The structure of maximal finite primitive matrix groups

Gabriele Nebe

Lehrstuhl B für Mathematik, RWTH Aachen
Templergraben 64, 52062 Aachen, Germany
gabi@math.rwth-aachen.de

1 Introduction

The finite subgroups of $GL_n(\mathbb{Q})$ are classified up to dimension $n = 31$ by giving a system of representatives for the conjugacy classes of the maximal finite ones ([12], [9], [5], [6], [7]) cf. [11] for a survey on this and interrelations between these groups. Recently the classification has been extended to the one of absolutely irreducible maximal finite subgroups G of $GL_n(\mathcal{D})$, where $\mathcal{D}$ is a totally definite quaternion algebra and $n \cdot dim_{\mathbb{Q}}(\mathcal{D}) \leq 40$. As usual a subgroup $G \leq GL_n(\mathcal{D})$ is called *absolutely irreducible*, if the enveloping $\mathbb{Q}$-algebra $\overline{\mathbb{Q}G} := \{\sum_{g \in G} a_g g \mid a_g \in \mathbb{Q}\} \subseteq \mathcal{D}^{n\times n}$ is the whole matrix ring $\mathcal{D}^{n\times n}$ (cf. [8]). The classification of these groups yields a partial classification of the rational maximal finite matrix groups in the new dimensions 32, 36, and 40 on one hand and on the other hand it gives nice Hermitian structures for interesting lattices. For example one finds eleven quaternionic structures of the Leech lattice as a Hermitian lattice of rank $n > 1$ over a maximal order in a definite quaternion algebra $\mathcal{D}$ with absolutely irreducible maximal finite automorphism group as displayed in Table 1.

Rather than giving a survey of the classification results this note is devoted to a general structure theorem (cf. Theorem 4 below).

2 The algebraic situation

The theoretical and computational methods apply to a quite general situation: Let $\mathcal{D}$ be a division algebra of finite dimension over $\mathbb{Q}$ equipped with a positive involution $^- : \mathcal{D} \to \mathcal{D}$, i.e. $^-$ is an anti-automorphism of order ≤ 2 of the $\mathbb{Q}$-algebra $\mathcal{D}$ such that the fixed

Table 1. Quaternionic structures of the Leech lattice

$\mathcal{D}$	n	$Aut_h(L)$	$\lvert Aut_h(L)\rvert$
$Q_{\infty,2}$	6	$2.G_2(4)$	$2^{13}\cdot 3^3\cdot 5^2\cdot 7\cdot 13$
$Q_{\infty,5}$	6	$SL_2(25)$	$2^4\cdot 3\cdot 5^2\cdot 13$
$Q_{\infty,5}$	6	$2.J_2.2$	$2^9\cdot 3^3\cdot 5^2\cdot 7$
$Q_{\infty,11}$	6	$SL_2(11).2$	$2^4\cdot 3\cdot 5\cdot 11$
$Q_{\infty,13}$	6	$SL_2(13).2$	$2^4\cdot 3\cdot 7\cdot 13$
$Q_{\sqrt{3},\infty^2}$	3	$(\pm U_3(3)).2$	$2^5\cdot 3^3\cdot 7$
$Q_{\sqrt{5},\infty^2}$	3	$2.J_2$	$2^8\cdot 3^3\cdot 5^2\cdot 7$
$Q_{\sqrt{7},\infty^2}$	3	$C_4 2^2 L_2(7)$	$2^6\cdot 3\cdot 7$
$Q_{\sqrt{13},\infty^2}$	3	$SL_2(13)$	$2^3\cdot 3\cdot 7\cdot 13$
$Q_{\sqrt{21},\infty^2}$	3	$\pm C_3 2^2 L_2(7)$	$2^5\cdot 3^2\cdot 7$
$Q_{\omega_{13},\infty^3,13}$	2	$\pm C_{13}.C_4$	$2^3\cdot 13$

