PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 125, Number 12, December 1997, Pages 3519–3526
S 0002-9939(97)04283-4

THE MAXIMAL ORDERS OF FINITE SUBGROUPS IN $GL_n(\mathbf{Q})$

SHMUEL FRIEDLAND

(Communicated by Ronald M. Solomon)

ABSTRACT. We give a relatively simple proof that the orthogonal group over the integers is the unique finite subgroup (up to a conjugation) in $GL_n(\mathbf{Z})$ of the maximal order for $n >> 1$.

§0. INTRODUCTION

In our recent paper [Fri] the following problem arose naturally. Let $\Gamma \le GL_n(\mathbf{Z})$ be a finite group. What is the exact upper bound for $|\Gamma|$? (It is well known that any finite group in $GL_n(\mathbf{Q})$ is conjugate to a finite group in $GL_n(\mathbf{Z})$, e.g. [Ser, p. 124].) In [Fri] we conjectured that $O_n(\mathbf{Z})$, the orthogonal group over the integers whose order is $2^n n!$, has the maximal order for all n. Very recently, Feit [Fei] gave the complete solution of the problem of characterizing the finite groups of the maximal order in $GL_n(\mathbf{Q})$ and their orders for all n. The orthogonal group is maximal exactly for $n = 1, 3, 5$ and $n > 10$. For $n = 2, 4, 6, 7, 8, 9, 10$, Feit characterizes the corresponding maximal groups. One of the main ingredients of Feit's proof for large values of n is the unpublished paper of Weisfeiler [Wei2] which gives almost sharp estimates of the Jordan number $j(n) \le (n+2)!$ for $n > 63$. (Jordan's theorem claims that any finite group $G \subset GL_n(\mathbf{C})$ contains a normal abelian subgroup whose index is at most $j(n)$. Note that $j(n) \ge (n+1)!$ and it is a common belief that $j(n) = (n+1)!$ for $n >> 1$.)

The purpose of this paper is to give a relatively simple proof of our conjecture that the orthogonal group is the unique (up to a conjugation) finite subgroup in $GL_n(\mathbf{Z})$ of the maximal order for $n >> 1$. Let $\Delta \le GL_n(\mathbf{Q})$ be a finite abelian group. We prove the sharp inequalities:

$$\begin{aligned} &|\Delta| \le 6^{\lfloor \frac{n}{2} \rfloor} 2^{n-2\lfloor \frac{n}{2} \rfloor}, \\ &|\Delta| \le 3^{\lfloor \frac{n}{2} \rfloor}, \quad \text{if} \quad 2 \not| \; |\Delta|, \\ &|\Delta| \le 2^n, \qquad \text{if} \quad 3 \not| \; |\Delta|. \end{aligned} \tag{0.1}$$

The proof of the above inequality uses the well known fact that if Δ acts irreducibly on $\mathbf{Q}^n$ then Δ imbeds in a cyclotomic extension field of $\mathbf{Q}$ of degree n at most, and $|\Delta|$ is bounded appropriately. Let $\Gamma \le GL_n(\mathbf{Z})$ be a finite group with a normal abelian subgroup $\Delta \le \Gamma$ of the maximal order. Then $|\Gamma| \le j(n)|\Delta|$. We deduce our main result by combining (0.1) with Weisfeiler's asymptotic bound [Wei1]

$$j(n) \le n^{a \log n + b} n!. \tag{0.2}$$

Received by the editors August 5, 1996.
1991 *Mathematics Subject Classification.* Primary 20C10, 20G30.

We remark that the problem of estimating the size of a finite group $\Gamma \le GL_n(\mathbf{Z})$ was considered by Minkowski [Min]. In fact, Minkowski [Min] found $\kappa(n)$—the least common multiple of all finite subgroups of $GL_n(\mathbf{Z})$. The right asymptotic order of $\kappa(n)$ was recently determined by Y. Katznelson [Kat]. See [R-T] for weaker bounds on $|\Gamma|$.

