}([g/2] - 1)! \geq 2^g([g/2] - 1)!$ et $4^g \geq 5^{g/2}(g + 12)$). $\square$

Cette proposition établit l'assertion (2) du théorème 3.8 (en oubliant $[g/12]$ qui sera exploité dans la partie suivante). Son assertion (1) est plus facile, nous pouvons la déduire des calculs déjà faits.

Lemme 5.5 *Nous avons $2\Gamma_{\mathbb{Q}}(g) \leq f(g)$.*

Démonstration. Pour tout corps de nombres K tel que $h_K \neq 1$ nous avons $\Gamma_{\mathbb{Q}}(g) \leq \Gamma_K(g) = \min(\Gamma_K(g), h_K \Gamma'_K(g))$. Il suffit donc d'appliquer la proposition 5.3 à un corps quadratique imaginaire bien choisi, comme par exemple $K = \mathbb{Q}(\sqrt{-6})$. $\square$

6 Cas exceptionnels

Dans cette partie, nous traitons les cas des corps quadratiques qui ne sont pas couverts par la proposition 5.3. Pour les corps non cyclotomiques, cela passe par plusieurs lemmes sur les sous-groupes finis du groupe linéaire. Rappelons qu'un sous-groupe G d'un groupe linéaire $\mathrm{GL}_g(K)$ est dit primitif si la représentation correspondante K^g de G ne peut être écrite comme somme directe de sous-espaces stricts permutés par G. Voici une conséquence facile de cette définition.

Lemme 6.1 *Soient K un corps de nombres et G un sous-groupe fini de $\mathrm{GL}_g(K)$. Si G n'est pas primitif alors l'une des deux assertions suivantes est vraie.*

(1) *Il existe un entier d avec $1 \leq d \leq g-1$ tel que $\mathrm{Card}G \leq S(d,K)S(g-d,K)$.*

(2) *Il existe un diviseur $s \geq 2$ de g tel que $\mathrm{Card}G \leq s!S(g/s,K)^s$.*

Démonstration. Si la représentation K^g de G n'est pas irréductible, il existe un sous-espace stable V de K^g de dimension d vérifiant $1 \leq d \leq g-1$. Notons W un supplémentaire stable de V de sorte que G s'identifie à un sous-groupe fini de $\mathrm{GL}(V) \times \mathrm{GL}(W) \simeq \mathrm{GL}_d(K) \times \mathrm{GL}_{g-d}(K)$. Sa première projection est donc de cardinal au plus $\mu_K \Delta'_K(d) = S(d,K)$, la seconde de cardinal au plus $S(g-d,K)$ donc nous sommes dans le cas (1). Supposons maintenant que K^g soit irréductible. Par hypothèse, nous pouvons écrire $K^g = V_1 \oplus \cdots \oplus V_s$ où G permute les V_i, transitivement par irréductibilité. En particulier, les V_i ont même dimension donc $s \mid g$ et $\dim V_i = g/s$ pour tout i. Le noyau de $G \to \mathfrak{S}_s$ laisse stables tous les V_i donc, comme ci-dessus, son cardinal divise $S(g/s,K)^s$ et nous en déduisons bien (2). □

La primitivité a la conséquence classique suivante (voir aussi la remarque page 762 de [C2]).

Lemme 6.2 *Soient K un corps, G un sous-groupe fini de $\mathrm{GL}_g(K)$ et H un sous-groupe abélien et distingué de G. Si G est primitif alors H est cyclique.*

Démonstration. Écrivons $K^g = V_1^{\oplus n_1} \oplus \cdots \oplus V_s^{\oplus n_s}$ la décomposition de K^g comme représentation de H où les V_i sont irréductibles et deux à deux non isomorphes et $n_i \geq 1$. Par le théorème de Clifford (voir page 255 de [Ja]), tous les V_i ont même dimension, tous les n_i sont égaux et G agit par permutations sur les sous-espaces $V_i^{\oplus n_i}$ de V. La primitivité force $s = 1$. Comme $K^g = V_1^{\oplus n_1}$ est une représentation fidèle de H, il en va de même de V_1 : H s'injecte dans $\mathrm{Hom}_H(V_1, V_1)$. La sous-K-algèbre engendrée par son image est, par le lemme de Schur (voir page 118 de [Ja]), un corps et ceci implique que H est cyclique. □

Ceci nous amène à considérer un sous-groupe cyclique distingué.

Lemme 6.3 *Soient K un corps quadratique non cyclotomique, G un sous-groupe fini de $\mathrm{GL}_g(K)$ et H un sous-groupe cyclique distingué de G. Si H contient strictement $\{I, -I\}$ alors $\mathrm{Card}G \leq f(g)$. Si, de plus, $g = 12$ et $K = \mathbb{Q}(\sqrt{-23})$ alors $\mathrm{Card}G \leq f(g)/4$.*

Démonstration. Notons $h = \mathrm{Card}H$ et $K' = K(\mu_h)$. En faisant agir G sur H par conjugaison, nous avons une suite exacte

$$0 \longrightarrow C_G(H) \longrightarrow G \longrightarrow \mathrm{Aut}(H)$$

où $C_G(H)$ est le sous-groupe de G des éléments qui commutent à tout élément de H. Par cyclicité, $\mathrm{Card}\mathrm{Aut}H = \varphi(h) = [\mathbb{Q}(\mu_h) : \mathbb{Q}] \leq 2[K' : K]$. L'action de H sur K^g fait de cet espace un espace vectoriel sur $K[H] \simeq K'$ donc $[K' : K] | g$ et

les éléments de $C_G(H)$ deviennent des K'-automorphismes donc nous avons une injection

$$C_G(H) \hookrightarrow \mathrm{GL}_{g/[K':K]}(K').$$

De cette façon, $\mathrm{Card} C_G(H) \leq \mu_{K'}\Delta'_{K'}(g/[K':K]) \leq \mu_{K'}\Gamma_{K'}(2g/[K':\mathbb{Q}])$. Par la suite exacte, nous avons $\mathrm{Card} G \leq 2[K':K]\mathrm{Card} C_G(H) = [K':\mathbb{Q}]\mathrm{Card} C_G(H)$, ce qui permet de conclure par la proposition 5.4 (puisque $h > 2$ assure $K' \neq K$ donc $[K':\mathbb{Q}] \geq 4$). Si $g = 12$ et $K = \mathbb{Q}(\sqrt{-23})$ alors $K' = \mathbb{Q}(\mu_h)$ est impossible et on utilise $\varphi(h) = [K':K]$. □

