COMPOSITIO MATHEMATICA

ARJEH M. COHEN
GABRIELE NEBE
WILHELM PLESKEN

Cayley orders

Compositio Mathematica, tome 103, nº 1 (1996), p. 63-74
<http://www.numdam.org/item?id=CM_1996__103_1_63_0>

Compositio Mathematica **103:** 63–74, 1996.

Cayley orders

ARJEH M. COHEN[1], GABRIELE NEBE and WILHELM PLESKEN[2]
[1]*Fac. Wisk. en Inf., TU Eindhoven, Postbox 513, 5600 MB Eindhoven, The Netherlands*
[2]*RWTH, Lehrstuhl B für Mathematik, Templergraben 64, 52062 Aachen, Germany*

Received 3 May 1994; accepted in final form 7 May 1995

1. Introduction

Let G be a finite subgroup of a real simple Lie group A. Then, viewing A as the real points of a simple algebraic group defined over $\mathbb{R}$ and using a result of Weil (cf. [Wei 64], [Slo 93], [CoW 94]), we can find a number field K and a K-form A_K of A so that G is conjugate in A to a subgroup of the group $A_K(K)$ of the K-rational points of A_K.

If A is compact of type G_2, then A is known to be the automorphism group $\mathrm{Aut}(C)$ of the real Cayley division ring C. In line with the above result, one might expect, for a finite subgroup G of A, a K-form C_K of C into whose automorphism group G embeds. Such a form C_K will be called a K-G-form (see below for a precise definition). Pushing it even further, one may ask for an RG-invariant order in C_K, where R is the ring of integers in K.

In [CoW 83], the finite subgroups of $G_2(\mathbb{C})$, resp. $\mathrm{Aut}(C)$, are described. The maximal finite ones that are not contained in a proper closed Lie subgroup (of nonzero dimension) are isomorphic to $2^3\cdot\mathrm{GL}(3,2)$, $G_2(2)$, $\mathrm{PSL}(2,8)$, or $\mathrm{PSL}(2,13)$ (one conjugacy class for each isomorphism type, see [Gri 94]). Viewed as subgroups of $\mathrm{GL}(C)$, they have unique minimal splitting fields K, namely $\mathbb{Q}, \mathbb{Q}, \mathbb{Q}(\cos(2\pi/9))$, $\mathbb{Q}(\sqrt{13})$ in the respective cases. It turns out that there is a unique K-form C_K with $G \leqslant \mathrm{Aut}(C_K)$.

Passing to the arithmetic of the situation, call a full $\mathbb{Z}$-lattice L in C_K a *Cayley order* for G, if

(i) L is multiplicatively closed;
(ii) L is G-invariant;
(iii) L is maximal with (i) and (ii).

GENERAL LEMMA. *Let L be a Cayley order in C_K for G. Then L is an R-lattice containing the unit element $e_0 = 1$ of C_K.*

Proof. Consider the full $\mathbb{Z}$-lattice generated by RL and Re_0. It is a Cayley order for G again and contains L, so must coincide with L. □

Remark. Let $C^0_{\mathbb{Q}}$ be the usual Cayley division algebra over $\mathbb{Q}$ (see section 2 below). A Cayley order in $C^0_{\mathbb{Q}}$ for the trivial group is a set of integral elements in the sense of [Dic 23], pp. 141–142; see also properties (i)–(iv) listed in [Cox 46].

In [Cox 46], Coxeter pointed out a Cayley order for the trivial group with $K = \mathbb{Q}$, which also is a Cayley order for $G_2(2)$. In [vdBS 59], it is shown that this Cayley order is unique up to isomorphism for the trivial group in $C^0_{\mathbb{Q}}$. This Cayley order is known to have 240 invertible elements. Its number theory has been investigated in [Reh 94].

The main result of this paper, which uses computer calculations as described in Section 4.2.2 of [HoP 89], contends that for all four maximal finite closed subgroups there are unique Cayley orders. But the Cayley orders for the three groups $\neq G_2(2)$ are less interesting in the sense that no surprising invertible elements are found to occur except for some well-known ones for $2^3 \cdot \mathrm{GL}(3,2)$. For instance the Cayley order for the latter group is spanned by the usual monomial basis $e_0, \ldots, e_7$ (see below) and $\frac{1}{2}(e_0 + \cdots + e_7)$; its invertible elements are $\pm e_i$ for $i = 0, \ldots, 7$.