§1. Preliminary results

Let F be a field of characteristic 0. We view $\mathbf{Q}$ as a subfield of F. Denote by $M_n(F) := \mathrm{End}_F(F^n)$ the ring of $n\times n$ matrices with entries in F. Let $\Gamma \le GL_n(F)$. Assume that W is a Γ-invariant subspace of F^n. Let $\Gamma' \triangleleft \Gamma$ be the subgroup which acts trivially on W: $\Gamma' = \{\gamma \in \Gamma : \quad \gamma(x) = x, x \in W\}$. We denote by $\Gamma\big|W$ the subgroup of $GL(W)$ which is induced by the restriction of Γ to W ($\Gamma\big|W \cong \Gamma/\Gamma'$). Recall the standard results about *FG-representations*. Consult for example with [C-R, Ch.1]. Let $R(\Gamma) = \mathrm{span}(\Gamma) \subset M_n(F)$ be the ring spanned by Γ. Then Maschke's theorem claims that any (left) $R(\Gamma)$-module V is semisimple. Let V be a semisimple $R(\Gamma)$-module and W a simple $R(\Gamma)$-module. The homogeneous component of V determined by W is the submodule generated by $\{U : U \le V, U \cong W\}$. V is homogeneous if it is generated by isomorphic simple submodules. Let $\Delta \triangleleft \Gamma$ be a normal subgroup. Let V be a finite dimensional simple $R(\Gamma)$-module. Then V is a semisimple $R(\Delta)$-module. Clifford's Theorem claims that Γ acts transitively on $R(\Delta)$-homogeneous components of V. Let $\phi(d)$ be the *Euler ϕ-function*, i.e. the number of integers n with $1 \le n \le d$ which are prime to d.

Lemma 1. *Let F be a field of characteristic 0 and assume that $\Delta \le GL_n(F)$ is a finite abelian group. Let*

$$R(\Delta) = \sum_{i=1}^{s} R_i, \quad \textit{and} \quad F^n = \sum_{1}^{s} \oplus W_i, \quad W_i = R_i F^n, \quad i = 1, ..., s,$$

be a decomposition of $R(\Delta)$ to $R(\Delta)$-simple ideals and the induced decomposition of F^n into Δ-invariant subspaces. Let $\Delta_i = \Delta\big|W_i, i = 1, ..., s$, and denote by $\mathbf{K}_i$ the minimal extension of F which splits the characteristic polynomial of each element in Δ_i. Then Δ_i is cyclic of order m_i and $[\mathbf{K}_i : F] = \frac{\phi(m_i)}{\phi(p_i)}$, where p_i is the maximal order of $m_i - th$ root of unity contained in F. Furthermore, $\dim_F W_i = \frac{d_i \phi(m_i)}{\phi(p_i)}, i = 1, ..., s$. The ring $R(\Delta_i)$ generated by $\Delta_i \subset End_F(W_i)$ is simple and isomorphic to R_i. Finally, Δ is isomorphic to a subgroup of $\sum_1^s \oplus \Delta_i$.

Proof. Let $V \le F^n$ be a Δ-irreducible subspace, i.e. V is a simple $R(\Delta)$-module. Set $\Theta = \Delta\big|V$. Assume that $l = \dim V$. We view $\Theta \le GL_l(F)$. We claim that Θ is a cyclic group. Observe that the centralizer $C \subset M_l(F)$ of $R := R(\Theta)$ is exactly the ring of R endomorphisms of V. By Schur's lemma C is a division ring. In particular, R generates a commutative division ring D, i.e. D is a field. Hence, R is a simple ring. For each k the equation $x^k = e, x \in \Theta$, has at most k solutions. Therefore $\Theta \le D$ is cyclic of order m. Assume that Θ is generated by $\theta \in GL_l(F)$. As V is Θ-irreducible space it follows that the characteristic polynomial of θ is irreducible over F. Since the order of θ is m we deduce that $det(xI - \theta) | x^m - 1$. Let ζ be an $m - th$ primitive root of unity. Then degree of cyclotomic polynomial $\sigma_m(x)$ corresponding to all $m - th$ primitive roots of 1 is $\phi(m)$. Let $F \cap \mathbf{Q}[\zeta] = \mathbf{Q}[\xi]$ where ξ is a $p - th$ primitive root and $p \mid m$. Then $det(xI - \theta)$ is an irreducible polynomial of degree l over $\mathbf{Q}[\xi]$ so that the extension of $\mathbf{Q}[\xi]$ with respect to $det(xI-\theta)$ yields $\mathbf{Q}[\zeta]$. Hence $l=\frac{\phi(m)}{\phi(p)}$.