Quelques estimations numériques permettent d'exprimer la borne du lemme 6.1 en fonction de $f(g)$ dans les cas qui nous intéressent.

Lemme 6.4 *Soit (K, g) l'un des dix couples de la proposition 5.3. Si G est un sous-groupe fini non primitif de $\mathrm{GL}_g(K)$ alors $\mathrm{Card} G \leq f(g)/3$.*

Démonstration. Soit d un entier avec $1 \leq d \leq g-1$. Nous avons $S(d,K) \leq \min(2\Gamma_K(d), 2h_K\Gamma'_K(d))$ que nous majorons par $f(d)$ si $d \notin \{6, 12, 20\}$ et par $(9/2)f(d)$ sinon, d'après la proposition 5.3. De cette façon, si d et $g-d$ sont hors de $\{6, 12, 20\}$, il vient $S(d,K)S(g-d,K) \leq f(d)f(g-d) \leq f(g)/3$ par (N1) (voir lemme 3.3). De même, si $s|g$ et $g/s \notin \{6, 12, g\}$ alors $s!S(g/s,K)^s \leq s!f(g/s)^s \leq f(g)/4$ par (N3). Dans les quelques cas restants, on vérifie $(9/2)^2 f(d)f(g-d) \leq f(g)/3$ ou $s!((9/2)f(g/s))^s \leq f(g)/3$. La conclusion découle alors du lemme 6.1. □

Pour conclure dans le cas des corps non cyclotomiques, il nous reste à utiliser le théorème de Collins sur la fonction de Jordan j dont l'énoncé sera rappelé plus bas (proposition 7.2).

Proposition 6.5 *Lorsque K est un corps quadratique imaginaire et non cyclotomique, nous avons toujours $\min(2\Gamma_K(g), 2h_K\Xi_K(g)) \leq f(g)$.*

Démonstration. Comme $\Xi_K(g)$ divise $\Gamma'_K(g)$, nous pouvons supposer d'après la proposition 5.3 que (K, g) est l'un des dix couples listés dans cet énoncé. Pour ceux-ci nous allons montrer $2h_K\Xi_K(g) \leq f(g)$. Nous avons $h_K = 1$ pour tous les couples concernés sauf $(\mathbb{Q}(\sqrt{-23}), 12)$ pour lequel nous avons $h_K = 3$. Notons G un sous-groupe fini de $\mathrm{GL}_g(K)$ de cardinal maximal c'est-à-dire $\mathrm{Card} G = 2\Xi_K(g)$. Il nous suffit de montrer $\mathrm{Card} G \leq f(g)$ en général et $\mathrm{Card} G \leq f(g)/3$ si $g = 12$ et $K = \mathbb{Q}(\sqrt{-23})$. Si G n'est pas primitif, le lemme 6.4 donne directement le résultat. S'il est primitif, notons H un sous-groupe abélien distingué de G de cardinal maximal. Par le lemme 6.2, H est cyclique. Par maximalité, G puis H contiennent la matrice centrale $-I$. Si $H \neq \{I, -I\}$, le lemme 6.3 fournit la majoration souhaitée de $\mathrm{Card} G$. Si $H = \{I, -I\}$, nous avons $\mathrm{Card} G \leq 2j(g)$ par définition de la fonction de Jordan. Grâce à la proposition 7.2, nous vérifions $2j(6) = f(6)$ et $6j(g) \leq f(g)$ pour $g \in \{12, 20, 24\}$. □

Nous pouvons terminer la démonstration du théorème 3.8 grâce au théorème de Feit (voir théorème 7.1 ci-dessous) qui nous donne la valeur exacte de $\Xi_K(g)$ (sous la forme $\beta(m,g)m^{g-1}g!$) pour tout g lorsque $K = \mathbb{Q}(\mu_4)$ ou $K = \mathbb{Q}(\mu_6)$. En particulier, nous avons $\Xi_{\mathbb{Q}(\mu_6)}(g) = f(g)/2$ pour tout $g \neq 2$ et $\Xi_{\mathbb{Q}(\mu_6)}(2) = f(2)/4$. Ceci établit l'assertion (5) et l'assertion (3) pour $K = \mathbb{Q}(\mu_6)$ qui vérifie $h_K = 1$. Par ailleurs, nous observons $\Xi_{\mathbb{Q}(\mu_4)}(g) = f(g)/2$ si $g \leq 2$ et $\Xi_{\mathbb{Q}(\mu_4)}(g) \leq 3f(g)/8$ si $g \geq 3$ (pour $g \geq 9$ ceci s'écrit $4^{g-1} \leq 6^g/8$). Nous en déduisons l'assertion (4) et l'assertion (3) pour $K = \mathbb{Q}(\mu_4)$ puisqu'ici aussi $h_K = 1$. Le théorème 3.8 est donc entièrement établi (voir la proposition 5.4 et le lemme 5.5 pour (1) et (2)). D'après le lemme 3.9, il en va de même du théorème 3.1 et donc de tous les énoncés de l'introduction.