field $K^+ := \{x \in \mathcal{D} \mid x = \bar{x}\}$ is a totally real number field and $x\bar{x}$ is totally positive for all $0 \neq x \in \mathcal{D}$. We assume further that K^+ is contained in the center $K := Z(\mathcal{D})$ of $\mathcal{D}$. The involution $^-$ is extended to a mapping of the whole matrix ring $\mathcal{D}^{n\times n}$ by applying it to the entries of the matrices such that $X \mapsto \bar{X}^{tr}$ is an involution of the matrix ring $\mathcal{D}^{n\times n}$. Then the $\mathcal{D}$-vector space $\mathcal{D}^n$ has a totally positive definite Hermitian form $(x, y) := \sum_{i=1}^n x_i\bar{y}_i$. Taking the average over the finite group G, one finds that

$$\frac{1}{|G|}\sum_{g\in G} g\bar{g}^{tr} \in \mathcal{F}_h^{>0}(G) :=$$
$$\{F \in \mathcal{D}^{n\times n} \mid F = \bar{F}^{tr},\ gF\bar{g}^{tr} = F \text{ for all } g \in G,$$
$$F \text{ totally positive definite }\}.$$

Since $\mathcal{D}$ is finite dimensional over $\mathbb{Q}$ the order of a finite subgroup G of $GL_n(\mathcal{D})$ can be bounded by a formula given in [14]. So there are only finitely many conjugacy classes of finite subgroups in $GL_n(\mathcal{D})$. The most interesting ones are the maximal finite subgroups of $GL_n(\mathcal{D})$ since they contain all the other finite ones. Moreover these maximal finite subgroups are full automorphism groups of highly symmetric Hermitian lattices. In this paper it is shown that the structure of the primitive maximal finite matrix groups is fairly restricted: The generalized Fitting group already determines a normal subgroup with metabelian factor group the index of which can be bounded.

Constructing the maximal finite groups, one clearly may restrict to the irreducible ones, as one can build up the reducible maximal finite matrix groups from the ones in smaller dimensions (cf. [10]). This is also true for imprimitive groups: the imprimitive maximal finite subgroups of $GL_n(\mathcal{D})$ are full wreath products of a maximal finite primitive subgroup of $GL_d(\mathcal{D})$ with the symmetric group of degree $\frac{n}{d}$. So one only has to construct the primitive maximal finite groups, where a finite subgroup G of $GL_n(\mathcal{D})$ is called *primitive*, if the natural representation of G is irreducible over $\mathcal{D}$ and G does not embed into a wreath product with more than one factor. Since the central primitive idempotents in the enveloping algebra of a normal subgroup of G give rise to a system of imprimitivity of G, primitivity has the following important consequence:

Remark 1. Let $G \leq GL_n(\mathcal{D})$ be a finite primitive group and $N \trianglelefteq G$ be a normal subgroup of G. Then the K-algebra $\overline{KN}$ spanned by the matrices in N over the centre $K = Z(\mathcal{D})$ is a simple algebra.

Therefore only one irreducible K-representation of N occurs in the restriction of the natural representation of a primitive matrix group G to a normal subgroup N. In particular if N is abelian this implies that N is cyclic. Since the p-groups for which all abelian characteristic subgroups are cyclic are classified by P. Hall (cf. [3, p. 357]) this observation yields a (short) list of possible normal p-subgroups of a primitive matrix group G. Using this list and the classification of finite simple groups and their characters (cf. [2], [4], [15]), one gets the candidates for the generalized fitting groups $Fit_{gen}(G)$, the product of the maximal nilpotent normal subgroup with the quasi-semi-simple normal subgroups of G, for finite primitive subgroups G of $GL_n(\mathcal{D})$.

3 Arithmetic properties

To get further insight in the structure of the maximal finite primitive matrix groups one has to use some arithmetic properties. Let $\mathbb{Z}_K$ be the ring of integers in K and $\mathfrak{M}$ a maximal order in $\mathcal{D} \cong End_{\mathcal{D}^{n\times n}}(\mathcal{D}^n)$.