THEOREM. *Let G be a subgroup of* $\mathrm{Aut}(C)$ *isomorphic to one of* $2^3 \cdot \mathrm{GL}(3,2)$, $G_2(2)$, $\mathrm{PSL}(2,8)$, *and* $\mathrm{PSL}(2,13)$, *and let* $K = \mathbb{Q}$, $\mathbb{Q}$, $\mathbb{Q}(2\cos(2\pi/9))$, $\mathbb{Q}(\sqrt{13})$ *in the respective cases. Then there is a unique K-G-form C_K of C on which G acts. Moreover, inside C_K there is a unique Cayley order for G. In the latter two cases, all of their invertible elements are contained in the units of R, the ring of integers of K (via the identification of $R \cdot e_0$ with R, where e_0 is the identity element of C).*

2. Preliminaries

We first recall an explicit construction of the real Cayley division ring C. As a vector space, C is 8-dimensional over $\mathbb{R}$ with basis $(e_i | i = 0, \ldots, 7)$ (the nonzero indices will be taken mod 7 with values in $1, \ldots, 7$). With respect to this basis the multiplication is given by

$$\begin{array}{ll} e_i^2 = -e_0 & \text{for } i = 1, \ldots, 7, \\ e_i e_j = -e_j e_i = e_k & \text{if } (i,j,k) = (1+\ell, 2+\ell, 4+\ell) \text{ for some } \ell, \\ e_0 e_j = e_j e_0 = e_j & \text{for all } j. \end{array}$$

We denote by $C^0_{\mathbb{Q}}$ the $\mathbb{Q}$-subalgebra of C with $\mathbb{Q}$-basis $e_0, \ldots, e_7$. By $(\cdot,\cdot)$ we denote the standard inner product with respect to this basis. A characteristic property of C is that the corresponding quadratic form N with $N(x) := (x,x)$ is multiplicative, i.e., $N(xy) = N(x)N(y)$ for all $x, y \in C$. Moreover this inner product defines an involution $^- : C \to C$, $x \mapsto 2(x, e_0)e_0 - x$. Then $(x,y)e_0 = \frac{1}{2}(x\overline{y} + y\overline{x}) = (x\overline{y}, e_0)e_0$ for all $x, y \in C$.

Let $\pi : C \to C$ be the orthogonal projection onto $\mathbb{R}e_0 = \mathrm{Fix}_C(^-)$ and $\pi' := \mathrm{id} - \pi$. Then $\pi(x) = \frac{1}{2}(x + \overline{x}) = (x, e_0)e_0$ and $\pi'(x) = \frac{1}{2}(x - \overline{x})$ for all $x \in C$.

Note $C = \mathbb{R}e_0 \oplus V$ with $V = \langle e_1, \ldots, e_7\rangle_{\mathbb{R}} = \pi'(C)$, the orthogonal complement of $\mathbb{R}e_0$ in C.

Let G be a finite subgroup of Aut(C). Call a K-subspace C_K of C a K-G-form of C, if

(i) C_K has a K-basis which is an $\mathbb{R}$-basis of C;
(ii) C_K is a K-subalgebra of C;
(iii) G acts on C_K by K-algebra automorphisms.

Denote the orthogonal complement (with respect to N) of Ke_0 in C_K by V_K.

Thus, for example, $C^0_{\mathbb{Q}}$ is a K-1-form of C and $V_{\mathbb{Q}} = \langle e_1, \ldots, e_7\rangle_{\mathbb{Q}}$.

For the proof of the next lemma one needs the following

MULTIPLICATION FORMULA. $\pi'(x \cdot \pi'(x \cdot y)) = (x, y)x - (x, x)y$ *for all* $x, y \in V$.

Proof. Let $x, y \in V$. Then using the fact that $\pi'(z) = z - (z, e_0)e_0$ for all $z \in C$, one gets $\pi'(x \cdot \pi'(x \cdot y)) = x(xy) - (xy, e_0)x - (x(xy), e_0)e_0 + (xy, e_0)(x, e_0)e_0$ $(*)$. Since $x, y \in V$ one has $(y, e_0) = (x, e_0) = 0$ and $x(xy) = x^2y = -N(x)y \in V$. Moreover $(xy, e_0) = (x, \overline{y}) = -(x, y)$. Using $(*)$, we find $\pi'(x \cdot \pi'(x \cdot y)) = -N(x)y + (x, y)x$. □

UNIQUE K-G-FORM LEMMA. *Let K be a subfield of $\mathbb{R}$ such that $G \leqslant$ Aut(C) is conjugate under* GL(C) *to a subgroup of* $\mathrm{GL}_8(K)$. *Assume that the character of G on C is $1 + \chi$ with χ absolutely irreducible.*

(a) *There exists at most one K-G-form C_K of C.*
(b) *If χ satisfies $(\chi^{2-}, \chi) = 1$ (where χ^{2-} denotes the character of G on the skewsymmetric part $\bigwedge^2 V$ of $V \otimes V$), then there exists a K-G-form C_K of C.*

Proof.

(a) Let C_K, C'_K be K-G-forms of C. Clearly $C_K = Ke_0 \oplus V_K$, with V_K a simple KG-submodule of V (the orthogonal complement of $\mathbb{R}e_0$ in C). Similarly $C'_K = Ke_0 \oplus V'_K$. By absolute irreducibility there exists a $\lambda \in \mathbb{R}$ with $V'_K = \lambda V_K$, because a KG-isomorphism from V_K to V'_K extends uniquely to an $\mathbb{R}G$-isomorphism of V. Choose $v_1, v_2 \in V_K$ with $v_1v_2 = \alpha e_0 + w$ and $0 \neq w \in V_K$. Then $\lambda v_1\, \lambda v_2 = \lambda^2\alpha e_0 + \lambda(\lambda w)$. Since $\lambda w \in \lambda V_K = V'_K$ and $\lambda^2 w \in V'_K$ one concludes that $\lambda \in K$.
(b) The morphism $\bigwedge^2 V \to V$ determined by $x \wedge y \mapsto \pi'(xy)$ is G-equivariant. But, by the character condition, any such morphism is a scalar multiple of a nonzero generator of the 1-space of G-equivariant morphisms $\bigwedge^2 V \to V$. This generator is defined over V_K, and so there is $\lambda \in \mathbb{R}$, $\lambda \neq 0$, such that $\pi'(xy) \in \lambda V_K$ for all $x, y \in V_K$. Replacing V_K by $\lambda^{-1}V_K$, we find that

