J. Eur. Math. Soc. 19, 581–599 © European Mathematical Society 2017

DOI 10.4171/JEMS/675

T. N. Venkataramana

Hypergeometric groups of orthogonal type

Received May 6, 2014 and in revised form January 29, 2015

Abstract. We obtain an infinite family of orthogonal hypergeometric groups which are higher rank arithmetic groups. We also list cases of arithmetic monodromy when the real Zariski closure of the hypergeometric group is $O(2, 3)$.

Keywords. Hypergeometric functions, monodromy, arithmetic groups of orthogonal groups

1. Introduction

Consider the ${}_nF_{n-1}$ type hypergeometric differential equation

$$D(\alpha, \beta, q)u = 0$$

where q varies over the thrice punctured sphere $C = \mathbb{P}^1 \setminus \{0, 1, \infty\}$, $\alpha, \beta \in \mathbb{Q}^n$,

$$D = D(\alpha, \beta, q) = \prod_{i=1}^{n} (\theta + \beta_i - 1) - q \prod_{i=1}^{n} (\theta + \alpha_i),$$

and $\theta = q\frac{d}{dq}$. Thus, D and θ are viewed as differential operators on the curve C. The fundamental group of C is the free group on two generators which can be taken to be small loops around 0 and ∞. The fundamental group acts on the space of solutions of this equation, and this action is called the *monodromy representation*. The action is by analytic continuation of solutions along the loops corresponding to elements of the fundamental group. The image of the resulting representation is called the *hypergeometric group* corresponding to the parameters α, β. If the images of the loops around 0 and ∞ under the monodromy representation are denoted h_0 and h_∞, then the hypergeometric group is generated by h_0, h_∞.

A theorem of Levelt completely describes the (${}_nF_{n-1}$-type) hypergeometric monodromy representation. We briefly recall the description. Assume that $\alpha_j - \beta_k$ is not an integer for any j, k. Equivalently, if we set $f(x) = \prod_{j=1}^{n}(x - e^{2\pi i\alpha_i})$ and $g(x) = \prod_{j=1}^{n}(x - e^{2\pi i\beta_j})$, then f, g have no common roots. Denote by A, B the companion matrices of f, g respectively. Then Levelt's theorem says that there exists a basis $\{u\}$ of solutions of the foregoing hypergeometric equation $Du = 0$ with respect to which the

T. N. Venkataramana: School of Mathematics, Tata Institute of Fundamental Research,
Homi Bhabha Road, Colaba, Mumbai 400005, India; e-mail: venky@math.tifr.res.in

Mathematics Subject Classification (2010): Primary 22E40; Secondary 20F36

matrix of the action of h_0 is A and that of h_∞ is B^{-1}. Thus a small loop around 1 goes to the matrix $C = A^{-1}B$ since $h_0 h_1 h_\infty = 1$. The element C is a complex reflection. Moreover, given any two coprime, monic, degree n polynomials f, g, the representation of the free group $F_2 = \langle x_0, x_\infty \rangle$ on two generators, given by $x_0 \mapsto A$, $x_\infty \mapsto B^{-1}$, is the hypergeometric monodromy representation corresponding to the parameters α, β with the roots of f, g being the exponentials of α_j, β_k as before.

Beukers and Heckman [2] have completely analysed the Zariski closure G of the foregoing monodromy. We now briefly describe their result, making the (simplifying) assumption that f, g are products of cyclotomic polynomials; their coefficients are then integers. Thus the hypergeometric group is a subgroup of $\mathrm{GL}_n(\mathbb{Z})$. Assume also that f, g form a primitive pair [2]. In [2] it is proved (see also [6, p. 6, (2)]) that if $f(0)/g(0) = -1$, then the Zariski closure G is (even as an algebraic group over $\mathbb{Q}$) either finite or the orthogonal group $O_n(h)$ of a non-degenerate rational quadratic form h (otherwise, n is even and G is the symplectic group). Thus the hypergeometric group is either a subgroup of an integral orthogonal group or a subgroup of the integral symplectic group.

In [9], Sarnak has asked when the hypergeometric group is *arithmetic* (i.e. has finite index in the integral points of its Zariski closure). Otherwise, the group is said to be *thin* [9]. In [6], the authors prove that when the resulting quadratic form has signature $(n-1, 1)$ (with very few exceptions; see [6, Conjecture 2]), the hypergeometric group is often thin, i.e. has infinite index in the integral orthogonal group. However, when the quadratic form has higher rank, i.e. has signature (p, q) with $p, q \geq 2$ or when the group G is the symplectic group, the situation is less clear. In [10], the case when G is the symplectic group is considered. It is proved in [10] that in a sizeable number of cases, the monodromy group is an arithmetic group; however, seven thin examples (with $G = \mathrm{Sp}_4$) have been given by Brav and Thomas [4] using a ping-pong argument. We understand that the methods of [4] can also prove thinness in some higher rank orthogonal cases. An example of a thin hypergeometric group in $O(2, 2)$ is given in [5].

In the present paper we show that for infinitely many odd integers n, and for suitable parameters α, β, the hypergeometric group is arithmetic, i.e. has finite index in the integral orthogonal group. We also give many examples of arithmetic monodromy when $G = O(2, 3)$ over $\mathbb{R}$ but has $\mathbb{Q}$-rank either one or two. There is some interest in constructing these examples because they are perhaps the first examples of higher rank arithmetic hypergeometric monodromy groups which are of *orthogonal* type. We prove

Theorem 1. *Let $m \geq 0$ be an integer. Let $f_0(x) = x^5 - 1$ and $g_0(x) = (x+1)(x^2+1)^2$. Suppose $P, Q \in \mathbb{Z}[x]$ are coprime monic polynomials of degree m such that if $f(x) = f_0(x)P(x^6)$ and $g(x) = g_0(x)Q(x^6)$ then f, g are coprime polynomials. Then the hypergeometric monodromy group $\Gamma(f, g)$ is an arithmetic subgroup of an integral orthogonal group $O(h)(\mathbb{Z})$ with $\mathbb{Q}$-rank$(h) \geq 2$.*

For example, if

$$f = (x^5 - 1)(x^{12} + x^6 + 1)^m, \quad g = (x+1)(x^2+1)^2(x^{12}+1)^m, \quad \text{or}$$
$$f = (x^5 - 1)(x^{12} - x^6 + 1)^m, \quad g = (x+1)(x^2+1)^2(x^{12}+1)^m,$$

then $\Gamma(f, g)$ is an arithmetic group.

Remark 1. Note that the degree of the representation is $n = 6m + 5$ with m *arbitrary*. Therefore, we get infinitely many examples of higher rank orthogonal monodromy.

The polynomials f_0, g_0 of Theorem 1 may be replaced by any pair f_1, g_1 for which $\mathbb{Q}$-rank$(H) = 2$, where $H = O_5$ is the Zariski closure of the 5×5 hypergeometric group $\Gamma(f_1, g_1)$. Thus the analogue of Theorem 1 gives many more examples of arithmetic monodromy. In Section 5, five more examples of pairs f_1, g_1 are given for which the monodromy group is arithmetic in $O(2, 3)$ and the associated group G has $\mathbb{Q}$-rank two.

Remark 2. Suppose $x = (x_1, \ldots, x_k) \in \mathbb{Q}^k$ and $r \in \mathbb{Q}$. Let us write $x + r$ for the k-tuple $(x_1 + r, \ldots, x_k + r)$. Consider the foregoing example $f = (x^5 - 1)(x^{12} + x^6 + 1)^m$. Its parameters are the $5 + 12m$ tuple which is obtained by pasting together the parameters $(0, 1/5, 2/5, 3/5, 4/5)$ of f_0 and the parameters $(1/3, 2/3)/6 + j/6$, with $j = 0, 1, 2, 3, 4, 5$, with the latter parameters repeated m times since $x^{12} + x^6 + 1$ occurs with the exponent m. The parameters of g can be worked out similarly.

1.1. Description of the proof

We first show that when $P = Q = 1$, the monodromy group is an arithmetic subgroup of $O(2, 3)$. This is proved by showing that the reflection subgroup generated by the elements $A^k C A^{-k}$ ($k \in \mathbb{Z}$) is arithmetic. We prove the arithmeticity of the reflection group Δ by explicit computation, by showing that Δ contains an arithmetic subgroup of the unipotent radical of a parabolic subgroup. The arithmeticity then follows by appealing to a generalization of a theorem of Tits on unipotent generators of arithmetic groups (see Theorem 7).