Consider the above decomposition of $R(\Delta)$ to simple ideals. The simplicity of each R_i implies that $R_jR_i=R_iR_j=0, j\neq i$. Hence this decomposition of $R(\Delta)$ induces the above decomposition of F^n. The natural projection $\pi:\Delta\to\sum_1^s\oplus\Delta_i$ is a faithful homomorphism. Hence, $\Delta\cong\pi(\Delta)$. Let $W_i=\sum_{j=1}^{d_i}\oplus V_{ij}$ be a decomposition to Δ_i-irreducible subspaces. Let $\Theta_{ij}=\Delta_i\big|V_{ij}$. The above arguments show that Θ_{ij} is cyclic and $R(\Theta_{ij})$ is simple. We claim that $\Delta_i\cong\Theta_{ij}$. Assume to the contrary that $\pi_{ij}:\Delta_i\to\Theta_{ij}$ has a nontrivial kernel $\Psi_{ij}\leq\Delta_i$. Consider the ideal $R_{ij}\subset R_i$ generated by all elements in R_i that act trivially on V_{ij}. Note that $\psi-e\in R_{ij}$ for any $\psi\in\Phi_{ij}$. Thus R_{ij} is a nontrivial $R(\Delta)$-submodule of R_j which contradicts the simplicity of R_j. Hence

$$[\mathbf{K_i}:F]=\frac{\phi(m_i)}{\phi(p_i)},\quad \dim_F W_i=\frac{d_i\phi(m_i)}{\phi(p_i)},\quad i=1,...,s.$$

Clearly $R(\Delta_i)\cong R_i$ and these rings are simple. □

Theorem 1. *Let F be a field of characteristic* 0 *and assume that $\Gamma\leq GL_n(F)$ is a finite group with a normal abelian subgroup $\Delta\triangleleft\Gamma$. Then there exists a decomposition $F^n=\sum_1^t\oplus W_i$ to Γ-invariant subspaces such that each W_i has a decomposition to Δ-invariant subspaces $W_{ij}=\sum_1^{k_i}\oplus W_{ij}, i=1,...,t,$ with the following properties: If we set*

$$G_i=\Gamma\big|W_i,\quad D_i=\Delta\big|W_i,\quad \tilde\Gamma_{ij}=\{\gamma:\ \gamma\in\Gamma,\gamma(W_{ij})=W_{ij}\},$$
$$\Gamma_{ij}=\tilde\Gamma_{ij}\big|W_{ij},\quad \Delta_{ij}=\Delta\big|W_{ij},\quad i=1,...,t,\quad j=1,...,k_i,$$

then each Δ_{ij} is a normal cyclic subgroup of Γ_{ij} of order m_i and $\dim_F W_{ij}=\frac{d_i\phi(m_i)}{\phi(p_i)}$, where p_i is the maximal order of m_i-th root of unity contained in F. Γ acts as a transitive subgroup of permutation $P_i\leq S_{k_i}\leq GL_{k_i}(\mathbf{Z})$ on $\{W_{i1},...,W_{ik_i}\}, i=1,...,t$. In particular, Γ is a subgroup of the direct product $G_1\times\cdots\times G_t$ and each G_i is isomorphic to a subgroup of $\Gamma_{i1}\wr P_i$.

Assume that $\Gamma\leq GL_n(F)$ is a finite strongly maximal subgroup, i.e. Γ is not isomorphic to any proper subgroup of a finite group $\Gamma'\leq GL_n(F)$. Let $\Delta\triangleleft\Gamma$ be a maximal normal abelian subgroup of the maximal order. Consider the above decomposition of F^n to Γ and Δ-invariant subspaces. Then

$$\Gamma=G_1\times\cdots\times G_t,\quad G_i\cong\Gamma_{i1}\wr S_{k_i},\quad i=1,...,t. \tag{1.1}$$

For $1\leq q<r\leq t$ $\Gamma_{q1}\not\cong\Gamma_{r1}$. Any normal abelian subgroup of $\Phi\triangleleft\Gamma_{i1}$ satisfies the inequality $|\Phi|\leq|\Delta_{i1}|$. If F is a subfield of the field of complex numbers $\mathbf{C}$ then $[\Gamma_{ij}:\Delta_{ij}]\leq j(\dim_F W_{ij})$.

Proof. Use Clifford's Theorem and Schur's Lemma (as in the proof of Lemma 1) to deduce the first part of the theorem which ends with the statement: Γ is a subgroup of the direct product $G_1\times\cdots\times G_t$ and each G_i is isomorphic to a subgroup of $\Gamma_{i1}\wr P_i$.