$$\pi'(xy) \in V_K \quad \text{for all} \quad x, y \in V_K.$$

But then the multiplication formula shows that $N(x) \in K$ and $(x, y) \in K$ for all $x, y \in V_K$. In particular, $xy = \pi'(xy) + \pi(xy) = \pi'(xy) + (xy, e_0)e_0 \in Ke_0 + V_K$. We conclude that $Ke_0 + V_K$ is a K-G-form. □

Now, let G be one of the four maximal finite subgroups mentioned above and let K be the minimal splitting field of the representation of G on C, resp. V. Then G satisfies the character conditions of the unique K-G-form lemma, hence there is a unique K-G-form in each case. Our computations show that $C_K = KC^0_{\mathbb{Q}}$. The latter follows immediately in the first 3 cases of G, but after some calculation in the last case (cf. below). It can also be concluded from [Spr 63], pg. 14. This establishes the first statement of the theorem in Section 1.

Coming to the arithmetic let L be a Cayley order for G in C_K. Then, as a KG-module, KL is isomorphic to $Ke_0 \oplus V_K$ where $V_K = \langle e_1, \ldots, e_7 \rangle_K$ is a simple KG-module of dimension 7. Set $L_1 := L \cap V_K$ and $L_1' := \pi'(L)$. Then L_1 and L_1' are RG-lattices in V_K by the General Lemma.

NORM LEMMA. *For any $x \in L$ we have $N(x) \in R$ and $\overline{x} = 2(x, e_0)e_0 - x \in L$.*

Proof. For $x \in L$ consider left multiplication with x. Its characteristic polynomial lies in $R[t]$, since $xL \subseteq L$. On the other hand x is a root of the quadratic polynomial $t^2 - 2(e_0, x)t + N(x)$ which must therefore divide the characteristic polynomial and hence lies in $R[t]$. The first part follows from a look at the constant term. The linear term gives $2(x, e_0) \in R$, so, by the General Lemma, $2(x, e_0)e_0 \in L$, whence $\overline{x} \in L$. □

COROLLARY. *Either* $L = \mathrm{R}e_0 \oplus L_1$ *or* $\mathrm{R}e_0 \oplus L_1 \subset L \subset \frac{1}{2}\mathrm{R}e_0 \oplus L_1'$ *with* $L_1'/L_1 \cong \frac{1}{2}R/R$ *and* $2(L_1, L_1') \subseteq R$.

Proof. Since $R \supseteq 2(e_0, L) = 2(e_0, \pi(L))$ one has $\pi(L) \subseteq \frac{1}{2}R$. Since $2R$ is a maximal ideal of R, there are only two possibilities: $\pi(L) = R$ or $\pi(L) = \frac{1}{2}R$. Moreover $2(L_1, L_1') = 2(L_1, L) \subseteq R$. □

For all four groups G it turns out that the second possibility occurs, i.e., L is a subdirect product of $\frac{1}{2}\mathrm{R}e_0$ and L_1' amalgamated over the common factor module $\frac{1}{2}R/R \cong L_1'/L_1 \cong \mathbb{F}_{2^n}$ with $n = [K : \mathbb{Q}]$ on which G acts trivially. For the prime ideals $\wp$ of R not containing 2 the above corollary has an important consequence.

ODD PRIME LEMMA. *Let $\wp$ be a prime ideal of R not dividing 2. Then the $\wp$-adic completion $L_\wp$ of L is given by $R_\wp e_0 \oplus (L_1)_\wp$ where $(L_1)_\wp$ is the unique $R_\wp G$-sublattice X of $K_\wp \otimes_K V_K$ with $X = X^\# := \{x \in K_\wp \otimes_K V_K \mid (X, x) \subseteq R_\wp\}$.*

Proof. From the decomposition numbers, cf. [JLPW 94], one immediately sees that $X/\wp X$ is a simple $R/\wp G$-module in all four cases. Therefore the set of $R_\wp G$-lattices in $K_\wp \otimes_K V_K$ forms a chain of the kind $\ldots \supseteq \wp^{-1}X \supseteq X \supseteq \wp X \supseteq \cdots$. Our later constructions show that there is an RG-lattice Y in V_K such that $Y \cdot Y \subseteq \mathrm{R}e_0 \oplus Y$ and $[Y^\# : Y]$ is a 2-power, where $Y^\# := \{x \in V_K \mid (Y, x) \subseteq R\}$.