We then prove the general case by using Proposition 6 below. The proposition says the following: if Γ is a Zariski dense subgroup of $O(h)(\mathbb{Z})$, where h is a non-degenerate quadratic form over $\mathbb{Q}$, such that Γ contains a finite index subgroup of $O(W)(\mathbb{Z})$ for some 5-dimensional W with $\mathbb{Q}$-rank$(W) = 2$, then Γ is itself an arithmetic group.

In Section 5, we list the pairs f_1, g_1 (up to a scalar shift, i.e. changing $f(x) \mapsto f_1(-x)$ and $g_1(x) \mapsto g_1(-x)$—see [2] and [6]) of degree 5 satisfying $f_1(0) = -1$, $g_1(0) = 1$ such that the hypergeometric group $\Gamma(f_1, g_1)$ is arithmetic. Two of the groups G have $\mathbb{Q}$-rank one, while the rest have $\mathbb{Q}$-rank two. The proof of arithmeticity in these cases is similar to that for the group Δ considered above.

The authors of [6] also give a list of hypergeometric $O(2, 1)$'s and they prove that in each case the group is arithmetic. An earlier version of the present paper used these computations in [6] to put together various arithmetic $O(2, 1)$'s to deduce arithmeticity; however, this method does not cover as many cases as the present one, and in addition the present proof is more uniform.

2. Preliminary results

2.1. The quadratic form h

Notation. We will view the quadratic vector space V as the $\mathbb{Q}$-algebra $V = \mathbb{Q}[x]/(f(x))$ and the operator A as multiplication by x; then with respect to the basis $1, x, \ldots, x^{n-1}$, the matrix of A is the companion matrix of f. Write $V_{\mathbb{Z}} = \mathbb{Z}[x]/(f(x)) \subset V$. We assume that $f \in \mathbb{Z}[x]$ is a product of cyclotomic polynomials with $f(0) = -1$.

Let $g \in \mathbb{Z}[x]$ be a product of cyclotomic polynomials with $g(0) = 1$. Assume f, g have no common root. We introduce the operator B on V by setting $B(w) = A(w) = w$ if $w = 1, x, \ldots, x^{n-2}$ and $B(x^{n-1}) = x^n - g(x)$; the latter being a polynomial of degree at most $n-1$, it can be viewed as an element of $V_{\mathbb{Z}}$. Denote by $\Gamma = \Gamma(f, g)$ the group generated by the two matrices A, B. Following [2], we say that f, g form an *imprimitive pair* if the the vector space V splits into a direct sum of subspaces V_i such that each element of the group Γ permutes these spaces V_i; if not, we say that f, g form a *primitive pair*. We assume henceforth that f, g form a primitive pair.

Let h be the quadratic form preserved by A, B; by [2], such a form exists and is unique up to scalar multiples. To ease the notation, we write $x.y = h(x, y)$ for $x, y \in V$.

The following observations are taken from [6, Section 2.4]. Since A and B coincide on the span of the first $n-1$ basis elements $1, x, \ldots, x^{n-2}$, it follows that if $C = A^{-1}B$, then C is the identity on $1, x, \ldots, x^{n-2}$ and the image of $C - 1$ is one-dimensional. Moreover, $(C-1)(V_{\mathbb{Z}})$ is of the form $\mathbb{Z}v$ for some $v \in V_{\mathbb{Z}}$. Therefore, $(C-1)(x^{n-1}) = v$. Since the determinant of C is -1, we have $C^2 - 1 = 0$; it follows that $Cv = -v$. Consequently, v is orthogonal to $1, x, \ldots, x^{n-2}$. Hence $x^{n-1}.v \neq 0$. We normalise h so that $x^{n-1}.v = 1$. Therefore, for any vector $w = u_0 + u_1 x + \cdots + u_{n-1}x^{n-1} \in V$ ($u_i \in \mathbb{Q}$), we have $w.v = u_{n-1}$. Denote by λ the linear form $w \mapsto u_{n-1}$.

It follows that $Av = A(C-1)(x^{n-1}) = (B-A)(x^{n-1}) = g - f$, where the latter is viewed as a linear combination of $1, x, \ldots, x^{n-1}$, i.e. an element of $V_{\mathbb{Z}}$; since f, g are monic of degree n, $f - g$ is a polynomial of degree not exceeding $n-1$ and there is no abuse of notation.

Lemma 2 (see [6, Proposition 2.10]). *Under the preceding notation and normalisation of h, we have the formulae*

$$v.w = u_{n-1} \quad \forall w \in V, \qquad v.v = 2, \qquad C(w) = w - (w.v)v \quad \forall w \in V.$$

Proof. The first part is already proved (see the second paragraph preceding the lemma); so we need only prove the second and the third equalities. Note that (by the first formula) the orthogonal complement to v is exactly the span of $1, x, \ldots, x^{n-2}$. We have also seen that $Av = g - f = c_{n-1}x^{n-1} + \cdots + c_1 x + 2$ where $c_i = b_i - a_i$. The operator on V given by multiplication by x is invertible. The equation

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x - 1 \equiv 0 \in V$$

shows that *in* V,

$$\frac{1}{x} \equiv x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2 x + a_1,$$

and that

$$\frac{1}{x}(x^k) = x^{k-1} \quad \text{whenever} \quad 1 \leq k \leq n-1.$$

Therefore,

$$\begin{aligned} v &= \frac{1}{x}(Av) = \frac{1}{x}(c_{n-1}x^{n-1} + \cdots + c_1 x + 2) \\ &= c_{n-1}x^{n-2} + \cdots + c_2 x + c_1 + 2(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1). \end{aligned}$$

The last equality shows that the coefficient of x^{n-1} in v (viewed as a linear combination of $1, x, \ldots, x^{n-1}$) is exactly two. Therefore $v.v = 2$.

The operator C is the identity on $1, x, \ldots, x^{n-2}$ and is -1 on v. The operator $w \mapsto w - (w.v)v$ is also the identity on $1, x, \ldots, x^{n-2}$ since v is orthogonal to $1, x, \ldots, x^{n-2}$; moreover, $v - (v.v)v = -v$; therefore, the third equality in the lemma follows. □

Remark 3. Since g and f are coprime, the element $Av = g - f$, viewed as an element of the algebra $V = \mathbb{Q}[x]/(f(x))$, is invertible. Hence Av is cyclic for the action of A, and hence so is v. Thus, $v, Av, \ldots, A^{n-1}v$ form a basis of the vector space V. In particular, the inner products $A^i v.A^j v$ determine the quadratic form h; the invariance of h under A implies that h is determined by the inner products $A^i v.v$ $(0 \le i \le n-1)$. By Lemma 2 the latter is just the coefficient of x^{n-1} in $A^i v$, viewed as a linear combination of $1, x, \ldots, x^{n-1}$. Hence h is determined by the "highest coefficients" of the remainders of the polynomials $g - f, x(g - f), \ldots, x^{n-1}(g - f)$ after division by f.

Lemma 3. *Suppose* two *of the roots of f (or of g) occur with multiplicity two (i.e. suppose f is divisible by the square of a quadratic polynomial). Then* $\mathbb{R}$-rank$(V) \ge 2$. *If $n \ge 7$, then* $\mathbb{Q}$-rank$(V) \ge 2$.

Proof. Write

$$f(x) = \prod_{j=1}^{n}(x - e^{2\pi i \alpha_j}), \quad g(x) = \prod_{j=1}^{n}(x - e^{2\pi i \beta_j}).$$

We assume, as we may, that

$$0 \le \alpha_1 \le \cdots \le \alpha_n < 1 \quad \text{and} \quad 0 \le \beta_1 \le \cdots \le \beta_n < 1.$$

If (p, q) is the signature of the quadratic form, then the real rank is $\frac{1}{2}(p + q - |p - q|)$. There is a formula ([2] or [6]) for $|p - q|$:

$$|p - q| = \Big|\sum_{j=1}^{n}(-1)^{j+m_j}\Big|$$

where m_j is the number of indices k such that $\beta_k < \alpha_j$ (here $\beta_1, \ldots, \beta_n$ are the parameters of g). The numbers α_j, β_k lie in the closed-open interval $[0, 1)$.

If f has one root with multiplicity one, i.e. for some index j we have $\alpha_j = \alpha_{j+1}$, then $m_j = m_{j+1}$ $(= m$, say). Hence

$$(-1)^{j+m_j} + (-1)^{j+1+m_{j+1}} = (-1)^{j+m} + (-1)^{j+1+m} = 0.$$

Hence two terms in the above expression for $|p - q|$ cancel out and $|p - q| \le p + q - 2$.

