Sous-groupes finis de $\mathrm{GL}_n(\mathbb{Q})$

Samuel Baumard Pierre Lairez

24 juin 2008

Sujet d'exposé de maîtrise
proposé par Philippe Gille

L'objet de ce mémoire est un résultat de Hermann Minkowski datant de 1887 qui majore la taille des sous-groupes finis de $\mathrm{GL}_n(\mathbb{Q})$. Nous suivons principalement la présentation faite par Jean-Pierre Serre dans un exposé récent [Ser07], puis celle de R. M. Guralnick et M. Lorenz [GL06].

Dans une première partie, nous énonçons et prouvons ledit théorème ; les outils utilisés dans la démonstration sont pour la plupart élémentaires, à l'exception d'un résultat général de théorie des caractères.

La deuxième partie donne une généralisation simple du théorème de Minkowski, découverte par Issai Schur en 1905 [Sch73]. Sa démonstration fait intervenir la théorie des caractères et des représentations des groupes finis.

En troisième partie, on explicite rapidement, à isomorphisme près, les sous-groupes finis de $\mathrm{GL}_2(\mathbb{Q})$, en vérifiant au passage un cas très particulier des théorèmes vus auparavant.

Enfin, la quatrième et dernière partie présente une généralisation de ces deux théorèmes, elle aussi démontrée par Schur en 1905 : le corps initial $\mathbb{Q}$ est alors remplacé par un corps de nombres quelconque. La preuve utilise la théorie des anneaux d'entiers de ces corps de nombres.

Table des matières

1 Théorème de Minkowski

1.1 Notations

Dans tout cet exposé, ℓ désigne un nombre premier, $[x]$ la partie entière du réel x, $v_\ell(n)$ la valuation ℓ-adique de l'entier n. Pour un ensemble fini A, $v_\ell(A)$ désigne la valuation ℓ-adique du cardinal de A. La notation $G \leqslant H$, si H est un groupe, signifie que G est un sous-groupe de H. Le symbole $\wedge$ désigne le pgcd.

1.2 Énoncé

Théorème 1. *Pour tout entier n et tout nombre premier ℓ, posons*

$$M(n,\ell) = r + v_\ell(r!) = \sum_{i=0}^{\infty} \left[\frac{n}{\ell^i(\ell-1)} \right]$$

avec $r = [\frac{n}{\ell-1}]$. Définissons de plus $M(n) = \prod_\ell \ell^{M(n,\ell)}$.

(i) Si G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Q})$, alors $|G|$ divise $M(n)$.

(ii) Les ℓ-sous-groupes de $\mathrm{GL}_n(\mathbb{Q})$ maximaux pour l'inclusion sont conjugués deux à deux et d'ordre $\ell^{M(n,\ell)}$.

Commençons par quelques remarques. Ce théorème n'est pas valable pour un corps quelconque, puisqu'il existe par exemple des matrices d'ordre arbitrairement grand à coefficients dans $\mathbb{C}$ ou même dans $\mathbb{R}$. Cependant, on verra qu'une majoration existe toujours lorsqu'on remplace $\mathbb{Q}$ par un corps de nombres.

De plus, le point (ii) du théorème est à rapprocher des théorèmes de Sylow pour les groupes finis. En effet, les deux premiers théorèmes de Sylow peuvent s'exprimer ainsi :

> *Si G est un groupe fini et ℓ un nombre premier, alors tous les ℓ-sous-groupes maximaux de G sont conjugués et d'ordre $\ell^{v_\ell(G)}$.*

La démonstration de Minkowski se développe en trois parties :

— On montre que tout $G \leqslant \mathrm{GL}_n(\mathbb{Q})$ fini est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$ ou d'un groupe orthogonal $\mathrm{O}_n(\mathbb{F}_p)$. Un p bien choisi prouvera le point (i).
— On exhibe ensuite un ℓ-sous-groupe de $\mathrm{GL}_n(\mathbb{Q})$ de cardinal $\ell^{M(n,\ell)}$.
— Pour voir que les ℓ-sous-groupes maximaux de $\mathrm{GL}_n(\mathbb{Q})$ sont conjugués deux à deux, on se ramène enfin à un problème de Sylow dans $\mathrm{GL}_n(\mathbb{F}_p)$.

1.3 Borne multiplicative

1.3.1 Quelques isomorphismes

La première étape de la démonstration consiste à se ramener à l'étude de matrices à coefficients entiers. On introduit pour cela la notion de réseau de $\mathbb{Q}^n$.

Proposition - définition 2. *Soit R un sous-$\mathbb{Z}$-module de $\mathbb{Q}^n$. Les deux assertions suivantes sont équivalentes :*

(i) R est de type fini, et engendre le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^n$;

(ii) R est libre de rang n.

Dans l'un ou l'autre cas, on dit que c'est un réseau *de $\mathbb{Q}^n$.*

Corollaire 3. *Une somme finie de réseaux (en tant que $\mathbb{Z}$-modules) est encore un réseau.*

Démonstration. C'est immédiat en utilisant la première caractérisation : une somme finie de modules de type fini est encore de type fini. □

Démonstration (de la proposition 2). Prouvons l'équivalence annoncée.

(i) $\Longrightarrow$ (ii) : soit $\mathcal{F}$ une famille génératrice finie du $\mathbb{Z}$-module R ; on peut donc écrire $R = \sum_{e\in\mathcal{F}} \mathbb{Z}e$. On en déduit que $\mathbb{Q}^n = \mathrm{Vect}_{\mathbb{Q}} \sum_{e\in\mathcal{F}} \mathbb{Z}e = \sum_{e\in\mathcal{F}} \mathbb{Q}e$: en particulier, $\mathcal{F}$ engendre $\mathbb{Q}^n$, et on peut en extraire une $\mathbb{Q}$-base $\mathcal{B} = (e_i)_{i\in[\![1,n]\!]}$. Par suite, tout élément x de $\mathcal{F}$ se décompose sous la forme $x = \sum q_i e_i$, où les q_i sont rationnels ; en notant d un dénominateur commun des q_i, on trouve par conséquent

$$\bigoplus_{i=1}^{n} \mathbb{Z}e_i \subset R \subset \frac{1}{d}\bigoplus_{i=1}^{n} \mathbb{Z}e_i$$

ce qui prouve d'une part que R est libre comme sous-module d'un module libre sur un anneau principal, et d'autre part qu'il est de rang n.

(ii) $\Longrightarrow$ (i) : soit $\mathcal{B}$ une $\mathbb{Z}$-base de R. Il s'agit en particulier d'une famille $\mathbb{Q}$-libre : en chassant les dénominateurs, on voit qu'une relation de liaison à coefficients rationnels impliquerait une relation de liaison à coefficients entiers. On en déduit donc que $\mathcal{B}$ est une $\mathbb{Q}$-base de $\mathbb{Q}^n$, et le résultat. □

Remarque. Faisons une remarque d'apparence triviale mais qui sera utile par la suite : dans la démonstration de la proposition, on a en fait utilisé le fait que $\mathbb{Z}$ est principal, en particulier factoriel, et que $\mathbb{Q}$ est son corps des fractions.

Dans la suite de ce paragraphe, on désigne par G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Q})$.

Lemme 1. *Le groupe G est conjugué à un sous-groupe de $\mathrm{GL}_n(\mathbb{Z})$.*

Démonstration. L'idée est de montrer que G stabilise un réseau de $\mathbb{Q}^n$. Posons $R = \sum_{g\in G} g\mathbb{Z}^n$, qui est un réseau par le corollaire 3. De plus, il est bien stable par G. Ainsi, dans une $\mathbb{Z}$-base de R, les matrices de G sont à coefficients entiers, ce qui prouve le lemme. □

Lemme 2. *Il existe une forme quadratique q sur $\mathbb{Q}^n$ définie positive et à coefficients entiers telle que $G \leqslant \mathrm{O}(q)$, où $\mathrm{O}(q)$ est l'ensemble des matrices de $\mathrm{GL}_n(\mathbb{Q})$ orthogonales pour la forme q.*

Démonstration. Le procédé est assez semblable à celui du lemme précédent. Posons $q(x) = \sum_{i=1}^{n} x_i^2$ pour des $x \in \mathbb{Q}^n$; c'est une forme quadratique définie positive sur $\mathbb{Q}^n$. Quitte à la multiplier par un entier, $\sum_{g\in G} q \circ g$ convient. □

1.3.2 Réduction dans $\mathbb{F}_p$

Lemme 3 (Minkowski)**.** *Soit $m \geqslant 3$. Alors le noyau du morphisme canonique $\varphi : \mathrm{GL}_n(\mathbb{Z}) \longrightarrow \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$ est sans torsion. En d'autres termes, l'identité est le seul élément d'ordre fini de $\mathrm{Ker}\,\varphi$.*

Démonstration. Supposons au contraire qu'il existe $g \in \mathrm{Ker}\,\varphi$, $g \neq 1$ et q entier tels que $g^q = 1$. Quitte à élever g à une certaine puissance, on peut supposer que q est premier.