(For instance $2L_1$ satisfies these requirements.) Hence there is exactly one $R_\wp G$-lattice X in $K_\wp \otimes_K V_K$ satisfying $X = X^\#$. Moreover $X \cdot X \subseteq R_\wp e_0 \oplus X$. □

This lemma leaves only the prime 2 to be investigated. There the lattice of RG-lattices in V_K is more complicated. It can however be computed by the method described in [HoP 89] pg. 105, which runs roughly as follows: Let M be any full RG-lattice in V_K and M' be a maximal RG-sublattice of M. Then M/M' is a simple $(R/\wp R)G$-module for some prime $\wp$ in R, hence M' is the kernel of an epimorphism $M \to S$ for some simple $(R/\wp R)G$-module S.

The remainder of this paper is devoted to this investigation and hence a case by case proof of the second part of the theorem in Section 1.

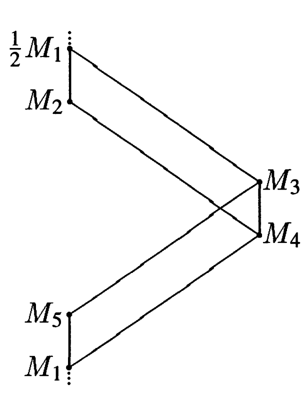
The final point of this section concerns the notation for matrices: they act from the right; diag$(A_1, \dots, A_n)$ denotes the block diagonal matrix with $A_1, \dots, A_n$ on the (block-)diagonal; for a permutation π in the symmetric group S_n usually given in disjoint cycle notation, $P_n(\pi)$ denotes the $n \times n$-permutation matrix whose (i, j)-entry is 1 if $i\pi = j$ and 0 otherwise.

3. The case $G = 2^3 \cdot \mathrm{GL}(3, 2)$

Here $K = \mathbb{Q}$ and $R = \mathbb{Z}$. With respect to the basis $(e_1, \dots, e_7)$ of V_K, the group G is generated by the following two matrices:

$$\mathrm{diag}(1,1,1,-1,-1,1,1) \cdot P_7((1,2)(3,6)),$$
$$\text{and } P_7((1,2,3,4,5,6,7)) \quad \text{(cf.[Cox 46])}.$$

Thus we can take $V_K = \oplus_{i=1}^7 \mathbb{Q} e_i$. Up to isomorphism (i.e., up to multiplication with elements of $\mathbb{Q}^*$) there are five $\mathbb{Z}G$-lattices $M_1, \dots, M_5$ in V_K. Representatives can be chosen as follows



$$M_1 = \langle e_1, \dots, e_7 \rangle$$
$$M_2 = \langle \textstyle\sum_{i=1}^7 \alpha_i e_i \mid \sum_{i=1}^7 \alpha_i \in \mathbb{Z}, \alpha_i \in \frac{1}{2}\mathbb{Z} \rangle$$
$$M_4 = \langle M_1, \tfrac{1}{2}(e_3 + e_5 + e_6 + e_7), \tfrac{1}{2}(e_2 + e_4 + e_5 + e_6), \tfrac{1}{2}(e_1 + e_4 + e_6 + e_7) \rangle$$
$$M_5 = \langle M_1, \tfrac{1}{2}(e_1 + \dots + e_7) \rangle$$

$\frac{1}{2}M_1/M_2$, M_2/M_4, and M_4/M_1 are nonisomorphic simple $\mathbb{F}_2G$-modules of dimensions 1, 3, 3, respectively. One has $M_1 \cdot M_1 = \mathbb{Z}e_0 \oplus M_1$, but $\langle M_1, \frac{1}{2}(e_0 + \dots + e_7) \rangle$ is still multiplicatively closed, whereas $M_4 \cdot M_4 = \frac{1}{2}\mathbb{Z}e_0 \perp^S \frac{1}{2}M_1$ is the subdirect product of $\frac{1}{2}M_1$ and $\frac{1}{2}\mathbb{Z}e_0$ amalgamated over the common factor module $S \cong \frac{1}{2}M_1/M_2 \cong \frac{1}{2}\mathbb{Z}e_0/\mathbb{Z}e_0$ and $M_5 \cdot M_5 = \frac{1}{4}\mathbb{Z} \oplus M_2$. Since the multiplicative closures of the lattices M_4 and M_5 are no longer lattices, one has that, as a $\mathbb{Z}$-lattice, the unique Cayley order for G is generated by $e_0, \dots, e_7$ and $\frac{1}{2}(e_0 + \cdots + e_7)$.