Similarly, if there are *two* roots with multiplicity two, then $|p-q| \leq p+q-4$. Hence

$$\mathbb{R}\text{-rank}(V) = \frac{1}{2}(p+q-|p-q|) \geq \frac{1}{2} \cdot 4 = 2.$$

The second part of the lemma is an easy consequence of the Hasse–Minkowski theorem: if a rational quadratic form in at least five variables represents a real zero, then it represents a rational zero. □

2.2. *The quadratic forms h and h_0*

Notation. We now consider $f_0 = x^5 - 1$ and $g_0 = (x+1)(x^2+1)^2$; they form a primitive pair by [2]. Denote the associated monodromy group by $\Delta = \Gamma(f_0, g_0)$ generated by the companion matrices A_0, B_0 of f_0, g_0 respectively; it is a subgroup of $\mathrm{GL}_5(\mathbb{Z})$ and preserves a non-degenerate quadratic form h_0 on $V_0 = \mathbb{Q}^5 = \mathbb{Q}[x]/(f_0(x))$. We have the vector $v_0 \in V_0$ as before (we have denoted the vector v of the previous subsection in this case ($n = 5$) by v_0). We view elements w of V_0 as polynomials of degree ≤ 4: $w = u_4x^4 + u_3x^3 + u_2x^2 + u_1x + u_0$ with $u_i \in \mathbb{Q}$. Denote by λ_0 the linear form $w \mapsto u_4$. It is easily seen that V_0 is spanned by the vectors $v_0, A_0v_0, A_0^2v_0, A_0^3v_0, A_0^4v_0$.

Fix an integer $m \geq 0$ and set $n = 6m + 5$. Let $P, Q \in \mathbb{Z}[x]$ be two (monic) polynomials of degree m, which are products of cyclotomic polynomials such that $P(0) = Q(0) = 1$. Consider the polynomials $f(x) = f_0(x)P(x^6)$ and $g(x) = g_0(x)Q(X^6)$. Then f, g have degree $n = 6m + 5$. We assume that f, g are coprime and that (f, g) form a primitive pair. Let $\Gamma = \Gamma(f, g)$ be the hypergeometric group. We have the vector v in $V = \mathbb{Q}[x]/(f(x))$. Denote by W the span of the vectors v, Av, A^2, A^3v, A^4v. We have an injective linear map $i : V_0 \to V$ given on the basis elements $\{A_0^kv_0 : 0 \leq k \leq 4\}$ by the formula $A_0^kv_0 \mapsto A^kv$.

We first prove an easy preliminary lemma.

Lemma 4. *If $k \leq 4$, then the coefficient of x^{n-1} in the remainder $R(x)$ of $x^k(f-g)$ upon division by f is the same as the coefficient of x^4 in the remainder $R_0(x)$ of $x^k(f_0 - g_0)$ upon division by f_0.*

Proof. We may write $R_0(x) = x^k(f_0 - g_0) + q_0(x)f_0(x)$ for some q_0, and $R(x) = x^k(f - g) + q(x)f(x)$ for some q. Consider the equation

$$x^k(f-g) = x^k(f_0P(x^6) - g_0Q(x^6)) = x^k(f_0 - g_0)P(x^6) + x^kg_0(P(x^6) - Q(x^6)).$$

Since P, Q are monic of degree m in x, the degree of $P(x^6) - Q(x^6)$ is at most $6m - 6$. Therefore, the degree of $x^k(P(x^6) - Q(x^6))$ is at most $6m - 2$, and hence does not contribute to the $x^{n-1} = x^{6m+4}$ term.

The polynomial $x^k(f_0 - g_0)P(x^6)$ may be written as $R_0(x)P(x^6) + q_0(x)f_0(x)P(x^6)$; since $f = f_0P(x^6)$, it follows that $R = R_0P(x^6)$. Hence the coefficient of x^{4+6m} in $R(x)$ is the coefficient of x^4 in $R_0(x)$. The lemma follows. □

Lemma 5. *The above linear map i is an isometry of the quadratic spaces (V_0, h_0) and $(W, h_{|W})$. In particular, the restriction $h_{|W}$ is non-degenerate. Write the orthogonal decomposition $V = W \oplus W^{\perp}$. The group generated by the reflections $A_0^r C_0 A_0^{-r}$, $0 \leq r \leq 4$, is isomorphic to the group Δ generated by the reflections $A^r C A^{-r}$, $0 \leq r \leq 4$. Moreover, Δ acts trivially on $W^{\perp}$.*

Proof. Since the map i is linear, to check isometry, we need only check that the inner products $h(A^k v, A^l v)$ and $h_0(A_0^k v_0, A_0^l v_0)$ coincide for $0 \leq k, l \leq 4$. Using the invariance of h, h_0 under A, A_0 it is sufficient to check that $h(v, A^k v)$ and $h_0(v_0, A_0^k v_0)$ coincide. But $h(v, A^k v)$ is none other than the coefficient of x^{n-1} in the vector $A^k A v = x^k(f - g)$ viewed as a linear combination of $1, x, \ldots, x^{n-1}$; similarly, $h_0(v_0, A_0^k v_0)$ is the coefficient of x^4 in the vector $A_0^k A_0 v_0 = x^k(f_0 - g_0)$ viewed as a linear combination of $1, x, x^2, x^3, x^4$.

By Lemma 4, the coefficient of x^{n-1} in $x^k(f - g)$ is the same as the coefficient of x^4 in $x^k(f_0 - g_0)$. Therefore the lemma follows. □

3. A bootstrapping step for integral orthogonal groups

In this section, we prove a result which will be used in the proof of Theorem 1. The result says that a subgroup of the integral unitary group has finite index if it contains finite index subgroups of smaller integral unitary groups.

Let h be a non-degenerate rational quadratic form on an n-dimensional $\mathbb{Q}$-vector space V. Suppose that $W \subset V$ is a 5-dimensional subspace on which the restriction of h is non-degenerate and such that if $V = W \oplus W^{\perp}$ is the orthogonal decomposition, then $O(W)$ may be viewed as the subgroup of V which fixes $W^{\perp}$ pointwise. Assume that $V_{\mathbb{Z}} \subset V$ is a lattice on which h takes integral values. Denote by $O(V, \mathbb{Z})$ the integer points of $O(V)$; define $O(W, \mathbb{Z})$ similarly.

Proposition 6. *If Γ is a Zariski dense subgroup of $SO(V, \mathbb{Z})$ whose intersection with $SO(W, \mathbb{Z})$ has finite index in $SO(W, \mathbb{Z})$, then Γ has finite index in $SO(V, \mathbb{Z})$ provided* $\mathbb{Q}$-rank$(W) = 2$

3.1. *Unipotent generators for arithmetic groups*

The following theorem (see [8], [13]) is an extension to all simple groups, and all opposing parabolic subgroups, of a result of Tits (the result of Tits [11] was proved for Chevalley groups of K-rank at least two).

Theorem 7. *Suppose G is an absolutely almost simple linear algebraic group defined over a number field K such that the K-rank of G is ≥ 1 and $G(O_K)$ has higher real rank, i.e.*

$$\infty\text{-rank}(G) := \sum_{v|\infty} K_v\text{-rank}(G) \geq 2.$$

Suppose P is a parabolic K-subgroup of G with unipotent radical U and let P^- be a parabolic K-subgroup defined over K and opposed to P with unipotent radical U^-. Let $\Gamma \subset G(O_K)$ be a subgroup which intersects $U(O_K)$ in a finite index subgroup (and similarly with $U^-(O_K)$). Then Γ has finite index in $G(O_K)$.

3.2. Algebraic groups

The reference for the material in this subsection is [3].

Notation. Let G be a $\mathbb{Q}$-simple linear algebraic group defined and isotropic over $\mathbb{Q}$. Fix a maximal split torus S and a minimal parabolic subgroup P_0 containing S. Under the adjoint action of S, the Lie algebras $\mathfrak{p}_0$ and $\mathfrak{g}$ of P_0 and G decompose as follows (Φ^+ is the system of positive roots, i.e. those roots occurring in $\mathfrak{p}_0$, and Φ is the system of all roots):

$$\mathfrak{p}_0 = \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in \Phi^+} \mathfrak{g}_\alpha, \qquad \mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in \Phi^+} \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}.$$

Given a root α denote by U_α the unipotent algebraic subgroup generated by the elements of the form $\exp(X)$ for all $m \geq 1$ and all $X \in \mathfrak{g}_{m\alpha}$. Given $X \in \mathfrak{g}_\alpha(\mathbb{Q})$ we get a one-parameter unipotent group $t \mapsto X_\alpha(t) : \mathbb{G}_\mathrm{a} \to U_\alpha$.