Assume now that $\Gamma\leq GL_n(F)$ is a strongly maximal finite group. Thus $\Gamma\leq G=G_1\times\cdots\times G_t\leq GL_n(F)$. The strong maximality of Γ implies that $\Gamma=G$. The maximality of Δ yields $\Delta=D_1\times\cdots\times D_t$. Recall that G_i is isomorphic to a subgroup of $\Gamma_{i1}\wr P_i$. Observe next $\Gamma_{i1}\wr S_{k_i}$ can be viewed as a finite group in $GL_{\dim_F W_i}(F)$ as follows: View the group $\tilde G_i=\Gamma_{i1}\times\cdots\times\Gamma_{i1}$ (k_i times) as a group of block diagonal $k_i\times k_i$ matrices. Set $G_i'=\tilde G_iS_{k_i}'$ where $S_{k_i}'\cong S_{k_i}$ is the group $k_i \times k_i$ block permutation matrix whose all square blocks are the identity matrices of dimension $\dim_F W_{i1}$. Then $\Gamma_{i1} \wr S_{k_i} \cong G_i' \le GL_{\dim_F W_i}(F)$. The strong maximality of Γ yields that $G_i \cong \Gamma_{i1} \wr S_{k_i}$.

Suppose that $\Gamma_{q1} \cong \Gamma_{r1}, 1 \le q < r \le t$. Then $G_q \times G_r$ is isomorphic to a proper subgroup $\Gamma_{q1} \wr S_{k_q+k_r}$. This contradicts the strong maximality of Γ.

We now show that $\Delta_{i1} \triangleleft \Gamma_{i1}$ has maximal order out of all normal abelian subgroups of Γ_{i1}. As W_{ij} is a Δ-invariant subspace for $j = 1, ..., k_i$ we deduce that $D_i \le \Delta_{i1} \times \cdots \times \Delta_{k_i}$. The maximal order of Δ yields that D_i is a normal abelian subgroup of G_i of the maximal order. Hence

$$D_i = \Delta_{i1} \times \cdots \times \Delta_{k_i}, \quad |D_i| = |\Delta_{i1}|^{k_i}.$$

Suppose that $\Delta_{i1}' \triangleleft \Gamma_{i1}$. Then G_i has a normal abelian subgroup isomorphic to $\Delta_{i1}' \times \cdots \times \Delta_{i1}'$ (k_i times). As Δ_i has a maximal order we deduce that $|\Delta_{i1}'| \le |\Delta_{i1}|$.

Suppose that F is a subfield of $\mathbf{C}$. Then Jordan's theorem yields that $[\Gamma_{ij} : \Delta_{ij}] \le j(\dim_F W_{ij})$. $\square$

In what follows we need the following lemmas.

Lemma 2. *Let $1 < l \in \mathbf{Z}$ and denote by $\zeta_{l,j}, j = 1, ..., \phi(l)$, all l-primitive roots of 1. Set $\psi(l) = \max_{1 \le j \le \phi(l)} |1 - \zeta_{l,j}|$. Then*

$$\psi(2k-1) = 2\cos\frac{\pi}{2(2k-1)},$$
$$\psi(2(2k-1)) = 2|\cos\frac{\pi}{(2k-1)}|,$$
$$\psi(2^m(2k-1)) = 2\cos\frac{\pi}{2^m(2k-1)}, \quad k \ge 1, \quad m > 1.$$

Proof. Clearly, $\psi(2) = 2$. Assume now that $l = 2k-1, k \ge 1$. Then $\zeta = e^{\frac{2\pi\sqrt{-1}k}{2k-1}}$ is a primitive l-root of unity. As $-1 = e^{\frac{2\pi\sqrt{-1}(k-\frac{1}{2})}{2k-1}}$ we easily deduce that ζ is the closest l-root of 1 to -1. Hence, $\psi(2k-1) = |1-\zeta| = 2\cos\frac{\pi}{2(2k-1)}$. Assume now that $l = 2(2k-1), k > 1$. As -1 is a nonprimitive l-root the above argument shows that $\zeta = e^{\frac{2\pi\sqrt{-1}(2k+1)}{2(2k-1)}}$ is the closest l-primitive root to -1 and the lemma follows for this case. Assume finally that $l = 2^m(2k-1), m > 1$. Then $e^{\frac{2\pi\sqrt{-1}(2^{m-1}(2k-1)+1)}{2^m(2k-1)}}$ is the closest l-primitive root to -1 and the lemma follows in this case too. $\square$