4. The case $G = G_2(2)$

Again $K = \mathbb{Q}$ and $R = \mathbb{Z}$. With respect to the basis $(e_1, \dots, e_7)$ of V_K, the group G is generated by the two matrices

$$\frac{1}{2}\begin{pmatrix} 0 & 1 & -1 & 0 & 0 & 1 & -1 \\ 0 & -1 & 0 & -1 & -1 & 1 & 0 \\ 0 & -1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & -1 & 0 & -1 \\ 0 & 0 & -1 & 1 & -1 & 0 & 1 \end{pmatrix} \quad \text{and } \operatorname{diag}(-1,1,1,1,1,1,-1) \cdot P_7((1,6)(4,7)).$$

Thus we can take $V_K = \oplus_{i=1}^{7} \mathbb{Q}e_i$. Up to isomorphism (i.e., up to multiplication with elements of $\mathbb{Q}^*$) there are two $\mathbb{Z}G$-lattices M_1 and M_2 in V_K. Representatives can be chosen as follows: $M_1 = \langle e_1,\ e_2,\ e_3,\ e_6,\ \frac{1}{2}(e_1 + e_2 + e_5 + e_6),\ \frac{1}{2}(e_2 + e_3 + e_6 + e_7),\ \frac{1}{2}(e_1 + e_2 + e_3 + e_4)\rangle_{\mathbb{Z}}$, $M_2 = \langle 2M_1,\ e_3 + e_4 + e_6\rangle$. Both M_1/M_2 and $M_2/2M_1$ are simple $\mathbb{F}_2G$-modules of dimensions 6 and 1, respectively. One has $M_2 \cdot M_2 = \mathbb{Z}e_0 \oplus M_2$, and $M_1 \cdot M_1 = \langle e_0,\ e_1,\ e_2,\ e_3,\ \frac{1}{2}(e_0 + e_3 + e_4 + e_6),\ \frac{1}{2}(e_1 + e_2 + e_5 + e_6),\ \frac{1}{2}(e_2 + e_3 + e_6 + e_7),\ \frac{1}{2}(e_1 + e_2 + e_3 + e_4)\rangle_{\mathbb{Z}} \cong \frac{1}{2}\mathbb{Z}e_0 \curlywedge^{S} \frac{1}{2}M_2$ is the subdirect product of $\frac{1}{2}\mathbb{Z}e_0$ and $\frac{1}{2}M_2$ amalgamated over the common factor module $S \cong \frac{1}{2}M_2/M_1 \cong \frac{1}{2}\mathbb{Z}e_0/\mathbb{Z}e_0$. Since $M_1 \cdot M_1$ is multiplicatively closed, it is the unique Cayley order for G.

5. The case $G = \mathrm{PSL}(2, 8)$

Now $R = \mathbb{Z}[\omega]$, where $\omega^3 - 3\omega + 1 = 0$, is the ring of all integers in $K = \mathbb{Q}(\omega) = \mathbb{Q}(\cos(2\pi/9))$. With respect to the basis $(e_1, \dots, e_7)$ of V_K, the group G is generated by the following three matrices

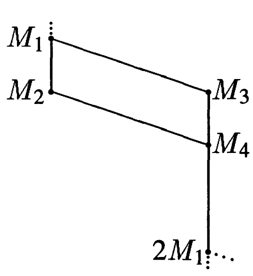
$$\operatorname{diag}(-1,1,1,-1,1,-1,-1) \leftrightarrow \begin{pmatrix} 1 & 0 \\ \omega & 1 \end{pmatrix},$$

$$P_7((1,2,3,4,5,6,7)) \leftrightarrow \begin{pmatrix} 1+\omega+\omega^2 & 0 \\ 1+\omega & \omega^2 \end{pmatrix},$$

$$\frac{1}{4}\begin{pmatrix} a & b & b+1 & c & -1 & a-1 & -\omega \\ b & b+1 & -c & -1 & -a+1 & \omega & -a \\ b+1 & -c & 1 & -a+1 & -\omega & a & -b \\ -c & 1 & a-1 & -\omega & -a & b & -b-1 \\ 1 & a-1 & \omega & -a & -b & b+1 & c \\ a-1 & \omega & a & -b & -b-1 & -c & -1 \\ \omega & a & b & -b-1 & c & 1 & -a+1 \end{pmatrix} \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Here $a := 3 - \omega - \omega^2$, $b := -2 + \omega^2$ and $c := -1 - \omega$. Again we can take $V_K = \oplus_{i=1}^7 K e_i$. The 2×2-matrices added indicate a correspondence with the usual presentation of $\mathrm{PSL}(2,8)$ over $\mathbb{F}_2[\omega]$. Note that $\langle e_1, \ldots, e_7 \rangle_R$ is not an RG-lattice in V_K.

Up to isomorphism (i.e., up to multiplication with elements of K^*) there are four RG-lattices $M_1, \ldots, M_4$ in V_K. Representatives can be chosen as follows



$$M_1 = \tfrac{1}{4}(e_1 + (\omega+\omega^2)e_2 + \omega e_3 + (1-\omega-\omega^2)e_4 - \omega^2 e_5 + (1+2\omega+\omega^2)e_6 - (1+\omega)e_7) \cdot RG$$

$$M_2 = \tfrac{1}{4}((-1+\omega)e_1 - e_2 + (\omega+\omega^2)e_3 - \omega e_4 - (1-\omega-\omega^2)e_5 - (2-2\omega-\omega^2)e_6 + (1+\omega^2)e_7) \cdot RG$$

$$M_3 = \tfrac{1}{2}(e_1 + \omega^2 e_4 + \omega e_6 + (-2+\omega-\omega^2)e_7) \cdot RG$$

$$M_4 = \tfrac{1}{2}(e_1 - \omega^2 e_3 - \omega^2 e_4 + \omega e_5 + \omega^2 e_6 + (1+\omega+\omega^2)e_7) \cdot RG$$

M_1/M_2, M_1/M_3, and $M_4/2M_1$ represent nonisomorphic simple $\mathbb{F}_8 G$-modules of dimensions 1, 4, 2, respectively.