If $G \leq GL_n(\mathcal{D})$ is a finite matrix group, then the $\mathbb{Z}$-lattice $\mathfrak{M} \otimes_{\mathbb{Z}_K} \overline{\mathbb{Z}_K G}$ spanned by $\mathfrak{M}$ and the matrices in G is closed under multiplication hence it is an order in the algebra $\mathcal{D} \otimes_K \overline{KG}$. Since orders are contained in maximal orders and the latter are endomorphism rings of lattices (finitely generated projective $\mathfrak{M}$-modules that span $\mathcal{D}^n$) one gets that the set of G-invariant $\mathfrak{M}$-lattices

$$\mathcal{Z}_{\mathfrak{M}}(G) := \{L \subseteq \mathcal{D}^n \mid L \text{ is a full } \mathfrak{M}\text{-lattice in } \mathcal{D}^n \text{ with } Lg = L \text{ for all } g \in G\}$$

is not empty. In particular a finite group $G \leq GL_n(\mathcal{D})$ is maximal finite, if and only if G is the full automorphism group of all its invariant lattices: $G = Aut(L, F) := \{x \in GL_n(\mathcal{D}) \mid Lx = L, xF\overline{x}^{tr} = F\}$ for all $(L, F) \in \mathcal{Z}_{\mathfrak{M}}(G) \times \mathcal{F}_h^{>0}(G)$.

There is a canonical process, the radical idealizer process, which attaches to an order Λ_0 in a semisimple algebra A a chain of orders $\Lambda_0 \subset \Lambda_1 \subset \ldots$ that ends with a hereditary order $\Lambda_e = \Lambda_{e+1}$. Namely Λ_i is the right idealizer of the arithmetic radical of Λ_{i-1} $i = 1, 2, \ldots$ (cf. [1], [13]). If N is a normal subgroup of a primitive matrix group G, then $\overline{\mathbb{Z}_K N} =: \Lambda_0$ is an order in the simple algebra $\overline{KN} =: A$. Clearly G acts on Λ_0 and hence on the hereditary order Λ_e by conjugation. Therefore the matrices in G and Λ_e generate an order and there is a Λ_e-lattice in $\mathcal{D}^n$ that is G-invariant.

Remark 2. Let N be a normal subgroup of a primitive maximal finite subgroup G of $GL_n(\mathcal{D})$ and V the irreducible $\overline{KN}$-module occurring in the natural representation of N. As above let Λ_e be the hereditary order obtained by applying the radical idealizer process to the order $\Lambda_0 := \overline{\mathbb{Z}_K N}$. Let $L_1, \ldots, L_s$ be a system of representatives of isomorphism classes of Λ_e-lattices in V and $F \in \mathcal{F}_h^{>0}(N)$ a positive definite N-invariant Hermitian form. Then the generalized Bravais group

$$B_K^{\circ}(N) := \{g \in \overline{KN} \mid L_i g = L_i \text{ for all } i = 1, \ldots, s \text{ and } gF\bar{g}^{tr} = F\}$$

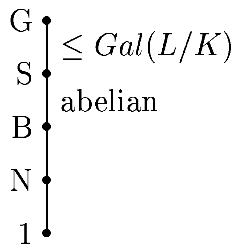
is a normal subgroup of G.

$B_K^{\circ}(N)$ is the unique maximal finite subgroup of the normalizer of N in the unit group of $\overline{KN}$ (cf. [12, (II.10)]).

Example 3. (cf. [8, Prop. 7.2, Cor. 7.4])
Let p be an odd prime and $N = O_p(G)$ the maximal normal p-subgroup of a primitive maximal finite matrix group G. It follows from a classification of P. Hall of those p-groups of which all abelian characteristic subgroups are cyclic, that there are $m, k \in \mathbb{N}_0$ such that $N = p_+^{1+2k} \curlyvee C_{p^m}$ is a central product of an extraspecial p-group of exponent p and a cyclic group of order p^m. Then $B^{\circ}_{\mathbb{Q}}(N) \cong \pm N.Sp_{2k}(p)$.

4 The structure of the maximal finite primitive matrix groups

Now we are able to describe the structure of the maximal finite primitive subgroups G of $GL_n(\mathcal{D})$. Let G be such a group, $N := Fit_{gen}(G)$ its generalized Fitting group. Then N is a normal subgroup of G that contains its centralizer. Let $B := B^{\circ}_K(N)$ be the generalized Bravais group of N. Since G is primitive, the enveloping algebra $A := \overline{KN} = \overline{KB}$ is a simple algebra. Hence the center $L := Z(A)$ is a field, the extension of K by the character values of an absolutely irreducible constituent of the natural character of N. The group G acts as Galois automorphisms on this abelian number field L. Let S be the kernel of this action.