7 Appendice : un théorème de Feit

L'objectif de cette partie est d'établir le résultat suivant.

Théorème 7.1 *Si m est un entier pair non nul et $g \geq 1$ alors le cardinal maximal d'un sous-groupe fini de $\mathrm{GL}_g(\mathbb{Q}(\mu_m))$ vaut $\beta(m,g)m^g g!$ où $\beta(m,g)$ est un nombre rationnel égal à 1 sauf pour 19 couples (m,g) auxquels β associe les valeurs présentes dans le tableau ci-dessous*

m \ g	2	4	5	6	7	8	9	10
2	3/2	3		9/4	9/2	135/2	15/2	9/4
4	3	15/2	3/2	9/5		45/28		
6		5		7/6				
8	3/2							
10	3	3		9/5				
20	3/2							

Comme nous l'avons dit dans l'introduction, ce théorème a été annoncé par Feit en 1996 (voir [Fe] ; le résultat est aussi cité dans l'article plus accessible [BDEPS]) mais aucune démonstration n'en a été publiée. De plus, la valeur de $\beta(4,6)$ était donnée incorrectement égale à 1 au lieu de 9/5. Pour ces raisons, nous redémontrons cet énoncé.

La première étape consiste à montrer que $\mathrm{GL}_g(\mathbb{Q}(\mu_m))$ contient bien un sous-groupe de cardinal $\beta(m,g)m^g g!$. Il contient toujours un sous-groupe de cardinal $m^g g!$ (à savoir $\mu_m \wr \mathfrak{S}_g$, le sous-groupe engendré par les matrices de permutations et les matrices diagonales d'ordre fini). Dans les 18 cas listés dans les tables 1 et 2 de [BDEPS], on vérifie directement que le groupe mentionné possède le cardinal prescrit. Le groupe manquant est $\mathrm{ST}_8 \wr \mathfrak{S}_3 \subset \mathrm{GL}_6(\mathbb{Q}(\mu_4))$ (où ST_8 est vu dans $\mathrm{GL}_2(\mathbb{Q}(\mu_4))$, voir aussi la démonstration du lemme 2.3) de cardinal $6(\mathrm{Card}\mathrm{ST}_8)^3 = 6(96)^3 = (9/5)4^6 6!$.

Il nous reste à établir la majoration. Comme outil principal, nous utiliserons les résultats de Collins que nous rappelons maintenant. La fonction j de Jordan (voir introduction) qu'il a calculée peut être décrite de la manière suivante.

Proposition 7.2 *Pour tout $g \geq 2$, nous avons*

$$j(g) = \max\left((g+1)!, \max_{g=rs+t} r!j(s)^r j(t)\right)$$

où, dans le second maximum, $r \geq 1$, $s \in \{2,3,4,6\}$ et $t \in \{0,1,3,4\}$ et, par convention, $j(0) = 1$. De cette façon, j est déterminée par ses valeurs en $g \leq 6$. Explicitement, les valeurs sont données par le tableau

g	$j(g)$	g	$j(g)$	g	$j(g)$
1	1	7	$j(4)j(3) = 18 \cdot 6!^2$	12, 13	$6j(4)^3 = 6!^3 6^7$
2	60	8	$2j(4)^2 = 2 \cdot 6!^2 6^4$	14	$7!j(2)^7 = 7!60^7$
3	360	9	$j(6)j(3) = 5 \cdot 9!6^4$	15	$6j(4)^3 j(3) = 3 \cdot 6!^4 6^6$
4, 5	$6!6^2$	10	$j(4)j(6) = 6!7!6^6$	16, 17	$24j(4)^4 = 4 \cdot 6!^4 6^9$
6	$7!6^4$	11	$2j(4)^2 j(3) = 6!^3 6^4$	19	$24j(4)^4 j(3) = 2 \cdot 6!^5 6^9$

ainsi que par $j(g) = 60^{[g/2]}[g/2]!$ si $20 \leq g \leq 62$ ou $g \in \{18, 64, 66, 68, 70\}$ et par $j(g) = (g+1)!$ dans tous les autres cas.

Démonstration. L'inégalité $j(g) \geq (g+1)!$ s'obtient en plongeant le groupe symétrique $\mathfrak{S}_{g+1}$ dans $\mathrm{GL}_g(\mathbb{C})$. La minoration $j(g) \geq r!j(s)^r j(t)$ s'obtient par $(G_s \wr \mathfrak{S}_r) \times G_t \subset \mathrm{GL}_g(\mathbb{C})$ où $G_s \subset \mathrm{GL}_s(\mathbb{C})$ est un groupe fini primitif avec $[G_s : Z(G_s)] = j(s)$

et de même pour G_t. Ceci montre que $j(g)$ est au moins égal au maximum indiqué et l'égalité résulte de l'explicitation des cas par Collins : voir le théorème B de [C1] pour $g \geq 20$ et le théorème D pour $g < 20$. $\square$

En dimension 2, 4 et 8, nous emploierons une version plus précise que la simple borne $j(g)$. Elle se déduit également du travail de Collins par examen des petits cas.