Suppose that α, β are two roots which are not rational multiples of each other. Then necessarily $\mathbb{Q}$-rank$(G) \geq 2$.

Before stating the next lemma, we fix some notation. Let X be a finite totally ordered indexing set and G a group. Let $g_x \in G$ for each index $x \in X$. We let

$$P = \prod_{x \in X} g_x,$$

where the product is taken in such a way that if $x < x'$ in X then g_x appears to the left of $g_{x'}$. Moreover, $[x, y]$ denotes the commutator element $xyx^{-1}y^{-1}$ in G.

We have the Chevalley commutator relations:

Lemma 8. *Suppose that G is a Chevalley group. For any integers $m, n \geq 1$ such that $m\alpha + n\beta$ is a root, there exist one-parameter unipotent groups $X_{m\alpha+n\beta}$ such that for all $s, t \in \mathbb{G}_\mathrm{a}$ we have the commutator relation*

$$[X_\alpha(s), X_\beta(t)] = \prod_{m,n} X_{m\alpha+n\beta}(s^m t^n),$$

where the product is of elements of the group G, and the roots $\theta_{m,n} = m\alpha + n\beta$ are arranged in some arbitrary but fixed order (so that if $m + n < m' + n'$ then $\theta_{m,n}$ appears before, i.e. to the left of, $\theta_{m',n'}$ in the product).

Lemma 9. *Let G be a Chevalley group. Fix an integer $N \geq 1$ and consider the group U_N generated by the commutators*

$$[X_\alpha(s), X_\beta(t)], \qquad s, t \equiv 0 \ (\mathrm{mod}\ N),$$

in $G(\mathbb{Z})$. Then there exists an integer $M \geq 1$ such that for **each** *$m, n \geq 1$ the group U_N contains the subgroup $X_{m\alpha+n\beta}(x)$ for $x \equiv 0$ (mod M).*

Proof. The Zariski closure U_0 of the group U_N of integral matrices is a unipotent group: in view of the commutator relations, the root groups $U_{m\alpha+n\beta}$, $m,n \geq 1$, generate a unipotent group, say U^*. Now a Zariski dense subgroup of $U_0(\mathbb{Z})$ has finite index in $U_0(\mathbb{Z})$ (see [7]). Hence we need only prove that the one-parameter groups $X_{m,n}$ lie in U_0 ($X_{m,n}$ denotes the group $X_{m\alpha+n\beta}$). Denote by $\mathfrak{u}_0$ and $\mathfrak{u}^*$ the Lie algebras of U_0 and of U^*. Denote by log the inverse of the exponential map from U^* onto $\mathfrak{u}^*$.

Taking the logs of the commutators in the commutator relations, we find that a polynomial P in t,s, namely

$$P(t,s) = \log\Big(\prod_{m,n} X_{m,n}(t^m s^n)\Big),$$

takes values in the subspace $\mathfrak{u}_0$; hence the coefficient of ts also does. This coefficient is precisely $\log(X_{1,1})$; hence the first element $X_{1,1}$ in the ordering lies in U_0; now an easy induction on the ordering implies that all the $X_{m,n}$ lie in U_0 (to ease the notation, we have denoted by $X_{m,n}$ the image of the one-parameter group $X_{m,n}$ in U^*). □

3.3. The special case of $O(2,3)$

We now assume that h_0 is a non-degenerate quadratic form on a 5-dimensional $\mathbb{Q}$-vector space W with $\mathbb{Q}$-rank$(W) = 2$. Denote by $w.w'$ the element $h_0(w,w')$. The rank assumption implies that there exists a basis $\varepsilon_1, \varepsilon_2, w_3, \varepsilon_2^*, \varepsilon_1^*$ of W such that $\varepsilon_1^2 = \varepsilon_2^2 = 0$, $(\varepsilon_2^*)^2 = (\varepsilon_1^*)^2 = 0$, $w_3^3 \neq 0$, $\varepsilon_i.w_3 = \varepsilon_i^*.w_3 = 0$ for $i = 1,2$ and $\varepsilon_i(\varepsilon_j^*) = \delta_{ij}$ (the Kronecker delta). With respect to this basis, $O(W)$ may be thought of as a subgroup of the group GL_5 of 5×5 matrices. We will informally denote $O(W)$ by $O(2,3)$.

The intersection of the diagonals with $H = O(W)$ is a 2-dimensional split group $S = \{(t_1,t_2) \in \mathbb{G}_m^2\}$ which acts by the characters t_i on ε_i , t_i^{-1} on ε_i^* and trivially on w_3. Denote by $\mathfrak{h}_{\pm x_i}$ (resp. $\mathfrak{h}_{\pm(x_1+x_2)}$) the subspace of the Lie algebra $\mathfrak{h}$ of $O(W)$ on which S acts by the character $t_i^{\pm 1}$ (resp. $(t_1t_2)^{\pm 1}$).

As a special case of Lemma 9, we have

Lemma 10. *In the notation of the preceding subsection, for any integer $N \geq 1$, the group generated by the commutators*

$$[X_{-x_1}(s), X_{x_1+x_2}(t)], \qquad s,t \equiv 0 \ (\mathrm{mod}\ N),$$

contains the group $X_{x_2}(M\mathbb{Z})$, which is the subgroup of $X_{x_2}(\mathbb{Z})$ of elements congruent to the identity modulo M.

Proof. We need only note that $x_2 = 1(x_1+x_2) + 1(-x_1)$ and apply Lemma 9 to the roots $\alpha = x_1 + x_2$ and $\beta = x_1$. □

3.4. The group $O(V)$

Since the $\mathbb{Q}$-rank of W is two, the $\mathbb{Q}$-rank r of V is at least two. There exists a basis $\varepsilon_1, \ldots, \varepsilon_r, v_1, \ldots, v_m, \varepsilon_r^*, \varepsilon_{r-1}^*, \ldots, \varepsilon_1^*$ of V ($\dim(V) = n = 2r + m$) such that (1) $\varepsilon_j.\varepsilon_j^* = \delta_{ij}$ and (2) W is the span of $\varepsilon_1, \varepsilon_2, \varepsilon_1^*, \varepsilon_2^*$ and an element w_3 which is a linear combination of the vectors v_j and the vectors $\varepsilon_3, \ldots, \varepsilon_r, \varepsilon_r^*, \ldots, \varepsilon_3^*$. Under the inclusion $O(W) \subset O(V) \subset \mathrm{GL}_n$, the torus S is the subgroup of diagonal matrices in GL_n which act by the characters t_1, t_2 on $\varepsilon_1, \varepsilon_2$, by $t_1^{-1}t_2^{-1}$ on $\varepsilon_1^*, \varepsilon_2^*$, and by the trivial character on all the other basis elements above.

Let X be the span of $\varepsilon_1, \varepsilon_2$, and Y the span of the basis vectors $\varepsilon_3, \ldots, \varepsilon_r, v_1, \ldots, v_m, \varepsilon_r^*, \ldots, \varepsilon_3^*$. Let L be the subgroup of $O(V)$ which stabilises the spaces X and Y; let P be the subgroup which stabilises the partial flag $X \subset X^\perp = X \oplus Y \subset V$, and U the subgroup of P which acts trivially on successive quotients of this flag. Since X is totally isotropic, P is a parabolic subgroup and U its unipotent radical. L is a Levi subgroup of P containing the torus S and we have $P = LU$. It is easy to see that $L = \mathrm{GL}_2 .O(Y)$ where $S \subset \mathrm{GL}_2$ and GL_2 is the subgroup of L which acts trivially on Y.

With respect to the adjoint action of S, the Lie algebra of U splits into the character spaces $\mathfrak{g}_{x_1}$, $\mathfrak{g}_{x_2}$ and $\mathfrak{g}_{x_1+x_2}$; it is easy to see that $\mathfrak{g}_{x_1+x_2}$ is one-dimensional and equals $\mathfrak{h}_{x_1+x_2}$. Moreover, the action of $L = \mathrm{GL}_2 .O(Y)$ on the direct sum $\mathfrak{g}_{x_1} \oplus \mathfrak{g}_{x_2}$ is simply the exterior tensor product $\mathrm{St} \otimes \mathrm{St}$ of the standard representations of GL_2 and $O(Y)$ (and in particular, is irreducible for the action of L). We note that $\mathfrak{h} \cap \mathfrak{g}_{x_1} \neq \{0\}$.