Theorem 4. *(cf. [8, Theorem 6.8]) If $L = Z(A)$ is a totally real number field then the quotient group S/B is of exponent 1 or 2.*

Proof. Denote the commuting algebra $C_{\mathcal{D}^{n\times n}}(A)$ by C. Then $Z(A) = Z(C)$. Choose $F \in \mathcal{F}_h^{>0}(N)$. Then $c \mapsto c^{\circ} := F\bar{c}^{tr}F^{-1}$ is an involution on C and on A. The other N-invariant Hermitian forms are of the form cF with $c \in C^+$, the fixed space of $\,^{\circ}$. Note that $\,^{\circ} : C \to C$ depends on the choice of F but the corresponding involution on A

does not. In particular the restriction of the involution to the center L is independent of the choice of F. One easily sees that the induced involution is the complex conjugation on L, hence it is trivial because L is totally real.

Let $s \in S$. Since s induces a L-algebra automorphism on the central simple L-algebra A, the theorem of Skolem and Noether implies that there is an invertible element $a \in A$ with $as^{-1} \in C$. The matrix $aF\bar{a}^{tr}$ is again N-invariant, hence $aF\bar{a}^{tr} = cF$ for some $c \in C^+$. Moreover $c = aF\bar{a}^{tr}F^{-1}$ lies in the center L of C, because for $x \in C$ one has $cx^\circ = aF\bar{a}^{tr}F^{-1}(F\bar{x}^{tr}F^{-1}) = aF\bar{a}^{tr}\bar{x}^{tr}F^{-1} = aF\bar{x}^{tr}\bar{a}^{tr}F^{-1} = ax^\circ F\bar{a}^{tr}F^{-1} = x^\circ c$.

Therefore $c \in A$ and $a^2c^{-1}F(\overline{a^2c^{-1}})^{tr} = F$. Since the element s has finite order, there is $m \in \mathbb{N}$ such that $(a^2c^{-1})^m \in L$ commutes with the elements of N. Then $F = (a^2c^{-1})^m F(\overline{(a^2c^{-1})^m})^{tr} = (a^2c^{-1})^m(a^2c^{-1})^m F$. Hence $(a^2c^{-1})^{2m} = 1$ and therefore a^2c^{-1} is a unit of finite order in A normalizing N. By Remark 2 one gets that $b := a^2c^{-1}$ lies in B. Moreover $b^{-1}s^2$ commutes with every element of N and therefore lies in $C_G(N) \subseteq N$. □

If $L = Z(A)$ is not totally real, then the theorem above may be no longer true. I have no example of a primitive maximal finite group G where S/B is of exponent > 2 but the following example shows that such groups are likely to exist. Let $N := C_3 \times C_7 : C_3 = \langle z, x, y \mid z^3, x^7, y^3, x^y = x^2 \rangle$. Then N has an automorphism s of order 3, with $z^s = z$, $x^s = x$, $y^s = yz$. The non split extension $C_2 \times N.\langle s \rangle$ is a maximal subgroup of the $GU_3(5)$, in fact one could replace N by the irreducible matrix group $3.U_3(5) \leq GL_{144}(L)$ where $L := \mathbb{Q}[\sqrt{-3}, \sqrt{-7}]$. N has an irreducible faithful representation into $GL_3(L)$. The corresponding character extends to $S := \pm N : \langle s \rangle$ but the character value of xs involves further irrationalities. So if N (or $3.U_3(5)$) is a normal subgroup of a maximal finite primitive group G, then 3 divides the order of S/B (in the notation above).

The reason for this phenomenon is that $L = Z(\overline{\mathbb{Q}N})$ is a complex field. The element a^2c^{-1} in the above proof only satisfies $(a^2c^{-1})^m\overline{(a^2c^{-1})^m} = 1$. Let P be a prime ideal in L and $(\Lambda_e)_P$ be the completion of the hereditary order Λ_e at the prime P. The $(\Lambda_e)_P$-lattices in the simple $(\Lambda_e)_P$-module form a chain Ch_P. If $P \neq \bar{P}$, then a^2c^{-1} acts on this chain Ch_P say by shifting k-steps down. But then a^2c^{-1} acts on the chain $Ch_{\bar{P}}$ by shifting k-steps up.