Théorème 7.3 *Si G est un sous-groupe fini de $\mathrm{GL}_g(\mathbb{C})$ et $H \subset G$ un sous-groupe abélien et distingué de cardinal maximal alors*

(1) *si $g = 2$, $[G : H]$ est un diviseur strict de 120 ;*
(2) *si $g = 4$, $[G : H] = j(4) = 25920$ ou $[G : H] \leq 14400$;*
(3) *si $g = 8$, $[G : H] = j(8) = 2j(4)^2$ ou $[G : H] \leq j(4)^2$.*

Démonstration. Nous supposons d'abord $g \in \{2, 4\}$. Si G n'est pas primitif alors $[G : H]$ est majoré dans le cas (1) par $2j(1)^2 = 2$ et dans le cas (2) par $\max(j(1)j(3), 2j(2)^2) = 2j(2)^2 = 7200$. Nous pouvons donc supposer que G est primitif comme dans [C2] auquel renvoient toutes les références ci-dessous. Par le lemme 1, $H = Z(G)$ et H est cyclique. Nous reprenons les notations $F^*(G)$, $E(G)$ et $E_1(G)$ de la page 763 et notons, comme dans le théorème 5, $P_1, \ldots, P_r$ les quasi-composantes de G et $E_1, \ldots, E_s$ ses composantes (avec $r \geq 0$, $s \geq 0$ et $r + s \geq 1$). Nous rappelons que $E_1(G)$ est le sous-groupe de G engendré par tous les P_i et E_i puis $F^*(G) = Z(G)E_1(G)$. Si C est l'un des P_i ou E_i nous notons $c(C)$ sa contribution (page 771) c'est-à-dire la quantité $[C : Z(C)]\mathrm{Card}(\mathrm{Out}_c(C))$ où Out_c est le sous-groupe des automorphismes extérieurs provenant d'automorphismes agissant trivialement sur le centre (page 764). Le théorème 5 montre $[G : H] \mid s!c(P_1) \cdots c(P_r)c(E_1) \cdots c(E_s)$ où de plus la contribution des quasi-composantes est contrôlée par les théorèmes 4 et 6 et la remarque page 766. Nous retenons seulement que si $[P_i : Z(P_i)]$ (qui est une puissance paire d'un nombre premier) vaut 2^2, 3^2 ou 4^2 alors $c(P_i)$ divise respectivement 24, 216 ou 11520 et toute représentation fidèle de P_i est de degré $\geq [P_i : Z(P_i)]^{1/2}$. Considérons maintenant une composante E_i possédant une représentation irréductible de degré 2. Comme $E_i/Z(E_i)$ est un groupe simple non abélien, nous avons nécessairement $[E_i : Z(E_i)] \geq 60$. Appliquons alors le théorème 8 à E_i (vu dans $\mathrm{GL}_2(\mathbb{C})$). Ici $E(E_i) = E_i$ donc le théorème montre que E_i est isomorphe à l'extension $2.A_5$ d'où $c(E_i) = 120$ (voir aussi la table page 772). Raisonnons maintenant comme page 771. Si $g = 2$, $E_1(G)$ est nécessairement irréductible donc $r + s = 1$ et comme nous avons vu soit $c(P_1) \mid 24$ soit $c(E_1) \mid 120$, le théorème 5 donne bien $[G : H] \mid 120$. Par le théorème A, $[G : H] = 120$ est exclu donc (1) est établi. Si $g = 4$ et si $E_1(G)$ n'est pas irréductible, il a une représentation irréductible de dimension 2 donc comme dans le cas précédent $[G : H] \mid 120$. Si $E_1(G)$ est irréductible, chaque composante ou quasi-composante a une représentation de degré 2 ou 4 donc $r + s \leq 2$. Si $r + s = 2$, seules des représentations de dimension 2 apparaissent donc $c(P_i) \mid 120$ et $c(E_i) \mid 120$ donc par le théorème 5, $[G : H] \mid 2(120)^2 = 28800$. L'égalité est exclue par le théorème A donc $[G : H] \leq 14400$. Il reste à étudier les cas où $r + s = 1$. Si $r = 1$, $[G : H] \mid c(P_1) \mid 11520$. Si $s = 1$, l'unique composante E_1 a une représentation de degré 4 et nous lui appliquons le théorème 8. Comme ci-dessus $E_1/Z(E_1)$ est un groupe simple non abélien donc ou bien $E_1/Z(E_1) \simeq A_5$ ou bien $[E_1 : Z(E_1)] \geq 168$ et alors le théorème montre que E_1 est l'un des quatre groupes notés $2.L_3(2)$, $2.A_6$, $2.A_7$ et $2.\mathrm{PSp}_4(3)$. Cela nous donne 5 cas à examiner. Excepté pour le dernier, on montre facilement $c(E_1) \leq 14400$ (c'est direct lorsque E_1 est connu ; si $E_1/Z(E_1) \simeq A_5$ on peut utiliser $\mathrm{Aut}_c(E_1) \hookrightarrow \mathrm{Aut}(A_5) \simeq \mathfrak{S}_5$ pour majorer très largement $\mathrm{CardOut}_c(E_1) \leq 120$). Lorsque $E_1 = 2.\mathrm{PSp}_4(3)$, nous avons $[E_1 : Z(E_1)] = 25920$ et $\mathrm{CardOut}_c(E_1) = 2$. Comme $Z(E_1) \subset Z(G)$ et $F^*(G) = Z(G)E_1$, il vient $[F^*(G) : Z(G)] = [E_1 : E_1 \cap Z(G)] = 25920$ tandis que le