Lemma 11. *For any $u \in U$ and any $v \in U$, we have $uvu^{-1} = v.u'$ where $u' \in X_{x_1+x_2}$. Moreover, given an integer N, there exists a power v^M of v such that $uv^Mu^{-1}v^{-M}$ lies in $X_{x_1+x_2}(N\mathbb{Z})$.*

Proof. The first part is just a restatement of the fact that $\mathfrak{u}/\mathfrak{g}_{x_1+x_2}$ is abelian. The second part is an easy consequence. □

3.5. Proof of Proposition 6

Let $\mathcal{U}$ denote the open Bruhat cell Pw_0U where w_0 is the longest Weyl group element. Since Γ is Zariski dense in $G = O(V)$, it follows that $\Gamma \cap \mathcal{U}$ is also Zariski dense in G. Given $\gamma \in \Gamma \cap \mathcal{U} \subset Pw_0U$ write $\gamma = pw_0u$ accordingly. Then the elements p (as Γ varies) form a Zariski dense subset of P. We fix a finite set F of elements of $\Gamma \cap \mathcal{U}$ such that the span of the conjugates $p(\mathfrak{h})_{x_2}p^{-1}$ contains all of $\mathfrak{g}_{x_1} \oplus \mathfrak{g}_{x_2}$; it is possible to find such a finite set since P acts irreducibly on $\mathfrak{u}/\mathfrak{g}_{x_1+x_2}$ and the P parts p of elements of $\Gamma \cap \mathcal{U}$ are Zariski dense in P (since $\Gamma \cap \mathcal{U}$ is Zariski dense in G).

Since Γ contains a finite index subgroup of $H(\mathbb{Z})$, it contains the congruence group $(U \cap H)(N\mathbb{Z})$ for some integer N. In particular, there exists an element $v \in (U \cap H_{x_2})(M\mathbb{Z})$ with the integer M large such that for all γ in F, the finite set of the previous paragraph, the elements $uvu^{-1}v^{-1}$ lie in $U_{x_1+x_2}(N\mathbb{Z}) \subset \Gamma$. Consider the commutator set

$$E = [{}^{\gamma}(vX_{x_1+x_2}(M\mathbb{Z})), X_{x_1+x_2}(M\mathbb{Z})]$$

(in a group, we denote ${}^{x}(y) = xyx^{-1}$). Since $\gamma = pw_0u$, it follows from Lemma 11 that this set contains the commutator set

$$[{}^{pw_0}(v), X_{x_1+x_2}(M\mathbb{Z})].$$

We note that for a large enough M, the conjugate ${}^{p^{-1}}(X_{x_1+x_2}(M\mathbb{Z}))$ lies in $X_{x_1+x_2}(N\mathbb{Z})$. Therefore, E contains the commutator set

$$^{p}([^{w_0}(v), X_{x_1+x_2}(N\mathbb{Z})]).$$

Since $v \in X_{x_2}$, it follows that $^{w_0}(v)$ lies in $X_{-x_2}(N\mathbb{Z})$. It follows from Lemma 10 that the group generated by the latter commutators contains $X_{x_2}(M\mathbb{Z})$ for some integer M divisible by large powers of N and by the denominators of the rational matrix p . Since the p-conjugates of $X_{x_1}(M\mathbb{Z})$ generate (modulo centre) all of $\mathfrak{g}_{x_1} \oplus \mathfrak{g}_{x_2}$ in the Lie algebra of the Zariski closure, it follows that the group generated by the p-conjugates of our commutator set contains $U_{x_1}(M\mathbb{Z})$ and $U_{x_2}(M\mathbb{Z})$, where $p = p(\gamma)$ and γ runs through a (possibly large) finite set in $\Gamma \cap \mathcal{U}$. These generate a finite index subgroup of $U(\mathbb{Z})$. Therefore, Γ contains a finite index subgroup of $U(\mathbb{Z})$.

Now U is the unipotent radical of the parabolic subgroup P, and G has real rank (even rational rank) at least two. By Theorem 7, it follows that Γ is arithmetic.

4. The arithmeticity of Γ

4.1. Arithmeticity of Δ

In this subsection, we prove that the group $\Delta = \Gamma(f_0, g_0)$ is an arithmetic subgroup of $O(W, h_0)$ and that $\mathbb{Q}$-rank$(W) = 2$. To ease the notation, we drop the subscript in v_0, A_0 and simply write v, A etc.

Lemma 12. *We have*

$$v.v = 2, \qquad Av.v = 1, \qquad A^2v.v = 2, \qquad A^3v.v = 2, \qquad A^4v.v = 1.$$

The vector $\varepsilon = v - A^2v$ is isotropic and the orthogonal complement $\varepsilon^{\perp}$ is the span of the four vectors $\varepsilon, v, Av, v' = A^3v + A^4v - v$. Moreover, the reflections about the three vectors $v, Av, v' = A^3v + A^4v - v$ lie in Γ and fix ε.

Proof. We view V as the space of polynomials of degree ≤ 4. We need only compute the coefficient of x^4 in the vectors v, Av, A^2v, A^3v, A^4v. Since $Av = g - f$ and $g = (x+1)(x^2+1)^2$, $f = x^5 - 1$, we have $Av = x^4 + 2x^3 + 2x^2 + x + 2$. Hence the coefficient of x^4 in Av is 1. Moreover, $A^2v = x^5 + 2x^4 + 2x^3 + x^2 + 2x = 2x^4 + 2x^3 + x^2 + 2x + 1$ (since $x^5 - 1 \equiv 0$ in V). Therefore, the coefficient of x^4 in A^2v is 2. The others are proved similarly.

The second part follows immediately from the first: as an illustration, we compute

$$\varepsilon.v = A^2v.v - v.v = 2 - 2 = 0,$$
$$\varepsilon.A^2v = A^2v.A^2v - v.A^2v = v.v - A^2v.v = 2 - 2 = 0.$$

Note that we have used the invariance of the “dot product” under the action of A, B. The other relations are proved similarly.

We denote by $\Delta(\varepsilon)$ the subgroup of Δ which fixes the line through ε. It is the intersection of Δ with the parabolic subgroup $P = P(\varepsilon)$ of G which fixes the isotropic vector ε. Since the vectors v, Av, v' are in the orthogonal complement of ε, it follows that the reflections $C_v, C_{Av}, C_{v'}$ about the vectors v, Av, v' fix the vector ε, and in particular lie in P. Since the reflections about v and Av are the elements C and ACA^{-1}, it follows that $C = C_v$ and $C_{Av} = ACA^{-1}$ lie in $\Delta(\varepsilon)$, since Δ is the group generated by A, C. We need only prove that $C_{v'}$ lies in Δ.

It is easy to show that ${}^{C_w}(C_{w'}) = C_{w'-(w'.w)w}$ for vectors $w \in V$ with $w.w = 2$. We use this observation and the formulae for the dot product in the preceding lemma to compute

$$^{C_{A^3v}C_v}(C_{A^4v}) = {}^{C_{A^3v}}(C_{A^4v-v}) = C_{A^4v-A^3v-v+2A^3v} = C_{v'}.$$

The leftmost term of the above equalities lies in Δ since each of the reflections about v, A^3v, A^4v does. Therefore, $C_{v'}$ lies in Δ. □

Notation. The element ε of Lemma 12 is isotropic. Hence we have the partial flag $\mathbb{Q}\varepsilon \subset \varepsilon^{\perp} \subset V$. The subgroup of $O(V)$ which preserves this flag is a parabolic subgroup P, and the subgroup which preserves this flag and acts trivially on successive quotients is its unipotent radical U. Consider the elements C_{A^2v} and C_v. They fix ε by Lemma 12. If $w \in V$, then $C_{A^2v}(w) = w - (w.A^2v)Av$ and $C_v(w) = w - (w.v)v$ since $A^2v.A^2v = v.v = 2$. Moreover, if $w \in \varepsilon^{\perp}$, then $w.(A^2v - v) = 0$, i.e.

$$\begin{aligned} C_{A^2v}C_v(w) &= C_{A^2v}(w - (w.v)v) = w - (w.A^2v)A^2v - (w.v)v + (w.v)(A^2v.v)A^2v \\ &= w - (w.v)A^2v - (w.v)v + 2(w.v)A^2v = w + (w.v)(A^2v - v), \end{aligned}$$

since $A^2v.v = 2$ (Lemma 12). That is,

$$C_{A^2v}C_v(w) = w + (w.v)(A^2v - v) = w + (w.v)\varepsilon \quad \forall w \in \varepsilon^{\perp}.$$

In particular, $u = C_{A^2v}C_v$ is a non-trivial element of $O(\varepsilon^{\perp})$ since its value on v is $v + 2(A^2v - v) \neq v$. Moreover, the formula $u = C_{A^2v}C_v$ shows that on the quotient $\varepsilon^{\perp}/\mathbb{Q}\varepsilon$, the action of u is trivial; thus we have one non-trivial unipotent element u in $\Delta \cap U$.