Lemma 3. *Let $m \ne 1, 2, 4, 6$. Then $m \le 3.5^{\frac{\phi(m)}{2}}$.*

Proof. Let

$$m = \prod_1^k p_i^{r_i}, \quad 2 \le p_1 < \cdots < p_k, \quad 1 \le r_i, \quad i = 1, ..., k,$$

be the prime decomposition of $m > 1$. Recall that $\phi(m) = \prod_1^k p_i^{r_i - 1}(p_i - 1)$. A simple induction on n proves that $n \ge 8 \Rightarrow n < 3^{\frac{n}{4}}$; $n \ge 3 \Rightarrow 3^{\frac{n-1}{2}}$. Then for every prime $p \ge 3$ and $r \ge 1$

$$p^r \le 3^{\frac{r(p-1)}{2}} \le 3^{\frac{p^{r-1}(p-1)}{2}}.$$

For $p = 2$ and $r \ge 3$

$$2^r < 3^{\frac{2^r}{4}} = 3^{\frac{\phi(2^r)}{2}}.$$

Thus $m \le 3^{\frac{\phi(m)}{2}}$ if either $p_1 \ge 3$ or $p_1 = 2$ and $k_1 \ge 3$. It is left to consider the cases $p_1 = 2$ and $k_1 = 1, 2$. A straightforward calculation shows that the lemma is valid for $m \le 30$. Suppose first that $p_1 = 2,\ k_1 = 1$, i.e. $m = 2(2q-1)$. For $2q - 1 > 15$ we have $\phi(2q-1) \ge 12$. Then

$$3.5^{\frac{\phi(m)}{2}} = 3.5^{\frac{\phi(2q-1)}{2}} = \left(\frac{3.5}{3}\right)^{\frac{\phi(2q-1)}{2}} 3^{\frac{\phi(2q-1)}{2}}$$
$$\ge \left(\frac{3.5}{3}\right)^{6} (2q-1) > m, \quad m = 2(2q-1) > 30.$$

Assume that $p_1 = 2,\ k_1 = 2$, i.e. $m = 4(2q-1)$. Then $\phi(m) = 2\phi(2q-1)$. For $2q - 1 > 7$

$$3^{\frac{\phi(m)}{2}} = 3^{\phi(2q-1)} \ge (2q-1)^2 > \frac{7}{4}m, \quad m = 4(2q-1) > 30,$$

and the lemma follows. □

For $A \in M_n(\mathbf{C}), x \in \mathbf{C}^n$, let A^*, x^* be the respective conjugate transposes. Assume that F is a subfield of $\mathbf{C}$ and suppose that $\Gamma \le GL_n(F)$ is a finite group. Set $S(\Gamma) = \sum_{\gamma \in \Gamma} \gamma^* \gamma$. Then $S(\Gamma) \in M_n(\mathbf{C})$ is a positive definite matrix. Define an inner product on $\mathbf{C}^n$:

$$(x, y) = y^* S(\Gamma) x, \quad x, y \in \mathbf{C}^n.$$

Then Γ is a finite group of unitary matrices with respect to $(\cdot,\cdot)$. If F is invariant under the conjugation, i.e. $\bar{F} = F$, then $S(\Gamma) \in GL_n(F)$ and $(\cdot,\cdot)$ is an inner product on F^n. Suppose furthermore that $\Gamma \le GL_n(\mathbf{R})$. In that case we view Γ as a subgroup of orthogonal matrices (with respect to $(\cdot,\cdot)$).

Assume in addition that Γ is abelian. Then $\mathbf{C}^n$ has an orthonormal basis consisting of the common eigenvectors of the elements of Γ. Since the complex eigenvectors come in conjugate pairs we deduce that $\mathbf{R}^n$ has a Γ-invariant orthogonal decomposition $V_1 \oplus \cdots \oplus V_m$, where each V_i is of dimension one or two. Assume that V_i is two dimensional. Then $\gamma^{(i)} = \gamma \big| V_i, \gamma \in \Gamma$, is a 2×2 orthogonal matrix. We call $\gamma^{(i)}$ a rotation if its two eigenvalues are conjugate complex numbers of the form $e^{\sqrt{-1}\theta}, e^{-\sqrt{-1}\theta}$. Otherwise $\gamma^{(i)}$ is called a reflection and its eigenvalues are $1, -1$.