théorème 5 donne ici une injection de $G/F^*(G)$ dans $\mathrm{Out}_c(E_1)$. Par suite, $[G : H]$ vaut 25920 ou 51840 mais cette dernière valeur est exclue par le théorème A donc (2) est entièrement établi. Venons-en à (3). Si G est primitif, le théorème A donne directement $[G : H] \leq 960 \cdot 9!$ (la deuxième colonne comporte une petite coquille car $960 \cdot 9! = 348\,364\,800$ et non $348\,368\,800$) et donc $[G : H] \leq j(4)^2$. Si G n'est pas irréductible, nous avons $[G : H] \leq \max(j(7), j(2)j(6), j(3)j(5), j(4)^2) = j(4)^2$. Si G est irréductible et permute 4 ou 8 sous-espaces $[G : H] \leq \max(8!, 4!j(2)^4) \leq j(4)^2$. Il reste le cas où G permute 2 sous-espaces de dimension 4 : ici G s'écrit comme sous-groupe d'un groupe de la forme $G_1 \wr \mathfrak{S}_2$ où $G_1 \subset \mathrm{GL}_4(\mathbb{C})$ est primitif. L'assertion (2) s'applique à l'indice $[G_1 : Z(G_1)]$. Le sous-groupe $G \cap Z(G_1)^2$ de G est abélien et distingué donc $[G : H] \leq [G : G \cap Z(G_1)^2]$ par maximalité de H. D'après l'injection $G/G \cap Z(G_1)^2 \hookrightarrow (G_1 \wr \mathfrak{S}_2)/Z(G_1)^2$, nous pouvons même majorer $[G : H] \leq [G_1 \wr \mathfrak{S}_2 : Z(G_1)^2] = 2[G_1 : Z(G_1)]^2$. Si $[G_1 : Z(G_1)] \neq j(4)$, nous avons la conclusion en remarquant $2(14400)^2 \leq j(4)^2$. De même si l'injection ci-dessus n'est pas un isomorphisme, nous gagnons un facteur ≥ 2 donc $[G : H] \leq j(4)^2$. Nous supposons donc maintenant $[G_1 : Z(G_1)] = j(4)$ et $[G : G \cap Z(G_1)^2] = [G_1 \wr \mathfrak{S}_2 : Z(G_1)^2]$. Cette deuxième égalité signifie $G \cdot Z(G_1)^2 = G_1 \wr \mathfrak{S}_2$ donc $(G \cap G_1^2)Z(G_1)^2 = G_1^2$. Ceci entraîne que $H \cap G_1^2$ est distingué dans G_1^2. Ses deux projections sont donc des sous-groupes abéliens distingués de G_1 : par primitivité, ils sont centraux donc $H \cap G_1^2 \subset Z(G_1)^2$. Grâce à cette inclusion, l'indice $[G : H \cap G_1^2]$ vaut

$$\frac{[G_1 \wr \mathfrak{S}_2 : H \cap G_1^2]}{[G_1 \wr \mathfrak{S}_2 : G]} = \frac{[G_1 \wr \mathfrak{S}_2 : H \cap G_1^2]}{[Z(G_1)^2 : G \cap Z(G_1)^2]}$$

$$= [G_1 \wr \mathfrak{S}_2 : Z(G_1)^2][G \cap Z(G_1)^2 : H \cap G_1^2] = 2j(4)^2[G \cap Z(G_1)^2 : H \cap G_1^2].$$

Finalement, $H/H \cap G_1^2$ s'injecte dans $\mathfrak{S}_2$ donc ce même indice vaut $[G : H]$ ou $2[G : H]$. Nous voyons ainsi que $j(4)^2$ divise $[G : H] \leq 2[G_1 : Z(G_1)]^2 = 2j(4)^2$ d'où $[G : H] = j(4)^2$ ou $[G : H] = 2j(4)^2$. □

Nous aurons encore besoin d'estimations un peu fastidieuses mais élémentaires sur β (dont les deux premières rappellent le lemme 3.3).

Lemme 7.4 *Soient m, g, h et s quatre entiers naturels non nuls tels que $2 \mid m$ et $s \mid g$.*

(1) *Nous avons*

$$\beta(m, g)\beta(m, h) \leq \binom{g+h}{h}\beta(m, g+h).$$

(2) *Nous avons*

$$\beta(m, g/s)^s \leq \frac{g!}{s!(g/s)!^s}\beta(m, g).$$

(3) *Soit p un nombre premier. Si $p \mid m$, posons $q = p$ et sinon $q = p - 1$. Supposons $q \mid g$. Alors*

$$q\beta(mp, g/q)p^{g/q}(g/q)! \leq \beta(m, g)m^{g(1-1/q)}g!.$$

Démonstration. (1) Si $\beta(m, g) = \beta(m, h) = 1$, la majoration est évidente. Nous pouvons donc supposer (par symétrie) que (m, g) est l'un des 19 couples tels que $\beta(m, g) \neq 1$. Pour chacun, nous vérifions la formule lorsque $h \leq 10$. Si $h \geq 11$, nous avons $\beta(m, h) = \beta(m, g + h) = 1$ et

$$\beta(m, g) \leq \frac{135}{2} \leq 78 = \binom{2+11}{11} \leq \binom{g+11}{11} \leq \binom{g+h}{h}.$$

(2) Notons ici $h = g/s$. La formule est claire si h ou s vaut 1. L'expression

$$\left(\frac{(sh)!}{s!h!^s}\right)^{1/s}$$

est croissante en s et en h. En particulier, en utilisant $s \geq 2$, elle vaut au moins $\sqrt{3}$ si $h \geq 2$, $\sqrt{35}$ si $h \geq 4$ et $3\sqrt{715}$ si $h \geq 8$. Ces valeurs sont supérieures à $\beta(m,h)$ sauf pour $(m,h) = (4,2)$, $(10,2)$ et $(4,4)$. Dans ces trois cas, notre expression dépasse $\beta(m,h)$ pour $s \geq 4$ et l'on vérifie directement la formule pour $s = 2$ et $s = 3$ (en faisant intervenir seulement ici $\beta(m,g)$). (3) Si $p \mid m$ et p impair alors $2p^2 \mid mp$ donc $mp = 18$ ou $mp \geq 36$. En particulier, $\beta(mp, g/p) = 1$. La formule résulte ici simplement de $\beta(m,g) \geq 1$, $g! \geq (g/p)!$ et $m^{g(1-1/p)} \geq p^{g(1-1/p)} \geq p^{1+g/p}$. Si $p = 3$, $g = 2$ et $p \nmid m$, la formule se réduit à $3 \leq m\beta(m,2)$ ce qui est vrai. Si $p = 3$, $p \nmid m$ et $g = 4$, nous trouvons $3 \leq 2m^2\beta(m,4)$ tout aussi vrai. Dans les autres cas où p est impair et ne divise pas m, nous majorons $\beta(mp, g/q)$ par 5, minorons $\beta(m,g)$ par 1 et m par 2. En écrivant encore $g = (p-1)h$, il reste à établir