Lemma 13. *The intersection of the group $\Delta(\varepsilon)$ with U has finite index in $U(\mathbb{Z})$.*

Proof. The quotient of the group $P = P(\varepsilon)$ by its unipotent radical is the orthogonal group $L = O(\varepsilon^{\perp}/\mathbb{Q}\varepsilon)$. By Lemma 12, the image of $\Delta(\varepsilon)$ in the quotient L contains the reflections about the basis elements v, A^2v, $v' = A^3v + A^4v - v$. Moreover, these basis elements are mutually non-orthogonal. Hence the group generated by these three reflections acts irreducibly on the standard representation $\mathbb{Q}^3$ of L. However, the conjugation action of L on U is clearly the standard representation of L. Moreover, by the paragraph preceding this lemma, $U \cap \Delta(\varepsilon)$ contains the non-trivial element u; hence the conjugates of u by these three reflections span $U(\mathbb{Q}) = \mathbb{Q}^3$. That is, $U \cap \Delta(\varepsilon)$ contains a spanning set of $\mathbb{Q}^3$. Hence $U \cap \Delta(\varepsilon)$ contains a finite index subgroup of $\mathbb{Z}^3$. □

Proposition 14. *If* $f_0 = x^5 - 1$ *and* $g_0 = (x+1)(x^2+1)^2$, *then the hypergeometric monodromy group* $\Delta = \Gamma(f_0, g_0)$ *is an arithmetic subgroup of* (V_0, h_0). *Moreover,* $\mathbb{Q}$-rank$(V_0) = 2$.

Proof. Consider the vector $\varepsilon' = A^3v + A^4v - Av$. By Lemma 12, ε' lies in $\varepsilon^{\perp}$. We compute the dot product of ε' with itself (we write w^2 for $w.w$):

$$\varepsilon'.\varepsilon' = (A^2v + A^3v - v)^2 = 2 + 2 + 2 + 2A^2v.A^3v - 2A^2v.v - 2A^3v.v.$$

By the formulae for the dot product in Lemma 12, this is $6 + 2v.Av - 2.2 - 2.2 = 6 + 2 - 4 - 4 = 0$. Thus $\varepsilon, \varepsilon'$ are linearly independent mutually orthogonal isotropic vectors. Hence $\mathbb{Q}$-rank$(V_0) \geq 2$. Since $h = h_0$ is non-degenerate [2] and is a quadratic form in five variables, it follows that $\mathbb{Q}$-rank$(V) = 2$.

By Lemma 13, the intersection $\Delta \cap U$ has finite index in $U(\mathbb{Z})$ and U is the unipotent radical of a parabolic $\mathbb{Q}$-subgroup of $H = O(V_0, h_0)$. By [2], the monodromy group Δ is Zariski dense in H. By the preceding paragraph, the $\mathbb{Q}$-rank of H is at least two. Therefore, by Theorem 7, Δ is an arithmetic subgroup of $H(\mathbb{Z})$. □

4.2. *Proof of the main theorem*

We now return to the situation of Lemma 5. We have the space V_0 which is 5-dimensional and V which has dimension $n = 6m + 5$. We also have an isometry $i : V_0 \to W \subset V$ where W is the image of i and is the span of v, Av, A^2v, A^3v, A^4v. The space W is non-degenerate since V_0 is. Hence we have the orthogonal decomposition $V = W \oplus W^{\perp}$. We may view $O(W)$ as a subgroup of $O(V)$ which leaves W invariant and acts trivially on $W^{\perp}$. The reflections with respect to the vectors $\{A^kv : 0 \leq k \leq 4\}$ lie in $O(W)$ since they act trivially on $W^{\perp}$. By Proposition 14, these reflections generate an arithmetic subgroup of $O(W)$.

Now Γ is Zariski dense in $O(V)$ by [2]. By Proposition 6, and by the last sentence of the preceding paragraph, Γ is arithmetic.

5. Examples of arithmetic monodromy in $O(2,3)$

In this section, we list some more cases of hypergeometric monodromy when the underlying vector space is 5-dimensional, the group G has $\mathbb{R}$-rank two, and the monodromy group $\Gamma = \Gamma(f, g)$ is arithmetic. In some examples, the $\mathbb{Q}$-rank of G is one, and sometimes it is two.

5.1. *Generalities*

Suppose $f, g \in \mathbb{Z}[x]$ are monic of degree 5 and are a primitive hypergeometric pair. Assume that $f(0) = -1$ and $g(0) = 1$. Set $V = \mathbb{Q}[x]/(f(x))$; let v, Av be as before and normalise the inner product h so that $v.v = 2$.

Lemma 15. *Suppose there exists $g \in \Gamma$ such that $\varepsilon = g(v) \pm v \in V$ is isotropic, and orthogonal to $g(v)$ and v. Suppose that the quotient $\varepsilon^{\perp}/\mathbb{Q}\varepsilon$ is spanned by three vectors of the form $v, g_2(v), g_3(v)$, with $g_i \in \Gamma$. Suppose $v.g_i(v) \neq 0$ and $g_1(v).g_2(v) \neq 0$. Suppose $\mathbb{R}$-rank$(V) = 2$. Then Γ is arithmetic.*

Proof. We only work out the case $\varepsilon = g(v) - v$, the other case being similar. The isotropy of ε means that $g(v).v = 2$. Let $w \in \varepsilon^{\perp}$. Then $C_{g(v)}(w) = w - (w.g(v))g(v)$. Since $w.(g(v) - v) = 0$, it follows that $C_{g(v)}(w) = w - (w.v)g(v)$. Also $C_v(w) = w - (w.v)v$. Therefore $C_{g(v)}(w) - C_v(w) = (w.v)(g(v) - v) = (w.v)\varepsilon$. Hence $C_{g(v)}$ and C_v coincide on the quotient $Q = \varepsilon^{\perp}/\mathbb{Q}\varepsilon$, but are not equal: the value of their difference on v is just 2ε. Hence $\theta = C_v^{-1}C_{g(v)}$ lies in the unipotent radical U of the parabolic subgroup P which fixes ε.

The Levi part of this parabolic is $O(Q)$ where $Q = \varepsilon^{\perp}/\mathbb{Q}\varepsilon$. The group R generated by the reflections C_v, $C_{g_2(v)}$ and $C_{g_3(v)}$ acts irreducibly on $\mathbb{Q}^3$, since $g_i(v)$ and v generate Q and are assumed to be mutually non-orthogonal. The action of $O(Q)$ on U is just the standard representation, and $U \cap \Gamma$ is not the identity: it contains θ. The irreducibility of the action of R on $\mathbb{Q}^3$ implies that the conjugates by elements of R of θ generate a finite index subgroup of $U(\mathbb{Z})$.

Now, $\mathbb{R}$-rank$(G) = 2$ and Γ is Zariski dense in G by [2]. By the conclusion of the preceding paragraph, Γ contains a finite index subgroup of $U(\mathbb{Z})$. The arithmeticity of Γ follows from Theorem 7. □

Remark 4. The real rank of G was 2. The $\mathbb{Q}$-rank of G may be either 1 or 2 (by the Hasse–Minkowski theorem). The proof does not distinguish between these cases.

Example 1. Let

$$f = (x-1)(x^2+1)^2, \qquad g = (x+1)(x^2-x+1)^2.$$

We will show that the hypergeometric group Γ is arithmetic and that the $\mathbb{Q}$-rank of V is two. As before, we view $V = \mathbb{Q}^5$ as the algebra $\mathbb{Q}[x]/(f(x))$, and A as the operator which is multiplication by x. Thus $f \equiv 0$ in V, and hence

$$f(x) = x^5 - x^4 - 2x^3 + 2x^2 - x + 1 \equiv 0.$$

In other words,

$$x^5 = x^4 - 2x^3 + 2x^2 - x + 1.$$

We will view V as the space of polynomials of degree ≤ 4. We have

$$Av = g - f = -x^3 + 3x^2 - 2x + 2$$

and, after a normalisation, the quadratic form h is such that $v.v = 2$. Moreover, after fixing this normalisation for h, for any $w \in V$, $w.v$ is precisely the coefficient of x^4. Hence $Av.v = 0$.