One has $M_1 \cdot M_1 = \frac{1}{4}\mathrm{Re}_0 \oplus M_1$, $M_2 \cdot M_2 = \frac{1}{4}\mathrm{Re}_0 \,{}^{S}\!\!\!\curlywedge \frac{1}{2}M_3$, where $S \cong \frac{1}{4}\mathrm{Re}_0/\frac{1}{2}\mathrm{Re}_0 \cong \frac{1}{2}M_3/\frac{1}{2}M_4$, $M_3 \cdot M_3 = \frac{1}{4}\mathrm{Re}_0 \oplus \frac{1}{2}M_4$ and $M_4 \cdot M_4 = \frac{1}{2}\mathrm{Re}_0 \,{}^{S}\!\!\!\curlywedge M_3$, where $S \cong \frac{1}{2}\mathrm{Re}_0/\mathrm{Re}_0 \cong M_3/M_4$. It follows that $L = M_4 \cdot M_4$ is the unique Cayley order for PSL(2, 8).

Invertible elements of L have invertible norms lying in R. Being interested in which invertible values from R the Cayley norm takes, we compute modulo squares, as they are the norms of elements from R themselves. Modulo squares we have $R^*/(R^*)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$. So there are 8 invertible values modulo squares of R^*. They correspond to the 8 different sign patterns for the 3 real embeddings. But the norm values must be positive in each embedding, and so only the class of $1 \in R^*$ occurs as a norm value. The elements of L of norm 1 are precisely $\pm e_0$.

6. The case $G = \mathrm{PSL}(2, 13)$

We recall from [CoW 83] the following three elements of $\mathrm{Aut}(C)$ generating a subgroup G isomorphic to PSL(2, 13). The action is written with respect to the basis $e_1, \ldots, e_7$ of V. The 2×2 matrices added indicate a correspondence with the usual presentation of PSL(2, 13).

$$a = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 2 & 0 \\ 0 & 7 \end{pmatrix};$$

$$k = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & c_2 & 0 & s_2 & 0 & 0 & 0 \\ 0 & 0 & c_6 & 0 & 0 & 0 & s_6 \\ 0 & -s_2 & 0 & c_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & c_8 & -s_8 & 0 \\ 0 & 0 & 0 & 0 & s_8 & c_8 & 0 \\ 0 & 0 & -s_6 & 0 & 0 & 0 & c_6 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix};$$

where $c_j = \cos(j\pi/13)$ and $s_j = \sin(j\pi/13)$,

$$n = \frac{1}{\sqrt{13}} \begin{pmatrix} 1 & 0 & 0 & -2 & 0 & -2 & -2 \\ 0 & c & d & 0 & e & 0 & 0 \\ 0 & d & e & 0 & c & 0 & 0 \\ -2 & 0 & 0 & u & 0 & v & w \\ 0 & e & c & 0 & d & 0 & 0 \\ -2 & 0 & 0 & v & 0 & w & u \\ -2 & 0 & 0 & w & 0 & u & v \end{pmatrix} \leftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix};$$

where

$$c = \tfrac{1}{2}(-7 + \sqrt{13} + 8\cos(2\pi/13) + 4(3 - \sqrt{13})\cos^2(2\pi/13)),$$

$$d = \tfrac{1}{2}(-7 + \sqrt{13} + 8\cos(8\pi/13) + 4(3 - \sqrt{13})\cos^2(8\pi/13)),$$

$$e = \tfrac{1}{2}(-7 + \sqrt{13} + 8\cos(6\pi/13) + 4(3 - \sqrt{13})\cos^2(6\pi/13)),$$

$$u = \tfrac{1}{\sqrt{13}}(c + 2e - 2d),$$

$$v = \tfrac{1}{\sqrt{13}}(e + 2d - 2c),$$

$$w = \tfrac{1}{\sqrt{13}}(d + 2c - 2e).$$

Note that in [CoW 83] there are some misprints: $13 - \sqrt{13}$ should be $3 - \sqrt{13}$ and $\cos(\alpha)$ should be $2\cos(\alpha)$ in c, d, and e.