$$5 \leq \frac{2^{(p-2)h}((p-1)h)!}{(p-1)p^h h!}.$$

Comme le membre de droite croît lorsque h est remplacé par $h+1$ ou p par $p+1$, l'inégalité est vraie pour tous $(h,p) \neq (1,3),(2,3)$ car elle l'est pour $(3,3)$ et $(1,5)$. Reste le cas où $p = 2$ (et donc $p \mid m$). La formule à établir est ici $2\beta(2m, g/2)2^{g/2}(g/2)! \leq \beta(m,g)m^{g/2}g!$. Elle vaut pour $m = 2$ et $g \in \{6,8\}$ par vérification directe. Dans tous les autres cas, on constate que $\beta(2m, g/2) \leq \beta(m,g)$ donc le résultat découle de $2 \leq m$ et $2(g/2)! \leq g!$. □

Nous entamons à présent la démonstration de la majoration du théorème 7.1. Supposons par l'absurde qu'il existe un couple (m,g) et un sous-groupe fini G de $\mathrm{GL}_g(\mathbb{Q}(\mu_m))$ tels que $\mathrm{Card}G > \beta(m,g)m^g g!$. Nous imposons de plus que la dimension g soit minimale parmi les contre-exemples au théorème. Comme le sous-groupe de $\mathrm{GL}_g(\mathbb{Q}(\mu_m))$ engendré par le groupe $\mu_m I$ des matrices centrales d'ordre fini et G est encore fini, nous pouvons supposer $\mu_m I \subset G$.

Lemme 7.5 *Le sous-groupe G de $\mathrm{GL}_g(\mathbb{Q}(\mu_m))$ est primitif.*

Démonstration. Si la représentation de G dans $\mathbb{Q}(\mu_m)^g$ n'était pas irréductible, G serait isomorphe à un sous-groupe de $H \times H'$ pour des sous-groupes finis $H \subset \mathrm{GL}_h(\mathbb{Q}(\mu_m))$ et $H' \subset \mathrm{GL}_{h'}(\mathbb{Q}(\mu_m))$ où $g = h + h'$, $h \geq 1$, $h' \geq 1$. Par minimalité de g, nous avons $\mathrm{Card}G \leq (\mathrm{Card}H)(\mathrm{Card}H') \leq (\beta(m,h)m^h h!)(\beta(m,h')m^{h'}h'!)$. L'assertion (1) du lemme 7.4 montre que ce dernier majorant est au plus $\beta(m,g)m^g g! < \mathrm{Card}G$. Cette contradiction entraîne que la représentation est irréductible. Si elle n'était pas primitive, G permuterait $s \geq 2$ sous-espaces de $\mathbb{Q}(\mu_m)^g$ de dimension g/s. Nous aurions donc une injection de G dans $H \wr \mathfrak{S}_s$ où H est un sous-groupe fini de $\mathrm{GL}_{g/s}(\mathbb{Q}(\mu_m))$. La minimalité de G et l'assertion (2) du lemme 7.4 conduiraient alors à $\mathrm{Card}G \leq s!(\mathrm{Card}H)^s \leq s!m^g(g/s)!^s\beta(m,g/s)^s \leq \beta(m,g)m^g g! < \mathrm{Card}G$, contradiction qui démontre le lemme. □

Soit à présent H un sous-groupe abélien distingué de G, contenant $\mu_m I$.

Proposition 7.6 *Nous avons $H = \mu_m I$.*

Démonstration. Par le lemme 6.2, la primitivité entraîne que H est cyclique. Nous allons raisonner comme pour le lemme 6.3. Supposons $H \neq \mu_m I$ et choisissons un nombre premier p divisant $(\mathrm{Card}H)/m$ puis un sous-groupe H' de cardinal mp avec

$\mu_m I \subset H' \subset H$. Ce groupe H' est encore cyclique et distingué dans G. Ainsi G agit par conjugaison sur H' laissant $\mu_m I$ (central) fixe. Nous avons donc une suite exacte

$$0 \longrightarrow C_G(H') \longrightarrow G \longrightarrow \mathrm{Aut}_{\mu_m I}(H')$$

avec le commutant de H' dans G et le groupe des automorphismes de H' laissant fixe $\mu_m I$. Par cyclicité, $\mathrm{Card}\mathrm{Aut}_{\mu_m I}(H') = \varphi(mp)/\varphi(m) = q$ avec $q = p$ si $p \mid m$ et $q = p - 1$ sinon. D'un autre côté, l'action de H' sur $\mathbb{Q}(\mu_m)^g$ fait de cet espace un espace vectoriel de dimension g/q sur $\mathbb{Q}[H'] \simeq \mathbb{Q}(\mu_{mp})$. Le groupe $C_G(H')$ respecte cette structure donc s'injecte dans $\mathrm{GL}_{g/q}(\mathbb{Q}(\mu_{mp}))$ donc, par minimalité de g, nous avons $\mathrm{Card}C_G(H') \leq \beta(mp, g/q)(mp)^{g/q}(g/q)!$. Si nous combinons alors $\mathrm{Card}G \leq q\mathrm{Card}C_G(H')$ avec l'assertion (3) du lemme 7.4, nous trouvons $\mathrm{Card}G \leq \beta(m,g)m^g g!$ et cette contradiction donne la proposition. □

La connaissance de la fonction j restreint beaucoup le nombre de cas à considérer.