Il existe $h \in \mathcal{M}_n(\mathbb{Z})$ non nulle à coefficients premiers entre eux dans leur ensemble et $d > 0$ tels que $g = 1 + mdh$. En écrivant $g^q = 1$, on obtient

$$\sum_{k=1}^{q} \binom{q}{k} (md)^k h^k = 0.$$

En particulier, m divise les coefficients de qh car

$$qh + \binom{q}{2} mdh^2 + \underbrace{\cdots}_{\text{multiple de } m} = 0.$$

Par hypothèse sur les coefficients de h, on en déduit que m divise q, et donc par primalité que $q = m$. Comme q est impair (car $m \geqslant 3$), il divise $\binom{q}{2}$. Puisque

$$h + \binom{q}{2} dh^2 + \underbrace{\cdots}_{\text{multiple de } q} = 0,$$

l'entier q divise tous les coefficients de h : c'est absurde. □

Corollaire 4. *Si G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$, $G \cap \operatorname{Ker} \varphi = \{1\}$.*

Remarque. En fait, seul le corollaire servira, et même une forme plus faible et évidente : pour m assez grand, $\varphi_{\restriction G}$ est une injection.

1.3.3 Lemmes calculatoires

Nous allons calculer explicitement la valuation de l'ordre de certains groupes de matrices, ce qui nous permettra de conclure quant au premier point du théorème.

Lemme 4. *Pour $\ell > 2$, et p premier générateur de $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$,*

$$v_\ell(\mathrm{GL}_n(\mathbb{F}_{p^r})) = (1 + v_\ell(r)) \left[\tfrac{n}{\tau}\right] + v_\ell\left(\left[\tfrac{n}{\tau}\right]!\right)$$

avec $\tau = \frac{\ell-1}{r \wedge (\ell-1)}$.

Remarque. Le théorème de la progression arithmétique de Dirichlet (voir par exemple [Hino8], théorème 1.4) assure l'existence d'une infinité de tels p. De plus, pour $r = 1$, le membre de droite est précisément la borne $M(n, \ell)$.

Démonstration. Montrons que pour $i > 0$,

$$v_\ell(p^i - 1) = \begin{cases} 1 + v_\ell(i) & \text{si } \ell - 1 \text{ divise } i \\ 0 & \text{sinon.} \end{cases}$$

D'abord, p est premier avec ℓ^2, donc avec ℓ. De plus, si $p^i \equiv 1 \pmod{\ell}$, alors $p^{\ell i} \equiv 1 \pmod{\ell^2}$ et $\varphi(\ell^2) = \ell(\ell-1) \mid \ell i$, d'où $\ell - 1 \mid i$. La réciproque étant facile, on en déduit que $p^i \equiv 1 \pmod{\ell}$ si et seulement si $\ell - 1 \mid i$.

Supposons maintenant que i est de la forme $m(\ell-1)\ell^k$ avec m premier avec ℓ et raisonnons par récurrence sur k. Notons $s = p^{m(\ell-1)}$.

Si $k = 0$, alors $\ell \mid p^i - 1$, mais $\ell^2 \nmid p^i - 1$ car $\ell(\ell-1) \nmid m(\ell-1)$. Pour $k > 0$, posons par hypothèse de récurrence $s^{\ell^{k-1}} - 1 = u\ell^k$, avec $\ell \nmid u$. Alors

$$s^{\ell^k} = \left(1 + u\ell^k\right)^\ell = 1 + u\ell^{k+1} + \underbrace{\sum_{j=2}^{\ell} \binom{\ell}{j} u^j \ell^{jk}}_{\text{multiple de } \ell^{k+2} \text{ car } \ell > 2}$$

et donc $v_\ell(s^{\ell^k}-1) = 1+k$.

Notons à présent $q = p^r$. Alors, si $\ell - 1$ divise i, c'est que τ divise i. Comme $v_\ell\left(\mathrm{GL}_n(\mathbb{F}_q)\right) = v_\ell\Big(q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(q^i-1)\Big)$ et $p \neq \ell$, on a finalement

$$\begin{aligned} v_\ell(\mathrm{GL}_n(\mathbb{F}_q)) &= \sum_{\substack{1\leqslant i\leqslant n \\ \tau | i}} (1 + v_\ell(ri)) = \left[\tfrac{n}{\tau}\right](1+v_\ell(r)) + \sum_{1\leqslant j\leqslant [\frac{n}{\tau}]} v_\ell(j) \\ &= \left[\tfrac{n}{\tau}\right](1+v_\ell(r)) + v_\ell\left(\left[\tfrac{n}{\tau}\right]!\right) \end{aligned}$$

qui est l'identité annoncée. □

Lemme 5. *Soit p premier congru à ± 3 modulo 8. Soit q une forme quadratique sur $\mathbb{F}_p$ non dégénérée. Notons $\mathrm{O}_n(\mathbb{F}_p)$ le groupe des matrices orthogonales pour q. Alors $v_2(\mathrm{O}_n(\mathbb{F}_p)) \leqslant M(n,2)$, et on a même égalité pour n impair.*

Démonstration. Notons Δ le discriminant de q et ε le symbole de Legendre $\left(\frac{(-1)^k\Delta}{p}\right)$. On montre par récurrence (voir par exemple [Gro02]) que

$$\begin{aligned} |\mathrm{O}_{2k}(\mathbb{F}_p)| &= 2p^{k(k-1)}(p^k-\varepsilon)\prod_{i=1}^{k-1}(p^{2i}-1) \\ \text{et} \quad |\mathrm{O}_{2k+1}(\mathbb{F}_p)| &= 2p^{k^2}\prod_{i=1}^{k}(p^{2i}-1). \end{aligned}$$

Un calcul direct mène alors au résultat, en remarquant que $\frac{p^{2k}-1}{p^k-\varepsilon} = p^k+\varepsilon$ est pair et en vérifiant par récurrence sur i que, si $p \equiv \pm 3 \pmod 8$, $v_2(p^{2i}-1) = 3 + v_2(i)$, de la même manière que dans la preuve du lemme 4. □

1.3.4 Preuve du premier point

Soient G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Q})$ et ℓ un nombre premier. Montrons que $v_\ell(G) \leqslant M(n,\ell)$. Par le lemme 1, on peut supposer que $G \leqslant \mathrm{GL}_n(\mathbb{Z})$.

- Cas $\ell > 2$.

Choisissons p un nombre premier impair générateur de $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$. Le corollaire du lemme 3 indique que la réduction $\varphi : G \longrightarrow \mathrm{GL}_n(\mathbb{F}_p)$ est une injection. Comme $|G| = |\varphi(G)|$ divise $|\mathrm{GL}_n(\mathbb{F}_p)|$, le lemme 4 assure que $v_\ell(G) \leqslant M(n,\ell)$.

- Cas $\ell = 2$.