We have $A^2v = x(Av) = -x^4 + 3x^3 - 2x^2 + 2x$ and $A^2v.v = -1$. Similarly,

$$\begin{aligned} A^3v &= -x^5 + 3x^4 - 2x^3 + 2x^2 \\ &= (-x^4 + 3x^3 - 2x^2 + x - 1) + 3x^4 - 2x^3 + 2x^2 = 2x^4 + x - 1. \end{aligned}$$

Hence $A^3v.v = 2$. Similarly, $A^4v = 2x^4 - 4x^3 + 5x^2 - 3x + 2$ and $A^4v.v = 2$. In particular, $\varepsilon = A^4v - v$ is isotropic. We now compute the orthogonal complement of ε. We have

$$\begin{aligned} \varepsilon.v &= A^4v.v - v.v = 0, \\ \varepsilon.Av &= A^4v.Av - v.Av = A^3v.v - Av.v = 2 - 0 = 2, \\ \varepsilon.A^3v &= A^4v.A^3v - v.A^3v = Av.v - A^3v.v = 0 - 2 = -2. \end{aligned}$$

Hence the orthogonal complement of ε is the span of ε, v, A^2v, $v' = Av + A^3v$. The square of $\varepsilon' = Av + A^3v - v$ is easily computed to be zero. Hence the span of ε and ε' is totally isotropic and the $\mathbb{Q}$-rank of V is two.

Secondly, the reflections C_v, C_{A^2v} lie in $\Gamma(\varepsilon)$. The reflection about $v' = Av + A^3v$ is computed to be

$${}^{C_{Av}}(C_{A^3v}) = C_{C_{Av}(A^3v)} = C_{A^3v-(Av.A^3v)Av} = C_{A^3v+Av} = C_{v'},$$

and therefore also lies in $\Gamma(\varepsilon)$. By Lemma 15, Γ is arithmetic in $O(2, 3)$; we have already shown that the $\mathbb{Q}$-rank is two.

Example 2. Let

$$f = (x - 1)(x^2 + 1)^2, \qquad g = (x + 1)\frac{x^5 - 1}{x - 1}.$$

In this case, we show that the $\mathbb{Q}$-rank of V is *one* and that Γ is arithmetic.

We have $g = x^5+2x^4+2x^3+2x^2+2x+1$ and $f = x^5-x^4+2x^3-2x^2+x-1 \equiv 0$. Hence $Av = g-f = 3x^4+x+2$ and $Av.v = 3$. Then $A^2v = 3x^5+x^2+2x$ and using the fact that $f \equiv 0$ we get $A^2v = 3(x^4-2x^3+2x^2-x+1)+x^2+2x = 3x^4-6x^3+7x^2-x+5$. Hence $A^2v.v = 3$. Similarly we compute $A^4v = -2x^4 + 11x^3 - 6x^2 + 6x - 3$. Hence $A^4v.v = -2$.

Therefore, if we write $\varepsilon = A^4v + v$ we see that $\varepsilon^2 = (A^4v)^2 + v^2 + 2A^4v.v = 2 + 2 + 2(-2) = 0$, and ε is isotropic. We compute the inner products $\varepsilon.A^kv$:

$$\begin{aligned} \varepsilon.v = A^4v.v + v.v = 0, \varepsilon.A^4v &= (A^4v)^2 + v.A^4v) = 2 - 2 = 0, \\ \varepsilon.Av = A^4.Av + Av.v &= A^3v.v + Av.v = -3 + 3 = 0, \\ \varepsilon.A^3v = A^4v.A^3v + v.A^3v &= Av.v + A^3v.v = 3 - 3 = 0. \end{aligned}$$

Consequently, the orthogonal complement $\varepsilon^{\perp}$ is spanned by ε, v, Av, A^3v. Since the reflections about the vectors v, Av, A^3v already lie in $\Gamma(\varepsilon)$, it follows from Lemma 15 that Γ is arithmetic.

It remains to show that the $\mathbb{Q}$-rank of V is one. Since ε is a rational isotropic vector, it is enough to check that on the quotient $\varepsilon^{\perp}/\mathbb{Q}\varepsilon$, the restriction of the quadratic form h is anisotropic over $\mathbb{Q}$ (it is isotropic over $\mathbb{R}$). With respect to the basis v, Av, A^3v of $\varepsilon^{\perp}/\mathbb{Q}\varepsilon$, the matrix of h is

$$\begin{pmatrix} v^2 & v, Av & v.A^3v \\ Av.v & (Av)^2 & Av.A^3v \\ A^3v.v & A^3v.Av & (A^3v)^2 \end{pmatrix} = \begin{pmatrix} 2 & 3 & -3 \\ 3 & 2 & 3 \\ -3 & 3 & 2 \end{pmatrix}.$$

(We have used the invariance of the dot product under A.) This is the quadratic form $2Q$ where

$$Q = x^2 + y^2 + z^2 + 3xy - 3xz + 3yx.$$

By completing the squares, and a linear change of variables, this form Q can be shown to be equivalent to the quadratic form

$$5x^2 - y^2 + 2z^2,$$

which has no integral zeros since 2 is not a quadratic residue modulo 5. Hence the $\mathbb{Q}$-rank of V is *one* but the group Γ is arithmetic.

Example 3. Let

$$f = (x-1)(x^2+x+1)^2, \quad g = \frac{x^5-1}{x-1}(x+1).$$

We show that Γ is arithmetic with $\mathbb{Q}\text{-rank}(V) = 2$.

Since f has *two* double roots, the real rank of V is two (Lemma 3). We have

$$f = x^5 + x^4 + x^3 - x^2 - x - 1 \equiv 0, \quad g = x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 1.$$

Therefore,

$$Av = g - f = x^4 + x^3 + 3x^2 + 3x + 2 \quad \text{and} \quad Av.v = 1.$$

Using $f \equiv 0$ we get

$$A^2v = x^5 + x^4 + 3x^3 + 3x^2 + 2 = 2x^3 + 4x^2 + 3x + 1 \quad \text{and} \quad A^2.v = 0.$$

Then

$$A^3v = 2x^4 + 4x^3 + 3x^2 + x \quad \text{and} \quad A^3v.v = 2.$$

Finally,

$$A^4v = 2x^4 + x^3 + 3x^2 + 2x + 2 \quad \text{and} \quad A^4v.v = 2.$$

Set $\varepsilon = A^4v - v$; then ε is isotropic. We compute

$$\varepsilon.Av = A^3v.v - Av.v = 2 - 1 = 1, \quad \varepsilon.A^3v = Av.v - A^3v.v = 1 - 2 = -1,$$

and $\varepsilon.A^2v = 0$. Therefore, $\varepsilon^{\perp}$ is spanned by ε, v, A^2v, $A^3v + Av$, and hence by the vectors ε, v, A^2v, $v' = A^2v - A^3v - Av$. Note that

$${}^{C_{Av}C_{A^3v}}(C_{A^2v}) = {}^{C_{Av}}(C_{A^2v-A^3v}) = C_{A^2v-Av-A^3v} = C_{v'}.$$

Then by Lemma 15, Γ is arithmetic.

Note also that if $w = A^3v + Av - v$, then

$$\begin{aligned} w.w &= (A^3v)^2 + (Av)^2 + v^2 + 2(A^3v.Av) - 2(A^3.v) - 2(Av.v) \\ &= 2 + 2 + 2 + 2.0 - 2.2 - 2.1 = 0, \end{aligned}$$

and hence w and ε are orthogonal and are both isotropic: $\mathbb{Q}$-rank$(V) = 2$.

Example 4. Let

$$f = (x-1)(x^2+1)(x^2+x+1), \qquad g = (x+1)\frac{x^5-1}{x-1}.$$

Then the group G has $\mathbb{R}$-rank two and $\mathbb{Q}$-rank one. The group Γ is arithmetic.

Example 5. Let

$$f = x^5 - 1, \qquad g = (x+1)(x^2-x+1)^2.$$

Then the group G has $\mathbb{Q}$-rank two and Γ is arithmetic.