Lemme 7.7 *Le couple (m, g) est l'un des 34 suivants :*
- $(2, g)$ *pour* $2 \leq g \leq 16$ *ou* $g \in \{18, 20\}$ *;*
- $(m, 2)$ *pour* $4 \leq m \leq 28$ *et* $m \notin \{10, 20\}$ *;*
- $(4, 3)$, $(6, 3)$, $(4, 4)$, $(8, 4)$, $(4, 6)$, $(4, 8)$.

Démonstration. D'après la proposition 7.6, le groupe $\mu_m I$ est le plus grand sous-groupe abélien distingué de G donc $\mathrm{Card}G \leq j(g)m$. Vu l'hypothèse sur G, nous avons donc $j(g) > \beta(m,g)m^{g-1}g!$. Les couples de l'énoncé sont ceux qui vérifient cette inégalité. Pour les déterminer, on calcule pour chaque $g \leq 70$ la valeur $(j(g)/g!)^{1/(g-1)}$ qui donne une borne supérieure pour m puis l'on examine séparément les cas restants. Pour $g > 70$, cette même borne vaut $(g+1)^{1/(g-1)} < 2 \leq m$ donc de tels g n'apparaissent pas. □

Pour conclure la démonstration du théorème 7.1 par l'absurde, nous allons exclure successivement tous ces cas. Tout d'abord $m \neq 2$: en effet, les sous-groupes finis maximaux de $\mathrm{GL}_g(\mathbb{Q})$ pour $g \leq 20$ sont connus à conjugaison près, voir [NP]. Nous pouvons donc vérifier sur les tables données que tous les groupes présents sont de cardinal au plus $\beta(2,g)2^g g!$ (par le lemme 7.5, il suffit même de consulter seulement les groupes primitifs).

Dans les autres cas, nous combinons différents arguments. En particulier, nous utilisons les bornes de Schur : $\mathrm{Card}G \mid S(g, \mathbb{Q}(\mu_m))$ (voir partie 4, le calcul est direct car $\mathbb{Q}(\mu_m)^{(\ell)} = \mathbb{Q}(\mu_{m\ell})$). En dimension 2, 3, 4 et 8, elles nous suffisent à l'aide du théorème 7.3.

Lemme 7.8 *Nous avons $g = 6$.*

Démonstration. Supposons d'abord $g = 2$. Nous constatons que $S(2, \mathbb{Q}(\mu_m)) = 2m^2$ si $3 \mid m$ et $6m^2$ sinon. Comme nous avons $\beta(m,2)2m^2 < \mathrm{Card}G$, il vient $3 \nmid m$ et $\mathrm{Card}G \in \{3m^2, 6m^2\}$. Par le théorème 7.3, $(\mathrm{Card}G)/m$ est un diviseur strict de 120. Par le lemme 7.7, $5 \nmid m$. Comme $3m \mid (\mathrm{Card}G)/m \mid 120$, nous avons $m = 4$ ou $m = 8$. Dans les deux cas, $\mathrm{Card}G > \beta(m,2)2m^2$ conduit à une contradiction. Lorsque $g = 3$, la situation est encore plus simple puisque $S(3, \mathbb{Q}(\mu_m)) = 6m^3$ pour tout m donc $\mathrm{Card}G > \beta(m,3)6m^3 = 6m^3$ est impossible. Considérons ensuite le cas $g = 4$. Nous avons donc $m \in \{4, 8\}$. Ici $S(4, \mathbb{Q}(\mu_m)) = 15m^4 4!$ ce qui interdit $\mathrm{Card}G = 25920m$ (car $27 \mid 25920$). Ainsi, par le théorème 7.3, il vient $\mathrm{Card}G \leq 14400m$. Or le plus grand diviseur de $360m^4$ inférieur à $14400m$ se trouve être $24m^4\beta(m,4)$. L'existence de G conduit donc à nouveau à une contradiction. Finalement si $g = 8$, et donc $m = 4$, nous avons $S(8, \mathbb{Q}(\mu_4)) = 2^{23}3^5 5^2 7$ qui interdit $\mathrm{Card}G = j(8)m$ donc, par le théorème 7.3, $\mathrm{Card}G \leq j(4)^2 m < \beta(4,8)4^8 8!$ et ce cas est lui aussi impossible. □