For $A \in M_n(\mathbf{C})$ we denote by $||A||$ the spectral norm of A with respect to the given inner product $(\cdot,\cdot)$:

$$||A||^2 = \max_{(x,x)=1} (Ax, Ax).$$

§2. Main results

Theorem 2. *Let $\Gamma \le GL_n(\mathbf{R})$ be a finite abelian group over the field of real numbers $\mathbf{R}$. Assume that each $A \in \Gamma$ is conjugate to some rational valued matrix $\tilde{A} \in GL_n(\mathbf{Q})$, i.e. $A = T\tilde{A}T^{-1}, T \in GL_n(\mathbf{R})$. Then* (0.1) *holds. All the bounds in* (0.1) *are sharp.*

Proof. As Γ is finite, each $\tilde{A} \in GL_n(\mathbf{Q})$ has a finite order. It is known that $\tilde{A}$ is similar to a matrix $\hat{A} \in GL_n(\mathbf{Z})$, e.g. [Ser, p. 124]. By considering the inner product induced by $S(\Gamma) \in GL_n(\mathbf{R})$ we may assume that Γ is a finite group of orthogonal matrices. As Γ is abelian we fix a real orthonormal basis so that each $A \in \Gamma$ is a direct sum of 2×2 or 1×1 real orthogonal matrices. Obviously, each 1×1 block is equal to ± 1. Assume that we factored out the maximal number of

1×1 blocks. Let $\Gamma' \leq \Gamma$ be the subgroup of all elements which have the entry 1 on 1×1 blocks. It easily follows that Γ' is normal and $|\Gamma/\Gamma'| \leq 2^k$, where k is the number of 1×1 blocks. Note that $2m = n - k$, where m is the number of 2×2 blocks in each $A \in \Gamma$. Let $A, B \in \Gamma'$. Then $A_1 \oplus \cdots \oplus A_m, B_1 \oplus \cdots \oplus B_m$ are the 2×2 components of A, B respectively. We claim that each A_i, B_i is a rotation on $\mathbf{R}^2$. Assume to the contrary that A_i is a reflection on $\mathbf{R}^2$. Since $AB = BA$ it follows that $B_i = A_i, -A_i, I, -I$. Obviously, by changing the orthogonal basis in $\mathbf{R}^2$ we get that all A_i are diagonal matrices, contrary to our assumption that we factored out the maximal number of 1×1 blocks. Let θ_i, ϕ_i be the the angles of rotations A_i, B_i respectively in $\mathbf{R}^2$ for $i = 1, ..., m$.

We now prove the first inequality of the theorem. Clearly, it is enough to show that $|\Gamma'| \leq 6^m$. Divide the unit circle $[0, 2\pi)$ to six equal parts each one consisting of half open and half closed intervals of length $\frac{\pi}{3}$. Assume that θ_i, ϕ_i are in the same part of $[0, 2\pi)$ for $i = 1, ..., m$. We claim that $A = B$. Assume to the contrary that $A \neq B$. As

$$||A_i - B_i|| = |e^{\sqrt{-1}\theta_i} - e^{\sqrt{-1}\phi_i}|, \quad i = 1, ..., m,$$

we deduce that $0 < ||A - B|| < 1$. Observe next that $||A - B|| = ||I - A^{-1}B||$. Our assumptions that each $E \in \Gamma$ is similar to $E' \in GL_n(\mathbf{Q})$ yields that $C = A^{-1}B$ is similar to $\hat{C} \in GL_{2m}(\mathbf{Z})$. As Γ is a finite group, it follows that $\hat{C}^q = I$. Hence, the spectrum of $\hat{C}$ is a union of the roots of several cyclotomic polynomials. As $\hat{C} \neq I$, it follows from Lemma 2 that

$$||I - C|| \geq \inf_{l>1} \psi(l) = \psi(6) = 1.$$

This contradicts our assumption that $||A - B|| < 1$. Hence, $A = B$. Thus, the matrix A is completely determined by specifying one of the six intervals where θ_i lies for $i = 1, ..., m$. Hence, $|\Gamma'| \leq 6^m$. To see that this inequality is sharp observe that a companion matrix of the cyclotomic polynomial $x^2 - x + 1$ generates a cyclic group of order 6 in $GL_2(\mathbf{Z})$.

Assume now that the order of Γ is odd. Then all 1×1 blocks consist of 1. That is $\Gamma = \Gamma'$. Partition the unit circle to three half open and half closed intervals of length $\frac{2\pi}{3}$. Lemma 2 yields that

$$\inf_{k>1} \psi(2k - 1) = \psi(3) = \sqrt{3}.$$

Deduce as above that if each θ_i, ϕ_i lie in the same part of $[0, 2\pi)$ for $i = 1, ..., m$, then $A = B$. Therefore $|\Gamma| \leq 3^m$. To see that this inequality is sharp observe that a companion matrix of the cyclotomic polynomial $x^2 + x + 1$ generates a cyclic group of order 3 in $GL_2(\mathbf{Z})$.