The group generated by all possible shifts is abelian, so one finds that the image S/B of S is abelian. To get bounds on the rank and exponent of this abelian group let $U_1(L) := \{x \in L^* \mid x\bar{x} = 1\}$ be the unitary group of L and $\varphi(U_1(L))$ be the image of $U_1(L)$ in $\prod Sh_P =: Sh$ where the product runs over the set of unordered pairs of prime ideal $P \neq \bar{P}$ of L. Then S^2/B is isomorphic to a subgroup of $Sh/(\varphi(U_1(L)))$.

Let Cl be the group of all ideals I of L with $I\bar{I} = (1)$ modulo the group of principal ideals that are generated by an element of $U_1(L)$. Denote the rank of Cl by t and its exponent by g. Let r be the number of pairs of prime ideals $P \neq \overline{P}$ of L that divide the discriminant of Λ_e (and therefore the order of N). Let d be the degree of a L-irreducible constituent of the natural representation of N.

Proposition 5. *The quotient group S/B is abelian. The rank of S^2/B is bounded by $r+t$ and its exponent divides dg.*

Proof. For a prime ideal P of L let $Sh_P \cong \mathbb{Z}$ denote the group of all inclusion preserving permutations of the $(\Lambda_e)_P$-lattices in the irreducible $(\Lambda_e)_P$-module that are induced by elements of the normalizer of $(\Lambda_e)_P$ in A_P^*. The multiplicative group L^* acts on the Λ_e-lattices, hence one gets a homomorphism $L^* \to Sh_P$. The image is generated by multiplication with P and a subgroup of finite index say λ_P of Sh_P. Note that λ_P divides the dimension of the irreducible $(\Lambda_e)_P$-module (and hence d) and that $\lambda_P = 1$ if P does not divide the discriminant of Λ_e. Hence one gets an exact sequence

$$0 \to U_1(L) \to \prod Sh_P \to Cl \to 0.$$

Hence the rank of S^2/B is bounded by the rank of $Sh/\varphi(U_1(L)) \leq r+t$ and the exponent of S^2/B divides $exp(Sh/\varphi(U_1(L)))$ which divides dg. □

References

[1] H. Benz, H. Zassenhaus, *Über verschränkte Produktordnungen.* J. Number Theory **20** (1985), 282-298.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of finite groups.* Oxford University Press 1985.

[3] B. Huppert, *Endliche Gruppen I.* Springer-Verlag 1967.

[4] V. Landazuri, G.M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups.* J. of Algebra **32** (1974), 418-443.

[5] G. Nebe, *Endliche rationale Matrixgruppen vom Grad 24.*, Dissertation, RWTH Aachen (1995).

[6] G. Nebe, *Finite rational matrix groups of degree 24.*, Exp. Math. vol 5, number 3, 163-195 (1996)

[7] G. Nebe, *Finite subgroups of* $GL_n(\mathbb{Q})$ *for* $25 \leq n \leq 31$., Comm. Alg., 24(7),2341-2397 (1996)

[8] G. Nebe, *Finite quaternionic matrix groups.*, Electronic Journal of Representation Theory, to appear.

[9] G. Nebe, W. Plesken, *Finite rational matrix groups of degree 16.* AMS-Memoirs, No. 556, vol. 116 (1995).

[10] W. Plesken, *Some applications of representation theory.* Progress in Mathematics, vol 95: Representation Theory of Finite Groups and Finite-Dimensional Algebras, (ed. by G. O. Michler, C. M. Ringel), (1991), 477-496.

[11] W. Plesken, *Finite rational matrix groups - a survey.* Proceedings of the conference "The Atlas Ten Years On" 10. - 13.7.95 in Birmingham. LMS Lecture Notes in Mathematics (R.T. Curits, R.A. Wilson, editors)

[12] W. Plesken, G. Nebe, *Finite rational matrix groups.* AMS-Memoirs, No. 556, vol. 116 (1995).

[13] I. Reiner, *Maximal Orders.* Academic Press, 1975.

[14] I. Schur, *Über eine Klasse von endlichen Gruppen linearer Substitutionen.* 128-142 in I. Schur: *Gesammelte Abhandlungen I.* Springer Verlag 1973.

[15] G.M. Seitz, A.E. Zalesskii, *On the minimal degrees of projective representations of the finite Chevalley Groups, II.* J. of Algebra **158** (1993), 233-243.