Nous avons maintenant $m = 4$ et $g = 6$. En fixant la base $(1, i)$ de $\mathbb{Q}(\mu_4)$ (où $i^2 = -1$), nous identifions $\mathbb{Q}(\mu_4)^6$ à $\mathbb{Q}^{12}$ et voyons donc G dans $\mathrm{GL}_6(\mathbb{Q}(\mu_4)) \subset \mathrm{GL}_{12}(\mathbb{Q})$. Nous savons que G agit primitivement sur $\mathbb{Q}(\mu_4)^6$, examinons son action sur $\mathbb{Q}^{12}$. Si $V \subset \mathbb{Q}^{12}$ est un sous-$\mathbb{Q}$-espace vectoriel stable par G alors, comme $iI \in G$, nous avons $iV = V$ donc V est aussi un sous-$\mathbb{Q}(\mu_4)$-espace de $\mathbb{Q}(\mu_4)^6$. La représentation $\mathbb{Q}^{12}$ de G est donc irréductible. Supposons maintenant qu'elle ne soit pas primitive. Alors G permute une famille S de sous-$\mathbb{Q}$-espaces de $\mathbb{Q}^{12}$ en somme directe. Si $V \in S$ alors $iV \neq V$ car V ne peut être un $\mathbb{Q}(\mu_4)$-espace et $iV \in S$. En regroupant deux par deux les sous-espaces de S, nous voyons que G permute les $V \oplus iV$ qui sont des sous-$\mathbb{Q}(\mu_4)$-espaces de $\mathbb{Q}(\mu_4)^6$. Par primitivité de la $\mathbb{Q}(\mu_4)$-action de G, ceci force $S = \{V, iV\}$ pour un sous-espace V de dimension 6 sur $\mathbb{Q}$. Mais ici le sous-groupe d'indice 2 de G qui fixe V s'identifie à un sous-groupe fini de $\mathrm{GL}_6(\mathbb{Q})$ donc $\mathrm{Card}G \leq 2\beta(2,6)2^6 6! < \beta(4,6)4^6 6!$. Ceci nous permet donc de supposer que G est encore primitif comme sous-groupe de $\mathrm{GL}_{12}(\mathbb{Q})$. Choisissons alors $G_1 \subset \mathrm{GL}_{12}(\mathbb{Q})$ fini, maximal pour l'inclusion et contenant G. Ce sous-groupe est *a fortiori* primitif donc il est conjugué à l'un des onze groupes donnés par Nebe et Plesken dans leur classification (voir la table page 36 de [NP]). Supposons d'abord que G_1 soit conjugué au groupe qu'ils notent $\mathrm{Aut}(A_{12})$ c'est-à-dire $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_{13}$ plongé dans $\mathrm{GL}_{12}(\mathbb{Q})$ à l'aide de la représentation standard de $\mathfrak{S}_{13}$ et $(1, \mathrm{id}) \mapsto -I$. Maintenant l'élément iI de G donne après conjugaison une matrice M de $\mathrm{GL}_{12}(\mathbb{Q})$ vérifiant $M^2 = -I$. Elle ne peut appartenir à l'image de $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_{13}$ puisque aucun élément (x, σ) de ce groupe ne peut satisfaire $(x, \sigma)^2 = (2x, \sigma^2) = (0, \sigma^2) = (1, \mathrm{id})$. Cette contradiction montre que G_1 est conjugué à l'un des dix autres sous-groupes primitifs listés par Nebe et Plesken. En consultant les cardinaux possibles, nous constatons $2^{11} \not| \mathrm{Card}G_1$ donc $2^{11} \not| \mathrm{Card}G$. Une dernière application de la borne de Schur montre $\mathrm{Card}G \mid S(6, \mathbb{Q}(\mu_4)) = 2^{16}3^4 5 \cdot 7$ et nous en déduisons $\mathrm{Card}G \mid 2^{10}3^4 5 \cdot 7 < 4^6 6!$. Cet ultime cas est encore exclu et la démonstration du théorème 7.1 est donc terminée.

Références

[BDEPS] N. Berry, A. Dubickas, N. Elkies, B. Poonen et C. Smyth. The conjugate dimension of algebraic numbers. *Q. J. Math.* 55. 2004. p. 237–252.

[CF] J. Cassels et A. Fröhlich. *Algebraic number theory.* Academic Press. Londres. 1986.

[C1] M. Collins. On Jordan's theorem for complex linear groups. *J. Group Theory* 10. 2007. p. 411–423.

[C2] M. Collins. Bounds for finite primitive complex linear groups. *J. Algebra* 319. 2008. p. 759–776.

[Fe] W. Feit. Orders of finite linear groups. *Proceedings of the First Jamaican Conference on Group Theory and its Applications.* The University of the West Indies. Kingston. 1996. p. 9–11.

[FKRS] F. Fité, K. Kedlaya, V. Rotger et A. Sutherland. Sato-Tate distributions and Galois endomorphism modules in genus 2. *Compos. Math.* 148. 2012. p. 1390–1442.

[FJ] M. Fried et M. Jarden. *Field arithmetic.* Springer-Verlag. Berlin. 2008.

[GK] R. Guralnick et K. Kedlaya. Endomorphism fields of abelian varieties. *Research in Number Th.* 3. 2017. p. 1–10.

[GL] R. Guralnick et M. Lorenz. Orders of finite groups of matrices. *Groups, rings and algebras*, p. 141–161. Contemp. Math. 420. Amer. Math. Soc. Providence. 2006.

[Ja] N. Jacobson. *Basic algebra II.* Seconde édition. Freeman. New York. 1989.

[Ka] Y. Katznelson. On the orders of finite subgroups of GL(n,Z). *Exposition. Math.* 12. 1994. p. 453–457.

[LT] G. Lehrer et D. Taylor. *Unitary reflection groups.* Australian Mathematical Society Lecture Series, 20. Cambridge University Press. Cambridge. 2009.

[Mu] D. Mumford. *Abelian varieties.* Oxford University Press. London. 1974.

[NP] G. Nebe et W. Plesken. Finite rational matrix groups. *Mem. Amer. Math. Soc.* 116. 1995.

[Re] I. Reiner. *Maximal orders*, volume 28 de *London Mathematical Society Monographs. New Series.* The Clarendon Press Oxford University Press. 2003.

[Sa] I. Satake. *Classification theory of semi-simple algebraic groups.* Lecture Notes in Pure and Applied Mathematics, 3. Marcel Dekker. New York. 1971.

[Se] J.-P. Serre. *Cohomologie galoisienne.* Lecture Notes in Mathematics, 5. Springer-Verlag. Berlin. 1994.

[ST] G. Shephard et J. Todd. Finite unitary reflection groups. *Canadian J. Math.* 6. 1954. p. 274–304.

[Si] A. Silverberg. Fields of definition for homomorphisms of abelian varieties. *J. Pure Appl. Algebra.* 77. 1992. p. 253–262.

[S1] J. Silverman. *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106. Springer. Dordrecht. 2009.

[S2] J. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151. Springer-Verlag. New York. 1994.

Gaël Rémond
Institut Fourier, UMR 5582
CS 40700
38058 Grenoble Cedex 9
France
`Gael.Remond@univ-grenoble-alpes.fr`