Soit q une forme quadratique donnée par le lemme 2. En choisissant p premier congru à ± 3 modulo 8 et strictement plus grand que le discriminant de q, la réduction de q dans $\mathbb{F}_p$ donne une forme quadratique non dégénérée. L'injection $\varphi : G \longrightarrow \mathrm{GL}_n(\mathbb{F}_p)$ est donc à valeurs dans $\mathrm{O}_n(\mathbb{F}_p)$, relativement à q. Le lemme 5 assure que $v_\ell(G) \leqslant M(n,\ell)$. □

1.4 Optimalité de la borne

Théorème 1'. *Soit ℓ premier. Il existe un sous-groupe fini G de $\mathrm{GL}_n(\mathbb{Q})$ tel que $v_\ell(G) = M(n,\ell)$.*

Démonstration. On utilise la représentation standard de $\mathfrak{S}_\ell$ dans un $\mathbb{Q}$-espace vectoriel V_0 de dimension $\ell - 1$. Soient $r = [\frac{n}{\ell-1}]$ et $V = V_0^r$. Soit ensuite

$G = \mathfrak{S}_\ell \wr \mathfrak{S}_r = \mathfrak{S}_\ell^r \rtimes \mathfrak{S}_r$ le produit en couronne obtenu grâce à l'action de $\mathfrak{S}_r$ par permutation des r-uplets de $\mathfrak{S}_\ell^r$. Ce groupe agit de façon naturelle sur V, et l'action est fidèle. Par conséquent, G s'injecte dans $\mathrm{GL}_{r(\ell-1)}(\mathbb{Q})$, et donc dans $\mathrm{GL}_n(\mathbb{Q})$. De plus, $v_\ell(G) = r + v_\ell(r!) = M(n,\ell)$, ce que l'on cherchait. □

1.5 Les ℓ-sous-groupes maximaux de $\mathrm{GL}_n(\mathbb{Q})$

Théorème 1". *Soient G et H des ℓ-sous-groupes de $\mathrm{GL}_n(\mathbb{Q})$. Si $v_\ell(G) = M(n,\ell)$, alors H est conjugué à un sous-groupe de G.*

Remarque. Les théorèmes 1' et 1" montrent bien le second point du théorème 1. En effet, le théorème 1' assure l'existence d'un sous-groupe G de $\mathrm{GL}_n(\mathbb{Q})$ de cardinal $\ell^{M(n,\ell)}$. Notons H un ℓ-sous-groupe maximal de $\mathrm{GL}_n(\mathbb{Q})$ pour l'inclusion. Le théorème 1" assure que H est conjugué à un sous-groupe de G, et donc, en inversant la conjugaison, que H est contenu dans un ℓ-sous-groupe de cardinal $\ell^{M(n,\ell)}$. Par maximalité de H, son cardinal est égal à $\ell^{M(n,\ell)}$ et il est donc conjugué à G.

Démonstration du théorème. Commençons par remarquer qu'un tel G existe, il suffit de prendre un ℓ-Sylow du groupe construit en 1.4.

- Cas $\ell > 2$.

On suppose que G et H sont dans $\mathrm{GL}_n(\mathbb{Z})$. Soit p premier, supérieur à $2n+1$ et générateur de $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$. Notons $\overline{G}$ et $\overline{H}$ les images respectives de G et de H dans $\mathrm{GL}_n(\mathbb{F}_p)$. Par le lemme 3, la réduction modulo p est injective, donc $\overline{G} \simeq G$ et $\overline{H} \simeq H$.

Par ailleurs, le lemme 4 et l'hypothèse $v_\ell(G) = M(n,\ell)$ impliquent que $\overline{G}$ est un ℓ-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$. Comme $\overline{H}$ est un ℓ-sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$, les théorèmes de Sylow assurent l'existence de $g \in \mathrm{GL}_n(\mathbb{F}_p)$ tel que $g\overline{H}g^{-1} \subset \overline{G}$. En relevant la conjugaison par g dans $\mathrm{GL}_n(\mathbb{Z})$, on obtient un morphisme injectif $\rho : H \to G$, qui n'est *a priori* pas intérieur.

Ceci permet de construire deux représentations différentes de H dans $\mathbb{Q}^n$:

$$H \hookrightarrow \mathrm{GL}_n(\mathbb{Q})$$
$$\text{et} \quad H \xhookrightarrow{\rho} G \hookrightarrow \mathrm{GL}_n(\mathbb{Q}).$$

Notons χ_0 et χ_ρ les caractères respectifs de ces deux représentations. Il sont à valeurs dans $\mathbb{Z}$. Notons $\overline{\chi}_0$ et $\overline{\chi}_\rho$ leurs réductions modulo p. Comme ρ est une conjugaison dans $\mathrm{GL}_n(\mathbb{F}_p)$ et que les caractères sont invariants par conjugaison, $\overline{\chi}_0 = \overline{\chi}_\rho$. Puisque χ_0 et χ_ρ sont bornés par n et que $p > 2n$, l'égalité $\overline{\chi}_0 = \overline{\chi}_\rho$ dans $\mathbb{F}_p$ implique l'égalité $\chi_0 = \chi_\rho$ dans $\mathbb{Z}$.

Comme $\mathbb{Q}$ est de caractéristique nulle, les représentations sont déterminées à isomorphisme près par leur caractère ; voir [Lan02], chapitre XVIII, théorème 2.3. Donc les deux représentations de H sont isomorphes, c'est-à-dire que ρ est une conjugaison dans $\mathrm{GL}_n(\mathbb{Q})$.

- Cas $\ell = 2$.

Contentons-nous de donner une ébauche de démonstration. Si n est impair, on se sert de groupes orthogonaux de façon similaire à ce qui a été fait au paragraphe 1.3.4. Si n est pair, on se ramène au cas où n est impair en plongeant $G \leqslant \mathrm{GL}_n(\mathbb{Q})$ dans $G \times \{\pm 1\} \leqslant \mathrm{GL}_{n+1}(\mathbb{Q})$, et en utilisant le fait que $M(n+1,2) = 1 + M(n,2)$. □

2 Traces et représentations

En 1905, Schur a donné une généralisation du théorème de Minkowski, dont la preuve s'appuie plutôt sur la théorie des caractères de groupes finis :

Théorème 5. *Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$ dont la trace de chaque élément soit rationnelle. Alors $v_\ell(G) \leqslant M(n, \ell)$.*

Nous commencerons par montrer que ce résultat est plus fort que celui de Minkowski si $n = 2$, puis nous verrons comment Schur l'a prouvé.

2.1 Domaine d'application

Il est clair que le théorème 1 est une conséquence du théorème 5. D'autre part, il existe des cas où l'on peut dans un certain sens appliquer le second, mais pas le premier. Voici un exemple emprunté à [GL06].

Considérons les deux matrices complexes

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad h = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Ces matrices engendrent un sous-groupe à huit éléments de $\mathrm{GL}_2(\mathbb{C})$, isomorphe au groupe des quaternions, que nous noterons encore $\mathbb{H}_8$. La trace de chaque élément de $\mathbb{H}_8$ est rationnelle, valant en fait 0, 2 ou -2. Le théorème de Schur s'applique donc, même s'il n'est pas d'un grand intérêt ici. Cependant, il serait difficile d'utiliser le théorème de Minkowski : en effet, il est impossible de conjuguer $\mathbb{H}_8$ à un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.

Supposons par l'absurde qu'il existe $a \in \mathrm{GL}_2(\mathbb{C})$ telle que $a\mathbb{H}_8a^{-1} \leqslant \mathrm{GL}_2(\mathbb{R})$. Notons $x = aga^{-1}$, $y = aha^{-1}$ et $z = xy$. On doit encore avoir $\det x = \det y = 1$ et $\operatorname{Tr} x = \operatorname{Tr} y = 0$. En utilisant ces informations, et le fait que $\operatorname{Tr} z$ est elle aussi nulle, on trouve que $x_{12}^2 + y_{12}^2 + z_{12}^2 = -x_{12}y_{12} \operatorname{Tr} z = 0$, et donc, x, y et z étant à coefficients réels, $x_{12} = 0$. Par conséquent $\det x = -x_{11}^2$ fournit une contradiction.

2.2 Démonstration du théorème

2.2.1 Lemme de Blichfeldt

Commençons par énoncer un lemme arithmétique qui nous donne un contrôle de l'ordre d'un groupe de matrices en fonction des traces de ses éléments.

Proposition 6 (lemme de Blichfeldt)**.** *Soient G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$ et $\Xi = \{\operatorname{Tr} g \mid g \in G,\ g \neq 1\}$. Alors $N = \prod_{x\in\Xi}(n - x)$ est un entier non nul divisible par $|G|$.*

Démonstration. Notons P le polynôme à coefficients complexes $\prod_{x\in\Xi}(X - x)$. Montrons que P est en fait à coefficients entiers.

Posons $m = |G|$, prenons z une racine primitive m-ième de l'unité et notons $K = \mathbb{Q}(z)$. En diagonalisant dans $\mathbb{C}$ les éléments de G, on voit que leurs traces sont des sommes de puissances de z, et donc sont des entiers algébriques. Comme les coefficients de P sont des polynômes en les éléments de Ξ, ce sont aussi des entiers algébriques.

Chaque élément σ de $\mathrm{Gal}(K/\mathbb{Q})$ envoie z sur z^a pour un certain entier a inversible modulo m. Par conséquent, pour $g \in G$, $\sigma(\mathrm{Tr}\, g) = \mathrm{Tr}(g^a)$. On en déduit que σ est une permutation de Ξ, car, l'entier a étant premier à m, l'élévation à la puissance a est une permutation de $G \setminus \{1\}$. Comme les coefficients de P sont des polynômes symétriques en les éléments de Ξ, ils sont fixés par $\mathrm{Gal}(K/\mathbb{Q})$, et donc rationnels. Ce sont dès lors des entiers algébriques rationnels, donc entiers.