Assume finally that $3 \not| \, |\Gamma|$. Consider the subgroup Γ'. Partition the unit circle to four half open and half closed intervals of length $\frac{\pi}{2}$. According to Lemma 2 $\inf_{k>1, 3 \not| k} \psi(k) = \psi(4) = \sqrt{2}$. Deduce as above that if each θ_i, ϕ_i lie in the same part of $[0, 2\pi)$ for $i = 1, ..., m$, then $A = B$. Therefore $|\Gamma'| \leq 4^m$. Hence, $|\Gamma| \leq 2^n$. This inequality is sharp for the following groups. For $n = 1$ the theorem is sharp for $G_1 = \{1, -1\}$. For $n = 2$ the theorem is sharp for G_2—the group of rotations of $\mathbf{R}^2$ by the angles $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$. Then the theorem is sharp for any group which is a direct sum of copies of G_1, G_2. Note that if $n = 2m$ then $G_2 \oplus \cdots \oplus G_2 \subset SO_{2m}(\mathbf{Z})$. $\square$

Theorem 3. *Let $\Gamma \leq GL_n(\mathbf{Q})$ be a finite group. Then there exists K so that $|\Gamma| \leq 2^n n!$ for $n > K$. Furthermore, $|\Gamma| = 2^n n!$ iff $\Gamma = TO_n(\mathbf{Z})T^{-1}$ for some $T \in GL_n(\mathbf{Q})$.*

Proof. Let $\Gamma \leq GL_n(\mathbf{Q})$ be a finite group of the maximal order. (See for example [Fri] for a crude upper bound on $|\Gamma|$.) Then Γ is strongly maximal. Let Δ be a maximal normal abelian subgroup of Γ of the maximal order. In what follows we use the notations and the results of Theorem 1.

Set $I = \{i : 1 \leq i \leq t, m_i \neq 1, 2, 4, 6\}$. Let $G' \subset GL_{n'}(\mathbf{Q})$ be the direct product of all $G_i, i \in I$. Since Δ is maximal, it follows that $D' = \prod_{i\in I} \times D_i$ is a normal abelian group of the maximal order. In view of Lemma 3,

$$|D'| = \prod_{i\in I} m_i^{k_i} \leq \prod_{i\in I} 3.5^{\frac{k_i\phi(m_i)}{2}} \leq 3.5^{\frac{n'}{2}}.$$

Hence

$$|G'| \leq j(n')3.5^{\frac{n'}{2}}.$$

Use Weisfeiler's bound (0.2) for $j(l)$ to deduce the existence of K' such that

$$j(l)3.5^{\frac{l}{2}} < 2^l l!, \quad l > K'.$$

We claim that $n' \leq K'$. Assume to the contrary that $n' > K'$. In the decomposition $\Gamma = \prod_1^t \times G_i$ replace the factor G' by $O_{n'}(\mathbf{Z})$ to obtain a finite group $\Gamma' \leq GL_n(\mathbf{Q})$ with $|\Gamma'| > |\Gamma|$. This contradicts that Γ has the maximal order.

We now treat the cases $m_i = 1, 2, 4, 6$. For the simplicity of notation for a positive integer k we let $J_k = \{i : 1 \leq i \leq t, m_i = k\}$. Set $G^{(k)}$ to be the direct product of all $G_i, i \in I_k$. Assume that $G^{(k)} \leq GL_{n^{(k)}}(\mathbf{Q})$.

Consider first the case $m_i = 6$. Observe that $\phi(6) = 2$. Hence, any $\Gamma_{i1} \leq GL_2(\mathbf{Q})$ (where Γ_{i1} is as in Theorem 1) is a finite group which contains a normal cyclic group Δ_{i1} of order 6. It is easy to show that $|\Gamma_{i1}| \leq 12$ and the equality holds iff $\Gamma_{i1} \cong \Lambda$—the group of rigid motions of the hexagon . Note that $n^{(6)}$ is even. From the assumption that Γ has the maximal order it follows that $G^{(6)} \cong \Lambda \wr S_{\frac{n^{(6)}}{2}}$. Thus

$$|G^{(6)}| = 12^{\frac{n^{(6)}}{2}}(\frac{n^{(6)}}{2})!.$$

Use Stirling's formula to deduce that

$$12^l l! < 2^{2l}(2l)!, \quad l > K^{(6)}.$$

Hence $n^{(6)} \leq 2K^{(6)}$.