Indeed, we find that $v.Av = -1, v.A^2v = 1, v.A^3v = 1, v.A^4v = -1$. Hence $\varepsilon = A^2v + A^3v - v$ is isotropic and its orthogonal complement is generated by ε, v, A^2v, $A^4v - Av$. Since $A^2v - A^4v + Av \in \varepsilon^{\perp}$, and is isotropic, it follows that $\mathbb{Q}$-rank$(V) = 2$. Since ${}^{C_{A^4v}}(C_{Av}) = C_{Av-A^4v}$, it follows that the reflections about the basis elements $v, A^2v, A^2v - A^4v$ of $\varepsilon^{\perp}/\mathbb{Q}\varepsilon$ all lie in Γ and fix ε. Hence (by arguments similar to those for Lemma 15), we get one non-trivial element u of the integral unipotent radical $U(\mathbb{Z})$ of the parabolic $P(\varepsilon)$ fixing the line through ε in Γ. To be specific, the element is $u = C_vC_{A^3v}C_vC_{A^2v}$, viewed as an element of $\Gamma(\varepsilon)$.

The conjugates of u by the reflections in $\Gamma(\varepsilon)$ generate a finite index subgroup of $U(\mathbb{Z})$ in $\Gamma(\varepsilon)$. Therefore, by Theorem 7, Γ is arithmetic.

Example 6. Let

$$f = x^5 - 1, \qquad g = (x+1)^3(x^2-x+1).$$

Then the group has $\mathbb{Q}$-rank two and Γ is arithmetic.

Indeed, we have $Av.v = 2$, $A^2v.v = 1$, $A^3v.v = 1$, $A^4v.v = 2$. Take $\varepsilon = Av - 1$. Then $\varepsilon^{\perp}/\mathbb{Q}\varepsilon$ is the span of v, A^3v, $A^2v + a^4v$. It is also the span of v, A^3v, v' where $v' = A^2v + a^4v - 2v$. Then

$${}^{C_{a^2v}C_v}(C_{A^4v}) = {}^{C_{A^2v}}(C_{A^4v-2v}) = C_{A^4v-2v+a^2v} = C_{v'},$$

and lies in $\Gamma(\varepsilon)$; the elements C_v, C_{A^3v} also do. Hence, by Lemma 15, the group is arithmetic.

The element $\varepsilon' = A^2v + A^4v - 2v - A^3v$ lies in $\varepsilon^{\perp}$ and is isotropic; hence $\mathbb{Q}$-rank$(G) = 2$.

Example 7. Let

$$f = (x-1)(x^2+x+1)^2, \qquad g = (x+1)(x^2-x+1)^2.$$

Then the group has $\mathbb{Q}$-rank two and Γ is arithmetic.

Indeed, we have $Av.v = -2$, $A^2v.v = 2$, $A^3v.v = 2$, $A^4v.v = -6$. Take $\varepsilon = A^2v - v$. Then $\varepsilon^\perp$ is the span of $v, Av, v' = A^4v + 2A^3v$. Now the reflections C_v and C_{Av} lie in $\Gamma(\varepsilon)$; the computation

$${}^{C_{A^3v}}(C_{A^4v}) = C_{A^4v+2A^3v} = C_{v'}$$

shows that so does $C_{v'}$. Hence by Lemma 15, Γ is arithmetic.

Example 8. Let

$$f = (x-1)(x^2+x+1)^2, \qquad g = (x+1)(x^4-x^2+1).$$

Then the group has $\mathbb{Q}$-rank two and Γ is arithmetic.

Indeed, we have $Av.v = 0$, $A^2v.v = 2$, $A^3v.v = -2$, $A^4v.v = 2$. Take $\varepsilon = A^2v - v$; then $\varepsilon^\perp$ is the span of ε, v, Av, A^4v and hence by Lemma 15, the group Γ is arithmetic. Since $A^4v - v$ is perpendicular to ε and is isotropic, the $\mathbb{Q}$-rank is two.

Example 9. Let

$$f = x^5 - 1, \qquad g = (x+1)(x^4-x^2+1).$$

Then the group G has $\mathbb{Q}$-rank two and Γ is arithmetic.

Indeed, we have $Av.v = 1$, $A^2v.v = -1$, $A^3v.v = -1$, $A^4v.v = 1$. It follows that $\varepsilon = A^2v - Av + v$ is isotropic and $\varepsilon^\perp$ is spanned by the vectors $\varepsilon, v, Av, A^4v - A^3v$. Since $\varepsilon' = A^2(\varepsilon)$ is also isotropic and is $(A^4v - A^3v) + A^2v$, it follows that the $\mathbb{Q}$-rank of G is two. Moreover, $A^4v - A^3v = {}^{C_{A^3v}}(C_{A^4v})$ and hence by Lemma 15 (to check that Lemma 15 applies, note that $\varepsilon = A^2v - Av - v$ is of the form $g(v) - v$ where $g = C_{Av}A^2 = AC_vA$), Γ is arithmetic.

Example 10. Let

$$f = (x-1)(x^2+1)^2, \qquad g = (x+1)(x^4-x^2+1).$$

Then Γ is arithmetic and the $\mathbb{Q}$-rank of G is two.

Indeed, a computation shows that $Av.v = 2$, $A^2v.v = -1$, $A^3v.v = -4$, $A^4v.v = 2$. Take $\varepsilon = A^4v - v$. Then

$$\varepsilon^\perp/\mathbb{Q}\varepsilon = \langle v, A^2v, v' = Av + A^3v = C_{A^3v}(Av)\rangle.$$

The formula for v' shows, by Lemma 15, that Γ is arithmetic. Moreover, if $\varepsilon' = v + A^2v - Av - A^3v = v + A^2v - v'$ then ε' is isotropic and orthogonal to ε; hence $\mathbb{Q}$-rank$(G) = 2$.

Acknowledgments. I thank Peter Sarnak for some very helpful communications concerning hypergeometric groups. I also thank Madhav Nori for suggesting (in a very different context) that Proposition 6 should be true.

The support of the JC Bose fellowship for the period 2013-2018 is gratefully acknowledged.

Most of the computations were done while the author was a visitor at the "Collaborative Research Centre, Spectral Structures and Topological Methods", Department of Mathematics, Bielefeld, Germany, and TIFR Centre for Applicable Mathematics, Bangalore. I thank Herbert Abels and Mythily Ramaswamy for invitation to visit, and the Bielefeld University and TIFR CAM for hospitality.

References

[1] Bass, H., Milnor, J., Serre, J-P.: Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$. Publ. IHES **33**, 59–137 (1967) Zbl 0174.05203 MR 0244257

[2] Beukers, F., Heckman, G.: Monodromy for the hypergeometric function ${}_nF_{n-1}$. Invent. Math. **95**, 325–354 (1989) Zbl 0663.30044 MR 0974906

[3] Borel, A., Tits, J.: Groupes réductifs. Publ. IHES **27**, 55–150 (1965) Zbl 0145.17402 MR 0207712

[4] Brav, C., Thomas, H.: Thin monodromy in $Sp(4)$. Compos. Math. **150**, 333–343 (2014) Zbl 1311.14010 MR 3187621

[5] Fuchs, E.: The ubiquity of thin groups. In: Thin Groups and Superstrong Approximation, MSRI Publ. 61, Cambridge Univ. Press, Cambridge, 73–92 (2014) Zbl 06587483 MR 3220885

[6] Fuchs, E., Meiri, C., Sarnak, P.: Hypergeometric monodromy groups for the hypergeometric equation and Cartan involutions. J. Eur. Math. Soc. **16**, 1617–1671 (2014) Zbl 1347.20054 MR 3262453

[7] Raghunathan, M. S.: Discrete Subgroups of Lie Groups. Ergeb. Math. Grenzgeb. 68, Springer, New York (1972) Zbl 0254.22005 MR 0507234

[8] Raghunathan, M. S.: A note on generators for arithmetic subgroups of algebraic groups. Pacific J. Math. **152**, 365–373 (1991) Zbl 0793.20045 MR 1141802

[9] Sarnak, P.: Notes on thin matrix groups. In: Thin Groups and Superstrong Approximation, MSRI Publ. 61, Cambridge Univ. Press, Cambridge (2014) Zbl 06587495 MR 3220897

[10] Singh, S., Venkataramana, T. N.: Arithmeticity of certain symplectic hypergeometric groups. Duke Math. J. **163**, 591–617 (2014) Zbl 1287.22005 MR 3165424

[11] Tits, J.: Systèmes générateurs de groupes de congruence. C. R. Acad. Sci. Paris Sér. A **283**, 693–695 (1976) Zbl 0381.14005 MR 0424966

[12] Vasershteĭn, L.: The structure of classical arithmetic groups of rank greater than 1. Math. USSR-Sb. **20**, 465–492 (1973) Zbl 0291.14016 MR 0349864

[13] Venkataramana, T. N.: On systems of generators for arithmetic subgroups of higher rank groups. Pacific J. Math. **166**, 193–212 (1994) Zbl 0822.22005 MR 1306038