En particulier, $N = P(n)$ est donc entier. De plus, si $g \in G \setminus \{1\}$, $\mathrm{Tr}\, g$ est somme de n complexes de module 1, et $\mathrm{Tr}\, g$ ne peut valoir n que si tous ces complexes valent 1, ce qui est exclu. Donc $N \neq 0$.

Rappelons que, si (ρ, V) est une représentation de G, l'application linéaire $\frac{1}{|G|}\sum_{g\in G} \rho(g)$ est un projecteur sur V^G, donc en particulier sa trace est entière. Par conséquent, si χ est un caractère (ou une combinaison linéaire à coefficients entiers de caractères), $\sum_{g\in G} \chi(g)$ est un entier divisible par m. En posant $\chi(g) = P(\mathrm{Tr}\, g)$, on voit que χ est une combinaison linéaire à coefficients entiers de caractères de la forme $g \mapsto \mathrm{Tr}(g)^k$. Comme χ vaut N sur l'identité et zéro ailleurs, $\sum_{g\in G} \chi(g) = N$, et N est bien divisible par m. □

2.2.2 Localisation des traces

À présent, il nous faut des informations sur les $\mathrm{Tr}\, g$. Elles nous sont fournies par le fait suivant :

Lemme 6. *Soit G un ℓ-sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$ dont la trace de chaque élément est rationnelle. Alors, si $g \in G$, on peut écrire $\mathrm{Tr}(g) = n - \ell y$ pour un certain entier y vérifiant $0 \leqslant y \leqslant \frac{n}{\ell-1}$.*

Démonstration. L'élément g étant d'ordre fini, toutes ses valeurs propres sont des racines de l'unité. De plus, les coefficients du polynôme caractéristique χ_g de g sont des fonctions symétriques élémentaires de ces valeurs propres, donc peuvent être écrits comme des polynômes rationnels en les $\mathrm{Tr}(g^k)$, qui sont rationnelles : χ_g est donc dans $\mathbb{Q}[X]$.

Il est en outre divisible par le polynôme minimal sur $\mathbb{Q}$ de chacune de ses racines, et peut donc s'écrire comme produit de polynômes cyclotomiques. On regroupe alors les valeurs propres en fonction du polynôme cyclotomique où elles apparaissent, et on étudie séparément les blocs, ce qui conduira au résultat, la formule annoncée étant additive vis-à-vis de n.

On a donc des blocs de taille $\varphi(\ell^\alpha)$ contenant les racines primitives ℓ^α-ièmes de l'unité. En prenant z une telle racine, la trace du bloc correspondant vaut $\sum_{a\in(\mathbb{Z}/\ell^\alpha\mathbb{Z})^\times} z^a$. En distinguant les cas, on trouve que :

- si $\alpha = 0$, la trace vaut 1, la dimension 1, et on peut prendre $y = 0$;
- si $\alpha = 1$, la trace vaut -1, la dimension $\ell - 1$, et on peut prendre $y = 1$;
- si $\alpha \geqslant 2$, la trace vaut $\sum_{a\in\mathbb{Z}/\ell^\alpha\mathbb{Z}} z^a - \sum_{a\in\mathbb{Z}/\ell^{\alpha-1}\mathbb{Z}} z^{\ell a} = 0$, la dimension $\ell^{\alpha-1}(\ell-1)$, et on peut prendre $y = \ell^{\alpha-2}(\ell-1) \leqslant \ell^{\alpha-1}$. □

2.2.3 Preuve du théorème de Schur

Munis de ces deux résultats préliminaires, nous sommes maintenant en mesure de démontrer rapidement le théorème 5. Soit G un groupe vérifiant les hypothèses mentionnées. Grâce aux théorèmes de Sylow, on peut sans restriction demander que l'ordre de G soit une puissance de ℓ.

Par la proposition 6 et le lemme 6, l'ordre de G divise N, dont chaque facteur est de la forme ℓy avec $1 \leqslant y \leqslant d = [\frac{n}{\ell-1}]$, et les y sont distincts puisque les facteurs le sont. Donc l'ordre de G divise $\ell^d d!$; puisque $v_\ell(\ell^d d!)$ est exactement $M(n,\ell)$, on trouve le résultat escompté. □

2.2.4 Conjugaison de sous-groupes

Que peut-on ajouter quant à l'existence et à la conjugaison d'éventuels ℓ-sous-groupes de matrices de trace rationnelle atteignant la borne $M(n,\ell)$?

La construction explicite effectuée dans la démonstration du théorème 1' reste valide, et on pourrait réutiliser la démonstration du 1" dans le cas $\ell > 2$, en admettant qu'alors un ℓ-sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$ dont les traces sont rationnelles est conjugué à un sous-groupe de $\mathrm{GL}_n(\mathbb{Q})$. Cependant, le cas $\ell = 2$ pose problème. Ainsi, le groupe $\mathbb{H}_8$ mentionné plus haut et le groupe diédral D_4 engendré par les matrices

$$g' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{et} \quad h' = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

atteignent tous deux la plus grande valuation 2-adique possible, sans pour autant être isomorphes.

3 Intermède : sous-groupes finis de $\mathrm{GL}_2(\mathbb{Q})$

Le théorème 1 nous fournit une majoration de l'ordre d'un sous-groupe fini quelconque de $\mathrm{GL}_2(\mathbb{Q})$: ce cardinal divise en effet $M(2) = 2^3 \cdot 3 = 24$. À titre d'exemple, nous allons déterminer explicitement la forme des sous-groupes finis de $\mathrm{GL}_2(\mathbb{Q})$, et on vérifiera sans peine que le plus petit multiple commun de leurs ordres est bien 24. Cet exemple est adapté de [New72].

Proposition 7. *À isomorphisme près, les sous-groupes finis de* $\mathrm{GL}_2(\mathbb{Q})$ *sont* C_1, C_2, C_3, C_4, C_6, D_3, D_4 *et* D_6, *où* C_n *est le groupe cyclique d'ordre* n *et* D_n *le groupe diédral d'ordre* $2n$.

Démonstration. Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbb{Q})$; commençons par regarder $G^+ = G \cap \mathrm{SL}_2(\mathbb{Q})$. Par un argument similaire à ceux utilisés dans la preuve du lemme 2, G^+ peut être vu comme un sous-groupe de $\mathrm{SO}(2)$, et donc, étant fini, comme un sous-groupe discret de $\mathbb{R}/\mathbb{Z}$. Par conséquent, G^+ est cyclique.

Soit par ailleurs x d'ordre fini n dans $\mathrm{SL}_2(\mathbb{Q})$. La matrice x est diagonalisable dans $\mathbb{C}$, et ses valeurs propres λ et $\bar{\lambda}$ sont des racines primitives n-ièmes de l'unité. Leur polynôme minimal est donc de degré $\varphi(n)$. Comme λ et $\bar{\lambda}$ sont les racines du polynôme caractéristique de x, c'est donc que $\varphi(n) \leqslant 2$, ce qui conduit — puisque $\varphi(n) = \prod_{p|n} p^{v_p(n)-1}(p-1)$ — à $n \in \{1,2,3,4,6\}$.

Passons maintenant à G. Si $G = G^+$, c'est terminé ; sinon, soit $x \in G \setminus G^+$. Tous les éléments de xG^+ sont de déterminant -1. Comme une matrice de taille 2 et de déterminant -1 a des valeurs propres réelles, elle ne peut être que d'ordre 2. Par conséquent, chaque élément de xG^+ est d'ordre 2. Si l'on prend y un générateur du groupe cyclique G^+, on a $x^2 = 1 = (xy)^2$, et donc G est un groupe diédral. Les groupes D_4 et D_6 pouvant être vus (géométriquement ou en utilisant la matrice-compagnon du sixième polynôme cyclotomique Φ_6) comme des sous-groupes de $\mathrm{GL}_2(\mathbb{Q})$, on obtient bien les groupes annoncés, qui sont des sous-groupes de ces derniers. □

4 Vers les corps de nombres

Dans toute cette partie, K désigne un corps de nombres, c'est-à-dire une extension finie de $\mathbb{Q}$.

Le but est d'étendre le théorème 5 à des groupes de matrices dont les traces sont dans K et non plus dans $\mathbb{Q}$. Après avoir défini la borne recherchée et mis en place quelques résultats auxiliaires, on prouve le théorème dans le cas des nombres premiers ℓ impairs.