Now $R = \mathbb{Z}[\frac{3+\sqrt{13}}{2}]$ is the ring of all integers in $K = \mathbb{Q}(\sqrt{13})$. The first (and main) problem is to find a K-form C_K of C. The above data can be interpreted as an F-G-form C_F of C (isomorphic to $FC_{\mathbb{Q}}^0$ as F-algebra), where $F := \mathbb{Q}(\zeta_{52}+\zeta_{52}^{-1}) = \mathbb{Q}(\sin(2\pi/13))$ with $\zeta_{52} = \exp(2\pi i/52)$. The Galois descent from C_F to C_K can be performed roughly as follows. Let $(V_F)_K$ be the KG-module obtained from the FG-module V_F (of dimension 7 over F) by restricting scalars to K, so in particular $\dim_K(V_F)_K = 7 \cdot 6$ and $E := \mathrm{End}_{KG}((V_F)_K) \cong K^{6\times 6}$. From the way $(V_F)_K$ is given, one obtains F as a maximal subfield of E and can therefore easily construct E as a crossed product algebra of F with $\mathrm{Gal}(F/K) \cong C_6$. As a result of this, a parametrization of all simple KG-submodules W of $(V_F)_K$ ensues. One readily finds a W with $W \cdot W \subseteq Ke_0 \oplus W$, which therefore yields the unique K-G-form $C_K = Ke_0 \oplus W$. To be explicit, $W = V_K$ can be chosen as $\lambda e_1 \cdot KG$ with $\lambda = 13s - 64s^3 + 83s^5 - 45s^7 + 11s^9 - s^{11}$, where $s = \sin(2\pi/13)$ (in particular $\lambda^2 = \frac{3\sqrt{13}-13}{2}$). To prove $C_K \cong K \otimes_{\mathbb{Q}} C_{\mathbb{Q}}^0$ it suffices to check that the norm forms are equivalent by [vdBS 59] pg. 410. Again by the result of [vdBS 59] on composition algebras over complete discrete valuation rings and the local-global principle for quadratic forms over number fields, cf. [Sch 85] Cor. 6.6, it suffices to check that the norm form of C_K is totally positive definite, cf. also [Spr 63].

Up to isomorphism, there are two RG-lattices M_1 and M_2 in V_K. The quotients M_1/M_2 and $M_2/2M_1$ represent nonisomorphic $\mathbb{F}_4G$-modules of dimension 1 and 6, respectively. M_1 is as RG-lattice generated by $\frac{1}{2}\lambda e_1$, where λ is as above. M_2 is as RG-lattice generated by $\frac{1}{13}(\lambda_2 e_2 + \lambda_3 e_3 + \lambda_5 e_5)$, $\lambda_2 = 65s^2 - 169s^4 + 130s^6 - 39s^8 + 4s^{10}$, $\lambda_3 = 13 - 117s^2 + 143s^4 - 65s^6 + 13s^8 - s^{10}$, $\lambda_5 = 52 - 286s^2 + 364s^4 - 182s^6 + 39s^8 - 3s^{10}$, where $s = \sin(2\pi/13)$ is as above ($\lambda_2\lambda_3\lambda_5 = -169\lambda^2$).

One computes $M_1 \cdot M_1 = \frac{1}{4}\,\mathrm{Re}_0 \oplus \frac{1}{2}M_2$ and $M := M_2 \cdot M_2 = \frac{1}{2}\,\mathrm{Re}_0 \,{}_{\wedge}|^{S} M_1$, with $S \cong_{RG} (\frac{1}{2}R)/R \cong_{RG} M_1/M_2$. Observe that M is multiplicatively closed, whereas the multiplicative closure of the superlattice M_1 of M_2 is no longer a lattice in C_K. As in the case $G = \mathrm{PSL}(2,8)$ one obtains that $M = L$ is the unique Cayley order for $\mathrm{PSL}(2,13)$ and the invertible elements in L are the elements in $R^* e_0$.

Though everything in the above description of V_K is explicit, it is often more convenient to describe V_K with respect to a basis more adjusted to G. The matrices of G are monomial with respect to the $\mathbb{Q}$-basis $(v_1, \ldots, v_{14})$ of V_K where $v_i = \sum_{j=1}^{7} \alpha_{ij} e_j$ and

$$(\alpha_{ij}) = \begin{pmatrix}
13\lambda & 0 & 0 & 0 & 0 & 0 & 0 \\
\sqrt{13}\lambda & 0 & 0 & -2\sqrt{13}\lambda & 0 & -2\sqrt{13}\lambda & -2\sqrt{13}\lambda \\
\sqrt{13}\lambda & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 \\
\sqrt{13}\lambda & \lambda_3 & \lambda_2 & \alpha_7 & \lambda_5 & \alpha_8 & \alpha_9 \\
\sqrt{13}\lambda & \alpha_2 & \alpha_4 & \alpha_6 & \alpha_1 & \alpha_3 & \alpha_5 \\
\sqrt{13}\lambda & -\alpha_4 & -\alpha_1 & \alpha_5 & -\alpha_2 & \alpha_6 & \alpha_3 \\
\sqrt{13}\lambda & \lambda_5 & \lambda_3 & \alpha_8 & \lambda_2 & \alpha_9 & \alpha_7 \\
\sqrt{13}\lambda & \lambda_2 & \lambda_5 & \alpha_9 & \lambda_3 & \alpha_7 & \alpha_8 \\
\sqrt{13}\lambda & -\lambda_2 & -\lambda_5 & \alpha_9 & -\lambda_3 & \alpha_7 & \alpha_8 \\
\sqrt{13}\lambda & -\lambda_5 & -\lambda_3 & \alpha_8 & -\lambda_2 & \alpha_9 & \alpha_7 \\
\sqrt{13}\lambda & \alpha_4 & \alpha_1 & \alpha_5 & \alpha_2 & \alpha_6 & \alpha_3 \\
\sqrt{13}\lambda & -\alpha_2 & -\alpha_4 & \alpha_6 & -\alpha_1 & \alpha_3 & \alpha_5 \\
\sqrt{13}\lambda & -\lambda_3 & -\lambda_2 & \alpha_7 & -\lambda_5 & \alpha_8 & \alpha_9 \\
\sqrt{13}\lambda & -\alpha_1 & -\alpha_2 & \alpha_3 & -\alpha_4 & \alpha_5 & \alpha_6
\end{pmatrix}.$$