We now consider the case $m_i = 4$. In that case $\phi(4) = 2$. Then $|\Gamma_{i1}| \leq 8$ where the equality holds iff $\Gamma_{i1} \cong O_2(\mathbf{Z})$—the group of the rigid motions of the square. Again, $n^{(4)}$ is even. Since Γ has the maximal order it follows that $G^{(4)} \cong O_2(\mathbf{Z}) \wr S_{\frac{n^{(4)}}{2}}$. Thus

$$|G^{(4)}| = 8^{\frac{n^{(4)}}{2}}(\frac{n^{(4)}}{2})!.$$

Clearly

$$8^l l! < 2^{2l}(2l)!, \quad l > 1.$$

Thus, if J_4 is not empty, $n^{(4)} = 2$.

Assume that $m_1 = 1$. Then

$$|G^{(1)}| = n^{(1)}! < 2^{n^{(1)}} n^{(1)}!.$$

Hence, $J_1 = \emptyset$.

Consider now the case $m_i = 2$. As $\phi(2) = 1$ it follows that either $\Gamma_{i1} = \{1\}$ or $\Gamma_{i1} = \{\pm 1\} = O_1(\mathbf{Z})$. The assumption that Γ has the maximal order implies that $\Gamma_{i1} = O_1(\mathbf{Z})$ and $G^{(2)}$ is conjugate to $O_{n^{(2)}}(\mathbf{Z})$. Thus

$$|G^{(2)}| = 2^{n^{(2)}} (n^{(2)})!.$$

We thus showed that

$$\begin{aligned} |\Gamma| = |G^{(2)}||G'||G^{(4)}||G^{(6)}|, \quad n^{(2)} \geq n - r, \quad r = (K' + 2 + 2K^{(6)}), \\ |G'||G^{(4)}||G^{(6)}| \leq \tilde{K}. \end{aligned} \tag{2.1}$$

Let L be the smallest number so that

$$\frac{|O_{L+1}(\mathbf{Z})|}{|O_L(\mathbf{Z})|} = 2(L+1) > \tilde{K}. \tag{2.2}$$

Assume that $n > L + r$. Use (2.1) and (2.2) to deduce that if one of the groups $G', G^{(4)}, G^{(6)}$ appears in the decomposition of Γ then by discarding one of these subgroups and enlarging correspondingly the size of the group $G^{(2)}$ we increase the order of Γ. This contradicts the maximality the order of Γ. Hence $\Gamma = G^{(2)}$. That is, in the decomposition of Γ given by Theorem 1 $t = 1$ and $k_1 = n$. Let $0 \neq w_1 \in W_{11}$. Note that $\{w_1\}$ form a basis in W_{11}. Let $w_i = \gamma w_1 \in W_{1i}$ for a corresponding $\gamma \in \Gamma$. Then $\{w_1, ..., w_n\}$ form a basis in $\mathbf{Q}^n$. In this basis Γ is represented by $O_n(\mathbf{Z})$. Thus, for $n > L + r$ the group $O_n(\mathbf{Z})$ is the unique subgroup (up to conjugacy) of the maximal order. The proof of the theorem is completed. $\square$

Acknowledgement

I would like to thank the referee for his valuable remarks.

References

[C-R] C.W. Curtis and I. Reiner, *Methods of representation theory I*, J. Wiley, 1981. MR **82i:**20001

[Fei] W. Feit, The orders of finite linear groups, preprint 1995.

[Fri] S. Friedland, Discrete groups of unitary isometries and balls in hyperbolic manifolds, *Linear Algebra Appl.*, 241-243 (1996), 305-341. CMP 96:15

[Kat] Y. Katznelson, On the orders of finite subgroups of $GL(n, \mathbf{Z})$, preprint, 1994.

[Min] H. Minkowski, Collected Works I, 212-218.

[R-T] D.N. Rockmore and K.S. Tan, A note on the order of finite subgroups of $GL(n, \mathbf{Z})$, *Arch. Math.* 64 (1995), 283-288. MR **95k:**20075

[Ser] J.P. Serre, *Lie algebras and Lie groups*, 2nd ed., Springer-Verlag, Berlin, 1992. MR **93h:**17001

[Wei1] B. Weisfeiler, Post-classification of Jordan's theorem on finite linear groups, *Proc. Natl. Acad. Sci. USA*, 81 (1984), 5278- 5279. MR **85j:**20041

[Wei2] B. Weisfeiler, On the size and structure of finite linear groups, preprint.

Department of Mathematics, University of Illinois at Chicago, Chicago, Illinois 60607-7045

E-mail address: `friedlan@uic.edu`