4.1 Théorème de Schur

4.1.1 Borne de Schur

Nous allons définir des bornes analogues aux $M(n)$ du théorème 1. On note, pour tout entier a, ζ_a une racine primitive a-ième de l'unité. Le symbole μ_{ℓ^∞} désignera l'ensemble de toutes les racines ℓ^k-ièmes de l'unité.

Fixons ℓ un nombre premier et K un corps de nombres. Les $K \cap \mathbb{Q}(\zeta_{\ell^k})$, pour $k \geqslant 1$, donnent une suite croissante de sous-extensions de K ; comme K est de dimension finie sur $\mathbb{Q}$, cette suite stationne. On pose alors

$$\begin{aligned} & m(K,\ell) &=& \min\{k \geqslant 1 \mid K \cap \mathbb{Q}(\zeta_{\ell^k}) = K \cap \mathbb{Q}(\zeta_{\ell^{k+1}})\} \\ \text{et} \quad & t(K,\ell) &=& [\mathbb{Q}(\zeta_{\ell^{m(K,\ell)}}) : K \cap \mathbb{Q}(\zeta_{\ell^{m(K,\ell)}})]. \end{aligned}$$

On notera éventuellement m et t quand il n'y aura aucune ambiguïté sur le corps et le nombre premier considérés.

On définit ensuite, pour tout entier n et tout nombre premier ℓ impair

$$\begin{aligned} S_K(n,\ell) &= m(K,\ell)\left[\frac{n}{t(K,\ell)}\right] + \sum_{k=1}^{\infty}\left[\frac{n}{\ell^k t(K,\ell)}\right] \\ \text{et} \quad S_K(n,2) &= n + (m(K,2)-1)\left[\frac{n}{t(K,2)}\right] + \sum_{k=1}^{\infty}\left[\frac{n}{2^k t(K,2)}\right]. \end{aligned}$$

Finalement, on pose

$$S_K(n) = \prod_{\ell} \ell^{S_K(n,\ell)}$$

où le produit est fait sur tous les nombres premiers. Les $S_K(n)$ vont jouer un rôle analogue à celui des $M(n)$ définis en 1.2.

Remarques. Comme $t(K,\ell)[K:\mathbb{Q}] \geqslant \ell - 1$ par le théorème de la base télescopique, il n'y a à n fixé qu'un nombre fini de nombres premiers ℓ tels que $S_K(n,\ell)$ ne soit pas nul, ce qui assure que $S_K(n)$ est bien défini.

De plus, par définition, $K \cap \mathbb{Q}(\zeta_{\ell^m}) = K \cap \mathbb{Q}(\mu_{\ell^\infty})$.

Enfin, pour $K = \mathbb{Q}$, on a $m_\ell = 1$ et $t_\ell = \varphi(\ell) = \ell - 1$; donc

$$S_{\mathbb{Q}}(n,\ell) = \sum_{i=0}^{\infty}\left[\frac{n}{\ell^i(\ell-1)}\right] = M(n,\ell)$$

et les bornes coïncident dans le cas rationnel.

Pour ℓ impair, les nombres t et m peuvent être décrits différemment, comme le montre la proposition que voici.

Proposition 8. *Pour ℓ impair, on a les égalités*

$$\begin{aligned} & m &=& 1 + v_\ell[K \cap \mathbb{Q}(\mu_{\ell^\infty}) : \mathbb{Q}] \\ \textit{et} \qquad & t &=& \frac{\ell - 1}{(\ell-1) \wedge [K \cap \mathbb{Q}(\mu_{\ell^\infty}) : \mathbb{Q}]}. \end{aligned}$$

Démonstration. Le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^k})/\mathbb{Q})$ est isomorphe à $\left(\mathbb{Z}/\ell^k\mathbb{Z}\right)^\times$. Soit σ l'élément de ce groupe qui envoie ζ_{ℓ^k} sur $\zeta_{\ell^k}^{\ell+1}$, qui correspond dans $(\mathbb{Z}/\ell^k\mathbb{Z})^\times$ à $\ell+1$, et qui est d'ordre ℓ^{k-1}. On vérifie que $\mathbb{Q}(\zeta_\ell)$ est égal au sous-corps de $\mathbb{Q}(\zeta_{\ell^k})$ fixé par σ. En effet, ζ_ℓ est fixé par σ, donc $\mathbb{Q}(\zeta_\ell)$ est inclus dans $\mathbb{Q}(\zeta_{\ell^k})^\sigma$; puis on compare les degrés $[\mathbb{Q}(\zeta_{\ell^k}) : \mathbb{Q}(\zeta_{\ell^k})^\sigma] = |\langle\sigma\rangle|$ et $[\mathbb{Q}(\zeta_{\ell^k}) : \mathbb{Q}(\zeta_\ell)] = [\mathbb{Q}(\zeta_{\ell^k}) : \mathbb{Q}]/[\mathbb{Q}(\zeta_\ell) : \mathbb{Q}]$.

Comme $\mathbb{Q}(\zeta_{\ell^k})/\mathbb{Q}$ est une extension abélienne — c'est-à-dire de groupe de Galois abélien —, toutes ses sous-extensions sont normales, donc stables par σ. Il est alors clair que $K \cap \mathbb{Q}(\zeta_\ell) = (K \cap \mathbb{Q}(\zeta_{\ell^k}))^\sigma$. Donc $[K \cap \mathbb{Q}(\zeta_{\ell^k}) : K \cap \mathbb{Q}(\zeta_\ell)]$ est l'ordre de la restriction de σ à $K \cap \mathbb{Q}(\zeta_{\ell^k})$, qui divise l'ordre ℓ^{k-1} de σ.

On a donc une suite $([K \cap \mathbb{Q}(\zeta_{\ell^k}) : K \cap \mathbb{Q}(\zeta_\ell)])_{k \geqslant 1}$ de puissances de ℓ qui croît strictement jusqu'à stationner à partir du rang m. Notons i_k la valuation ℓ-adique du k-ième terme de cette suite. La suite $(i_k)_{k\geqslant 1}$ est donc strictement croissante jusqu'au rang m, et on a vu que $i_k \leqslant k-1$ pour tout k. Par une récurrence facile, c'est donc que $i_k = k-1$ pour $k \in [\![1, m]\!]$. Par conséquent $\ell^{m-1} = [K \cap \mathbb{Q}(\mu_{\ell^\infty}) : K \cap \mathbb{Q}(\zeta_\ell)]$. Comme $[K \cap \mathbb{Q}(\zeta_\ell) : \mathbb{Q}]$ divise $\ell - 1$ qui est premier à ℓ, on a bien $m = 1 + v_\ell[K \cap \mathbb{Q}(\mu_{\ell^\infty}) : \mathbb{Q}]$.

Enfin, on vérifie les égalités suivantes :

$$\begin{aligned} t &= [\mathbb{Q}(\zeta_{\ell^m}) : K \cap \mathbb{Q}(\mu_{\ell^\infty})] \\ &= \frac{[\mathbb{Q}(\zeta_{\ell^m}) : \mathbb{Q}]}{[K \cap \mathbb{Q}(\mu_{\ell^\infty}) : \mathbb{Q}]} \\ &= \frac{\ell^{m-1}(\ell-1)}{\ell^{m-1}[K \cap \mathbb{Q}(\zeta_\ell) : \mathbb{Q}]} \\ &= \frac{\ell - 1}{(\ell-1) \wedge [K \cap \mathbb{Q}(\mu_{\ell^\infty}) : \mathbb{Q}]}, \end{aligned}$$

où la dernière égalité est justifiée car $[K \cap \mathbb{Q}(\mu_{\ell^\infty}) : \mathbb{Q}] = \ell^{m-1}[K \cap \mathbb{Q}(\zeta_\ell) : \mathbb{Q}]$ et que $[K \cap \mathbb{Q}(\zeta_\ell) : \mathbb{Q}]$ divise $\ell - 1 = [\mathbb{Q}(\zeta_\ell) : \mathbb{Q}]$. □

4.1.2 Énoncé du théorème

Avec les outils définis au paragraphe précédent, on peut à présent énoncer une dernière généralisation du théorème 1 :

Théorème 9. *Si G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$ dont la trace de chaque élément appartient à K, alors $|G|$ divise $S_K(n)$.*

4.1.3 Remarque sur une borne naïve

Le théorème 1 permet déjà de montrer que les sous-groupes finis de $\mathrm{GL}_n(K)$ ont un ordre majoré par un nombre ne dépendant que de n et de K. La borne multiplicative obtenue est explicite, mais loin d'être optimale.