Here λ, λ_2, λ_3, and λ_5 are as above, and

$$\alpha_1 = 39 - 260s^2 + 416s^4 - 273s^6 + 78s^8 - 8s^{10},$$

$$\alpha_2 = 13 - 91s^2 + 52s^4 + 13s^6 - 13s^8 + 2s^{10},$$

$$\alpha_3 = -78s + 364s^3 - 442s^5 + 221s^7 - 49s^9 + 4s^{11},$$

$$\alpha_4 = -\alpha_1 - \alpha_2 - 13,$$

$$\alpha_5 = 26s - 91s^3 + 78s^5 - 26s^7 + 3s^9,$$

$$\alpha_6 = -26s + 78s^3 - 78s^5 + 39s^7 - 10s^9 + s^{11},$$

$$\alpha_7 = 13s + 26s^5 - 39s^7 + 16s^9 - 2s^{11},$$

$$\alpha_8 = 39s - 273s^3 + 390s^5 - 221s^7 + 55s^9 - 5s^{11},$$

and

$$\alpha_9 = 39s - 208s^3 + 221s^5 - 91s^7 + 16s^9 - s^{11},$$

where $s = \sin(2\pi/13)$ is as above.

With respect to the $\mathbb{Q}$-basis $(v_1, \ldots, v_{14})$ of V_K one has

$$a = -I_{14}P_{14}((3,12,11,14,5,6)(4,9,7,13,8,10)),$$

$$k = P_{14}((2,3,4,5,6,7,8,9,10,11,12,13,14)),$$

and

$$n = \operatorname{diag}(I_3, -1, I_2, -I_4, I_2, -1, 1)P_{14}((1,2)(3,14)(4,8)(5,6)(9,13)(11,12)).$$

The element in the commuting algebra of G corresponding to $\sqrt{13}$ is $(a_{ij})_{i,j=1}^{13}$, where

$$a_{ij} = \begin{cases} 0 & \text{if } i = j \\ -1 & \text{if } i = 1 \text{ or } j = 1 \text{ or } |i-j| \in \{1,3,4,9,10,12\} \\ 1 & \text{otherwise} \end{cases}$$

References

[CoW 83] Cohen, A. M. and Wales, D. B.: Finite subgroups of $G_2(C)$, *Comm. Algebra*, 11 (1983) 441–459.

[CoW 94] Cohen, A. M. and Wales, D. B.: Finite simple subgroups of semisimple complex Lie groups – a survey, pp. 77–96 in "Groups of Lie type and their geometries", eds. W. M. Kantor and L. Di Martino, LMS Lecture Notes, no. 207, Cambridge University Press, 1995.

[Cox 46] Coxeter, H. S. M.: Integral Cayley Numbers, *Duke Math. J.* 13 (1946) 561–578.

[Dic 23] Dickson, L. E.: A new simple theory of hypercomplex integers, *Journal de Mathématiques Pures et Appliquées (9)*, Vol. 2 (1923), 281–326.

[Gri 94] Griess, Jr., R. L.: Basic Conjugacy Theorems for G_2, Preprint 1994, University of Michigan, Ann Arbor.

[HoP 89] Holt, D. F. and Plesken, W.: Perfect Groups, Oxford University Press 1989.

[JLPW 94] Jansen, C., Lux, K., Parker, R. A. and Wilson, R. A.: An Atlas of Brauer Characters. In preparation.

[Reh 94] Rehm, H. P.: Prime factorization of integral Cayley octaves, *Annales de la Faculté des Sciences de Toulouse*, Vol. II, no. 2, (1993) 271–289.

[Sch 85] Scharlau, W.: Quadratic and Hermitian Forms, Springer-Verlag, 1985.

[Slo 93] Slodowy, P.: Two notes on a finiteness problem in the representation theory of finite groups, *Hamburger Beiträge zur Mathematik*, Heft 21, 1993, Universität Hamburg.

[Spr 63] Springer, T. A.: Oktaven, Jordan-Algebren und Ausnahmegruppen, Lecture Notes, Göttingen 1963.

[vdBS 59] van der Blij, F. and Springer, T. A.: The arithmetics of octaves and of the group G_2, *Proc. Nederl. Akad. Wet.* (1959) 406–418.

[Wei 64] Weil, A.: Remarks on the cohomology of groups, *Annals of Math.* 80 (1964) 149–157.