Proposition 10. *Soit G un sous-groupe fini de $\mathrm{GL}_n(K)$. Alors l'ordre de G divise $M(n[K:\mathbb{Q}])$.*

Démonstration. Soit $d = [K : \mathbb{Q}]$. Choisissons une $\mathbb{Q}$-base de K^n. On injecte alors $\mathcal{M}_n(K)$ dans $\mathcal{M}_{nd}(\mathbb{Q})$ par la flèche d'oubli

$$\mathrm{End}_K(K^n) \longrightarrow \mathrm{End}_{\mathbb{Q}}(K^n)$$

qui est un morphisme d'anneaux, et qui induit par conséquent une injection $\mathrm{GL}_n(K) \longrightarrow \mathrm{GL}_{nd}(\mathbb{Q})$. Par le théorème 1, $|G|$ divise alors $M(nd)$. □

Remarque. Les bornes $S_K(n)$ que l'on vient de définir sont dans de nombreux cas strictement meilleures que la borne $M(nd)$ obtenue à la proposition précédente. Pour le voir, considérons un corps de nombres qui soit une extension cyclotomique, c'est-à-dire $K = \mathbb{Q}(\zeta_{\ell^s})$ pour un certain nombre premier ℓ et un certain entier s, et regardons les valuations ℓ-adiques des deux bornes. On trouve facilement que $d = \varphi(\ell^s) = \ell^{s-1}(\ell-1)$, $m = s$ et $t = 1$. Alors

$$\begin{aligned} & & S_K(n,\ell) &= sn + v_\ell(n!) \\ \text{et} & & M(nd,\ell) &= n\ell^{s-1} + v_\ell((n\ell^{s-1})!). \end{aligned}$$

En choisissant ℓ et s suffisamment grands pour que $s < \ell^{s-1}$, on voit alors immédiatement que $S_K(n,\ell) < M(nd,\ell)$.

4.1.4 Schéma de la démonstration

Dans le cas des corps de nombres, on voudrait adapter l'idée de Minkowski, qui consiste à se ramener à un groupe de matrices sur un corps fini, dont on peut calculer le cardinal par le lemme 4. Pour ce faire, on a besoin de la notion de localisation d'un anneau. Ceci fait l'objet du paragraphe 4.3.

Enfin, on établit le résultat au paragraphe 4.5 dans le cas de la valuation pour un nombre premier impair ℓ, le cas $\ell = 2$ étant admis.

4.2 Préliminaires algébriques

Nous allons prochainement avoir besoin de deux lemmes de conjugaison. La démonstration du premier est inspirée du chapitre 9 de [Isa76].

Lemme 7. *Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$. Alors il existe un corps de nombres K tel que G soit conjugué à un sous-groupe de $\mathrm{GL}_n(K)$.*

Démonstration. Nous allons utiliser de la théorie des représentations. Soient K un corps et L/K une extension. Pour toute K-représentation $\rho : G \to \mathrm{GL}_d(K)$ de G, on note ρ^L la L-représentation obtenue en étendant les scalaires à L, c'est-à-dire en prolongeant ρ par l'injection naturelle $\mathrm{GL}_d(K) \to \mathrm{GL}_d(L)$.

Soit $\rho : G \to \mathrm{GL}_d(\overline{\mathbb{Q}})$ une $\overline{\mathbb{Q}}$-représentation irréductible de degré d de G. Montrons que $\rho^{\mathbb{C}}$ est irréductible. Par le théorème de Burnside, comme $\overline{\mathbb{Q}}$ est algébriquement clos et ρ irréductible, $\mathrm{Vect}_{\overline{\mathbb{Q}}}(\mathrm{Im}\,\rho) = \mathcal{M}_n(\overline{\mathbb{Q}})$. On voit alors que $\mathrm{Vect}_{\mathbb{C}}(\mathrm{Im}\,\rho^{\mathbb{C}}) = \mathcal{M}_n(\mathbb{C})$, et donc que $\rho^{\mathbb{C}}$ est irréductible.

Montrons que toute $\mathbb{C}$-représentation irréductible σ est isomorphe à une $\overline{\mathbb{Q}}$-représentation irréductible. Notons $\mathrm{R}(K)$ la représentation régulière de G sur un corps K quelconque. Toutes les représentations complexes irréductibles de G

sont isomorphes à des sous-représentations de $\mathrm{R}(\mathbb{C})$, donc de $\mathrm{R}(\overline{\mathbb{Q}})^{\mathbb{C}}$, ces deux représentations étant identiques.

Décomposons $\mathrm{R}(\overline{\mathbb{Q}})$ en somme de sous-$\overline{\mathbb{Q}}$-représentations irréductibles sous la forme $\mathrm{R}(\overline{\mathbb{Q}}) = \bigoplus_i \rho_i$. On vérifie que $\mathrm{R}(\overline{\mathbb{Q}})^{\mathbb{C}} = \bigoplus_i \rho_i^{\mathbb{C}}$. Par ce qui précède, les $\rho_i^{\mathbb{C}}$ sont irréductibles, et on a décomposé $\mathrm{R}(\overline{\mathbb{Q}})^{\mathbb{C}}$ en somme de facteurs irréductibles. Comme σ est un facteur irréductible de $\mathrm{R}(\overline{\mathbb{Q}})^{\mathbb{C}}$, ceci montre que $\sigma \simeq \rho^{\mathbb{C}}$ où ρ est une $\overline{\mathbb{Q}}$-représentation irréductible de G.

On considère à présent γ la représentation de G donnée par l'inclusion $G \subset \mathrm{GL}_n(\mathbb{C})$. Par ce qui précède, comme γ est somme de sous-représentations irréductibles, elle est isomorphe à une $\overline{\mathbb{Q}}$-représentation γ'. Autrement dit, G est conjugué à un sous-groupe G' de $\mathrm{GL}_n(\overline{\mathbb{Q}})$. Soit maintenant l'extension K de $\mathbb{Q}$ engendrée par les coefficients des matrices de G'. Cette extension est finie car les coefficients en question sont des éléments de $\overline{\mathbb{Q}}$, donc algébriques. Il est alors clair que $G' \subset \mathrm{GL}_n(K)$, et le tour est joué. □

Lemme 8. *Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{F}_q)$, avec $q = p^r$ pour un certain nombre premier $p > n$. Supposons que l'ordre de G est premier à p. Si de plus toutes les traces des éléments de G sont dans K pour un certain sous-corps K de $\mathbb{F}_q$, alors G est conjugué à un sous-groupe de $\mathrm{GL}_n(K)$.*

Une démonstration de ce lemme peut être trouvée dans [GLo6], et s'appuie sur un résultat de cohomologie galoisienne énoncé dans [Ser68], proposition X.3. Une autre démonstration, plus longue, est fondée sur la théorie des représentations des algèbres de groupes et fait intervenir le théorème de commutativité de Wedderburn ; voir [Isa76], corollaire 9.23.

Nous admettrons le lemme 8.

4.3 Réduction modulo $\mathfrak{p}$

4.3.1 Définition de l'application de réduction

Définition (localisation)**.** Soient A un anneau commutatif intègre et S une partie non vide de A, stable par le produit et ne contenant pas zéro. On définit la *localisation* A_S de A en S comme le quotient $(A \times S)/\sim$, avec

$$(a, s) \sim (b, t) \overset{\text{déf}}{\iff} at = bs.$$

On obtient alors un anneau A_S, et la classe de (a, s) sera généralement notée $\frac{a}{s}$.

Par exemple, si $\mathfrak{p}$ est un idéal premier de A, on peut prendre $S = A \setminus \mathfrak{p}$. L'anneau A_S est alors plus couramment noté $A_{\mathfrak{p}}$.

On rappelle qu'un anneau est dit *local* s'il n'a qu'un seul idéal maximal.

Proposition 11. *Soit $\mathfrak{p}$ un idéal premier d'un anneau A intègre et unitaire. Alors $A_{\mathfrak{p}}$ est un anneau unitaire local, d'idéal maximal $\mathfrak{p}A_{\mathfrak{p}}$, et $A_{\mathfrak{p}}^{\times} = A_{\mathfrak{p}} \setminus \mathfrak{p}A_{\mathfrak{p}}$.*

Démonstration. Par définition, $A_{\mathfrak{p}}^{\times} = A_{\mathfrak{p}} \setminus \mathfrak{p}A_{\mathfrak{p}}$: si $a \notin \mathfrak{p}$, alors $\frac{1}{a} \in A_{\mathfrak{p}}$, et réciproquement. Par conséquent, $\mathfrak{p}A_{\mathfrak{p}}$ est maximal, puisque si $x \notin \mathfrak{p}A_{\mathfrak{p}}$, x est inversible et $\mathfrak{p}A_{\mathfrak{p}} + (x) = A_{\mathfrak{p}}$. D'autre part, si $\mathfrak{m}$ est un idéal maximal de $A_{\mathfrak{p}}$, on a $\mathfrak{m} \subset A_{\mathfrak{p}} \setminus A_{\mathfrak{p}}^{\times} = \mathfrak{p}A_{\mathfrak{p}}$, et par maximalité, $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$.

De plus, $A_{\mathfrak{p}}$ est unitaire de neutre multiplicatif $\frac{1}{1}$, puisque $1_A \in A \setminus \mathfrak{p}$. □

On considère à présent le cas des corps de nombres, et surtout des anneaux d'entiers qui leur sont associés. L'intérêt essentiel de la localisation est alors de se ramener à des anneaux principaux, et à obtenir des résultats similaires au lemme 1.

Proposition 12. *Soient $K/\mathbb{Q}$ un corps de nombres, et $\mathcal{O} = \mathcal{O}_K$ son anneau d'entiers. Soit encore $\mathfrak{p}$ un idéal premier de $\mathcal{O}$. Alors le localisé $\mathcal{O}_\mathfrak{p}$ est un anneau principal intègre.*

Démonstration. Il est immédiat que $\mathcal{O}_\mathfrak{p}$ est intègre. D'autre part, la théorie des anneaux d'entiers montre [Hino8] que tout idéal premier de $\mathcal{O}$ est maximal. Soit maintenant $\mathfrak{a}$ un idéal de $\mathcal{O}_\mathfrak{p}$. Montrons qu'il existe alors un entier α tel que $\mathfrak{a} = \mathfrak{p}^\alpha \mathcal{O}_\mathfrak{p}$. En effet, $\mathfrak{a} = (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_\mathfrak{p}$; comme $\mathfrak{a} \cap \mathcal{O}$ est un idéal de $\mathcal{O}$, il s'écrit $\prod_\mathfrak{q} \mathfrak{q}^\beta$ où les $\mathfrak{q}$ sont des idéaux premiers de $\mathcal{O}$. En multipliant par $\mathcal{O}_\mathfrak{p}$, on élimine alors tous les $\mathfrak{q} \neq \mathfrak{p}$, car ils sont inclus dans $\mathcal{O}_\mathfrak{p}^\times$.

Il suffit donc de montrer que l'idéal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ est principal : toutes ses puissances le seront. Prenons $x \in \mathfrak{p}\mathcal{O}_\mathfrak{p} \setminus \mathfrak{p}^2\mathcal{O}_\mathfrak{p}$, qui existe bel et bien, sans quoi on aurait $\mathfrak{p} = \mathfrak{p}^2$ en prenant les intersections avec $\mathcal{O}$. On peut alors écrire $(x) = \mathfrak{p}^\alpha \mathcal{O}_\mathfrak{p}$, et $\alpha \geqslant 2$ conduirait à l'absurdité $x \in \mathfrak{p}^\alpha \mathcal{O}_\mathfrak{p} \subset \mathfrak{p}^2 \mathcal{O}_\mathfrak{p}$. Par conséquent, $\mathfrak{p}\mathcal{O}_\mathfrak{p} = (x)$, ce que l'on voulait. □

Rappelons que la *norme* $\mathrm{N}(\mathfrak{a})$ d'un idéal $\mathfrak{a}$ de $\mathcal{O}$ est le cardinal du quotient $\mathcal{O}/\mathfrak{a}$.

Proposition 13. *On a des isomorphismes d'anneaux*

$$\frac{\mathcal{O}_\mathfrak{p}}{\mathfrak{p}\mathcal{O}_\mathfrak{p}} \simeq \frac{\mathcal{O}}{\mathfrak{p}} \simeq \mathbb{F}_{\mathrm{N}(\mathfrak{p})}.$$

Démonstration. En effet, on a une inclusion $\iota : \mathcal{O} \to \mathcal{O}_\mathfrak{p}$ et une projection $\pi : \mathcal{O}_\mathfrak{p} \to \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$. Le noyau de $\pi \circ \iota$ est alors $\iota^{-1}(\operatorname{Ker}\pi)$, soit exactement $\mathfrak{p}\mathcal{O}_\mathfrak{p} \cap \mathcal{O} = \mathfrak{p}$. Le dernier isomorphisme vient de ce que $\mathfrak{p}$ est premier, donc maximal. □

Lemme 9. *Soit G un sous-groupe fini de $\mathrm{GL}_n(K)$. Alors, pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}$, le groupe G est conjugué à un sous-groupe de $\mathrm{GL}_n(\mathcal{O}_\mathfrak{p})$.*

Démonstration. On peut réécrire exactement la même preuve que pour le lemme 1, en utilisant la remarque page 4 et en remplaçant $\mathbb{Q}$ par K et $\mathbb{Z}$ par $\mathcal{O}_\mathfrak{p}$, dont on a vu à la proposition 12 qu'il est principal. □

Remarque. On peut faire une remarque similaire à celle de la page 5 : en prenant un dénominateur commun d aux coefficients des éléments de G, on voit que G est d'emblée contenu (à identification près) dans $\mathrm{GL}_n(\mathcal{O}_\mathfrak{p})$ pour tout idéal premier $\mathfrak{p}$ ne contenant pas d.

4.3.2 Lemme de torsion

Voici une variante du lemme 3, qui nous sera utile dans le cas local :

Lemme 10. *Soient A un anneau local, $\mathfrak{m}$ son idéal maximal et $k = A/\mathfrak{m}$ son corps résiduel. Alors, si ℓ est un nombre premier différent de $\operatorname{car} k$, le noyau du morphisme de réduction $\mathrm{GL}_n(A) \longrightarrow \mathrm{GL}_n(k)$ ne contient aucune matrice d'ordre ℓ.*

Démonstration. Supposons que $x \in \mathrm{GL}_n(A)$ vérifie $x^\ell = 1$ et $x \equiv 1 \pmod{\mathfrak{m}}$. On peut écrire $x = 1 + y$, avec $y \in \mathcal{M}_n(\mathfrak{m})$. Le fait que $x^\ell = 1$ se traduit par $\sum_{k=1}^{\ell} \binom{\ell}{k} y^k = 0$, soit $yu = 0$ avec

$$u = \sum_{k=1}^{\ell} \binom{\ell}{k} y^{k-1} = \ell\, 1 + \binom{\ell}{2} y + \cdots + y^{\ell-1}.$$

De plus, $u \equiv \ell\, 1 \pmod{\mathfrak{m}}$, et comme ℓ est inversible dans k, u est inversible dans $\mathcal{M}_n(k)$. Donc le déterminant de u n'est pas dans $\mathfrak{m}$, et il est par conséquent inversible dans A, car A est local. Mais $yu = 0$, donc $y = 0$ et $x = 1$. □

Corollaire 14. *Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}$. Écrivons $\mathrm{N}(\mathfrak{p}) = p^r$ pour un certain entier r et un certain nombre premier p. Alors les éléments d'ordre fini du noyau du morphisme de réduction*

$$\mathrm{GL}_n(\mathcal{O}_\mathfrak{p}) \longrightarrow \mathrm{GL}_n(\mathbb{F}_{\mathrm{N}(\mathfrak{p})})$$

sont d'ordre une puissance de p.

Démonstration. Ce morphisme est bien défini grâce à l'isomorphisme de la proposition 13, et le résultat est rendu évident par le lemme 10 et le fait que $\mathcal{O}_\mathfrak{p}$ est local d'idéal maximal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ (proposition 11). □

4.4 Inertie de certains nombres premiers

On a le théorème suivant, démontré dans [IR90] (théorème 2 page 196), et que nous admettrons :

Théorème 15. *Soient m un entier et p un nombre premier ne divisant pas m. Soit r l'ordre de p modulo m. Alors, dans l'anneau d'entiers $\mathcal{O}_{\mathbb{Q}(\zeta_m)} \subset \mathbb{Q}(\zeta_m)$, on a une décomposition en produit d'idéaux*

$$(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_g$$

où les $\mathfrak{p}_k$ sont des idéaux premiers distincts de $\mathcal{O}_{\mathbb{Q}(\zeta_m)}$, et $g = \frac{\varphi(m)}{r}$.

On déduit facilement de ce théorème le résultat que voici, qui nous sera utile dans la démonstration finale :

Corollaire 16. *Soient ℓ un nombre premier impair et p un générateur de $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$. Alors, pour tout entier $s \geqslant 2$, p reste premier dans $\mathcal{O}_{\mathbb{Q}(\zeta_{\ell^s})}$.*

Démonstration. On a vu dans la preuve du lemme 4 que, sous ces hypothèses, p engendre $(\mathbb{Z}/\ell^s\mathbb{Z})^\times$ pour tout s. On peut alors appliquer le théorème vu ci-dessus, avec $m = \ell^s$, $r = \varphi(\ell^s)$ et $g = 1$. □

4.5 Démonstration pour ℓ impair

Rappelons que l'on considère un groupe $G \leqslant \mathrm{GL}_n(\mathbb{C})$ tel que la trace de chaque élément soit dans un corps de nombres K. Nous allons suivre le même chemin que dans le cas rationnel du théorème de Minkowski : après avoir inclus le groupe G dans un groupe de matrices sur un corps de taille convenable, on calculera la valuation ℓ-adique de ce groupe de matrices, ce qui permettra de

conclure. Quitte à remplacer G par un de ses ℓ-Sylow, on peut supposer que l'ordre de G est une puissance de ℓ.

Par le lemme 7, on peut conjuguer G à un groupe de matrices dont tous les coefficients sont dans un corps de nombres L contenant K. Notons $\mathcal{O} = \mathcal{O}_L$. Prenons un nombre premier $p > n$ engendrant $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$, et un idéal premier $\mathfrak{p}$ de $\mathcal{O}$ contenant p ; on a alors $(p) = \mathfrak{p} \cap \mathbb{Z}$. Par le lemme 9, G peut être conjugué à un sous-groupe de $\mathrm{GL}_n(\mathcal{O}_\mathfrak{p})$. Par le corollaire 14, puisque $\ell \neq p$, le morphisme de réduction $\varphi : G \to \mathrm{GL}_n(\mathbb{F}_{\mathrm{N}(\mathfrak{p})})$ est une injection.

Par hypothèse, toutes les traces des éléments de G sont dans K, et elles sont aussi dans $\mathbb{Q}(\mu_{\ell^\infty})$ en diagonalisant chaque matrice. De plus, ce sont des entiers algébriques. On en déduit que les traces sont dans l'anneau des entiers $\mathcal{O}_{K'}$ du corps de nombres $K' = K \cap \mathbb{Q}(\mu_{\ell^\infty})$. Par l'application de réduction φ, elles sont par conséquent envoyées dans $\mathbb{F}_q = \frac{\mathcal{O}_{K'}}{\mathfrak{p} \cap \mathcal{O}_{K'}}$ pour $q = p^f = \mathrm{N}(\mathfrak{p} \cap \mathcal{O}_{K'})$, la norme étant celle de $\mathcal{O}_{K'}$ et l'idéal $\mathfrak{p}$ restant premier dans $\mathcal{O}_{K'}$. Grâce au lemme 8, on a donc à conjugaison et identification près que

$$G \leqslant \mathrm{GL}_n(\mathbb{F}_q).$$

Il s'agit à présent de contrôler $v_\ell(\mathrm{GL}_n(\mathbb{F}_q))$; par le lemme 4 et le choix de p, cette valuation est

$$v_\ell(\mathrm{GL}_n(\mathbb{F}_q)) = (1 + v_\ell(f)) \left[\frac{n}{\tau}\right] + \sum_{i=1}^{\infty} \left[\frac{n}{\ell^i \tau}\right]$$

où $\tau = \frac{\ell-1}{(\ell-1)\wedge f}$. Par le corollaire 16, pour tout entier $s \geqslant 1$, l'entier p est premier dans $\mathcal{O}_{\mathbb{Q}(\zeta_{\ell^s})}$, et par conséquent dans $\mathcal{O}_{K'} \subset \mathcal{O}_{\mathbb{Q}(\zeta_{\ell^m})}$. On en tire donc que $p\mathcal{O}_{K'}$ et $\mathfrak{p} \cap \mathcal{O}_{K'}$ sont deux idéaux premiers, donc maximaux, de $\mathcal{O}_{K'}$; l'un étant inclus dans l'autre, ils sont égaux. En prenant la norme dans $\mathcal{O}_{K'}$, on en déduit finalement que

$$p^f = \mathrm{N}(\mathfrak{p} \cap \mathcal{O}_{K'}) = \mathrm{N}(p\mathcal{O}_{K'}) = p^{[K':\mathbb{Q}]}$$

et donc

$$f = [K \cap \mathbb{Q}(\mu_{\ell^\infty}) : \mathbb{Q}].$$

En réécrivant, on obtient alors, en utilisant la proposition 8, que

$$\begin{aligned} m(K,\ell) &= 1 + v_\ell(f) \\ \text{et} \qquad t(K,\ell) &= \tau \end{aligned}$$

et par conséquent

$$v_\ell(\mathrm{GL}_n(\mathbb{F}_q)) = v_\ell(S_K(n))$$

ce qui achève la démonstration. □

Conclusion

Nous avons donc vu une majoration du plus petit multiple commun des ordres de tous les sous-groupes finis de $\mathrm{GL}_n(\mathbb{Q})$. On pourrait dans un autre ordre d'idées se demander quel est le *maximum* de ces ordres. En considérant le sous-groupe $\mathfrak{S}_n^{\pm}$ des permutations signées, on voit que ce maximum est supérieur à $2^n n!$.

En fait, on a presque toujours égalité, comme l'affirme le résultat suivant :

> *Pour $n \notin \{2, 4, 6, 7, 8, 9, 10\}$, un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Q})$ est d'ordre au plus $2^n n!$. De plus, à conjugaison près, $\mathfrak{S}_n^{\pm}$ est le seul groupe atteignant cette borne.*

Cet énoncé a été démontré en 1995 par Walter Feit dans un article encore inédit ; sa démonstration repose sur un article inachevé de Boris Weisfeiler, dépendant lui-même du théorème de classification des groupes finis simples. Shmuel Friedland a donné en 1997 une preuve plus simple pour n assez grand [Fri97], elle aussi déduite d'un résultat de Weisfeiler [Wei84] s'appuyant aussi sur le théorème de classification.

Références

[Fri97] Friedland, Shmuel: *The maximal orders of finite subgroups in* $\mathrm{GL}_n(\mathbb{Q})$. Proc. Amer. Math. Soc., 125(12) :3519–3526, 1997, ISSN 0002-9939.

[GL06] Guralnick, Robert M. et Martin Lorenz: *Orders of finite groups of matrices*. Dans *Groups, rings and algebras*, tome 420 de *Contemp. Math.*, pages 141–161. Amer. Math. Soc., Providence, RI, 2006.

[Gro02] Grove, Larry C.: *Classical groups and geometric algebra*, tome 39 de *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002, ISBN 0-8218-2019-2.

[Hin08] Hindry, Marc: *Arithmétique*. Calvage et Mounet, Paris, 2008.

[IR90] Ireland, Kenneth et Michael Rosen: *A classical introduction to modern number theory*, tome 84 de *Graduate Texts in Mathematics*, pages 173–197. Springer-Verlag, New York, deuxième édition, 1990.

[Isa76] Isaacs, I. Martin: *Character theory of finite groups*. Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976. Pure and Applied Mathematics, n° 69.

[Lan02] Lang, Serge: *Algebra*, tome 211 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, troisième édition, 2002.

[New72] Newman, Morris: *Integral matrices*. Academic Press, New York, 1972. Pure and Applied Mathematics, volume 45.

[Sch73] Schur, Issai: *Über eine Klasse von endlichen Gruppen linearer Substitutionen*, pages 128–142. Springer-Verlag, Berlin, 1973. Herausgegeben von Alfred Brauer und Hans Rohrbach.

[Ser68] Serre, Jean Pierre: *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, n° VIII.

[Ser07] Serre, Jean Pierre: *Bounds for the orders of the finite subgroups of* $G(k)$. Dans *Group representation theory*, pages 405–450. EPFL Press, Lausanne, 2007.

[Wei84] Weisfeiler, Boris: *Post-classification version of Jordan's theorem on finite linear groups*. Proc. Nat. Acad. Sci. U.S.A., 81(16, Phys. Sci.) :5278–5279, 1984, ISSN 0027-8424.