HYPERGEOMETRIC GROUPS OF ORTHOGONAL TYPE

T.N.VENKATARAMANA

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 $O(2,3)$.

1. Introduction

Consider the $_{n}F_{n-1}$-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 $\theta$ are viewed as differential operators on the curve $C$. The fundamental group of $C$ (namely the free group on the two generators: small loops around 0 and $\infty$) acts on the space of solutions of this equation (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 $\alpha, \beta$. It is the group generated by $h_0, h_\infty$ where $h_0$ and $h_\infty$ are the images of the loops around 0 and $\infty$ under the monodromy representation.

The $_{n}F_{n-1}$-type hypergeometric monodromy representation is completely described by a result of Levelt. We briefly recall the description. Assume that $\alpha_j - \beta_k$ is not an integer for any $j, k$. If we put $f(x) = \prod_{j=1}^{n}(x - e^{2\pi i \alpha_j})$ and $g(x) = \prod_{j=1}^{n}(x - e^{2\pi i \beta_j})$, then $f, g$ have

1991 Mathematics Subject Classification. primary: 22E40. Secondary: 20F36
T.N.Venkataramana, School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Colaba, Mumbai 40005, INDIA.
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 hypergeometric equation $Du = 0$, with respect to which, the action of $h_0$ is by the matrix $A$ and that of $h_\infty$ 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 co-prime, 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 parameters $\alpha, \beta$ with the roots of $f, g$ being the exponentials of $\alpha_j, \beta_k$ as before.

The Zariski closure $G$ of the monodromy has been completely analysed by Beukers and Heckman ([2]). 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 $GL_n(\mathbb{Z})$. Assume also that $f, g$ form a primitive pair ([2]). In [2] it is proved 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 Conjecture 2 of [6]) the hypergeometric group is 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, 7 thin examples (with $G = Sp_4$) have been given by Brav and Thomas [4] using a ping-pong argument. We understand that the methods of [4] can also prove thin-ness 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 $\alpha, \beta$ 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 these 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 co-prime 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 co-prime polynomials. Then the hypergeometric monodromy group $\Gamma(f, g)$ is an arithmetic subgroup of an integral orthogonal group $O(h)(\mathbb{Z})$ with $\mathbb{Q} - \text{rank}(h) \geq 2$.

For example, if

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

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 we can prove that $\mathbb{Q} - \text{rank}(H) = 2$, where $H = O_5$ is the Zariski closure of the $5 \times 5$ hypergeometric group $\Gamma(f_1, g_1)$. Thus the analogue of Theorem 1 gives many more examples of arithmetic monodromy. In section 5 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 $x = (x_1, \cdots, x_k) \in \mathbb{Q}^k$ and $r \in \mathbb{Q}$. Let us write $x + r$ for the $k$-tuple $(x_1 + r, x_2 + r, \cdots, x_k + r)$. 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 to the exponent $m$. The parameters of $g$ can similarly be worked out.
1.1. **Description of the Proof.** We first show that when \( P = Q = 1 \), the monodromy group is an arithmetic subgroup of \( O(2, 3) \). To do this, we show 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 \( \Delta \) by explicit computation, by showing that \( \Delta \) 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 6).

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

In section , we list the pairs \( f_1, g_1 \) (up to scalar shift changing \( f(x) \mapsto f_1(-x) \) \( g_1(x) \mapsto g_1(-x) \) see [2], and [6]) of degree 5, with \( f_1(0) = -1, g_1(0) = 1 \) 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 are of \( \mathbb{Q} \)-rank two. The proof of arithmeticity in these cases is similar to the proof for \( \Delta \) considered above.

The authors of [6] also give a list of hypergeometric \( O(2, 1) \) 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, which in addition, 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 $1, x, \cdots, x^{n-1}$, 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 $w = 1, x, \cdots, x^{n-2}$ and $B(x^{n-1}) = x^n - g(x)$; the latter being a polynomial of degree at most $n - 1$, has been 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 vector space $V$ splits into a direct sum of subspaces $V_i$ such that each element of the group $\Gamma$ 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 first $n - 1$ basis elements $1, x, \cdots, x^{n-2}$, it follows that if $C = A^{-1}B$, then $C$ is identity on $1, x, \cdots, x^{n-2}$ 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 $1, x, \cdots, x^{n-2}$. Hence $x^{n-1}.v \neq 0$. We normalise $h$ so that $x^{n-1}.v = 1$. Therefore, for any vector $w = u_0 + u_1x + \cdots + u_{n-1}x^{n-1} \in V$ ($u_i \in \mathbb{Q}$), we have $w.v = u_{n-1}$. Denote by $\lambda$ 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 $1, x, \cdots, x^{n-1}$ 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

\[ v \cdot w = u_{n-1} \quad \forall w \in V, \]
\[ v \cdot v = 2 \quad \text{and} \]
\[ C(w) = w - (w \cdot v)v, \quad \forall w \in V. \]

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 $1, x, \cdots, x^{n-2}$. We have also seen that $Av = g - f = c_{n-1}x^{n-1} + \cdots + c_1x + 2$ where $c_i = b_i - a_i$. The operator on $V$ given by multiplication by $x$ is invertible. The equation

\[ f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x - 1 \equiv 0 \in V \]

shows that in $V$,

\[ \frac{1}{x} x^n = a_{n-1}x^{n-2} + \cdots + a_2x + a_1, \]

and that

\[ \frac{1}{x} (x^k) = x^{k-1} \quad \forall k \quad \text{with} \quad 1 \leq k \leq n - 1. \]

Therefore,

\[ v = \frac{1}{x} (Av) = \frac{1}{x} (c_{n-1}x^{n-1} + \cdots + c_1x + 2) = c_{n-1}x^{n-2} + \cdots + c_2x + c_1 + 2(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1). \]

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

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

Remark 3. Since $g$ and $f$ are co-prime, 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, $v, Av, \cdots, A^{n-1}v$ 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 the quadratic form $h$ under $A$ implies that $h$ is determined by the inner products $A^i v, (0 \leq i \leq n - 1)$. By Lemma 2 the latter is just the $x^{n-1}$-th coefficient of $A^i v$, viewed as a linear combination of $1, x, \cdots, x^{n-1}$. Hence $h$ is determined by the “highest coefficients” of the remainders of the polynomials $g - f, x(g - f), \cdots, x^{n-1}(g - f)$, 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 \( \mathbb{R} - \text{rank}(V) \geq 2 \). If \( n \geq 7 \), then \( \mathbb{Q} - \text{rank}(V) \geq 2 \).

Proof. 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 \(|p - q|\):

\[
|p - q| = \sum_{j=1}^{n} (-1)^{j+m_j} \left| \right|
\]

where if \((\alpha_1, \cdots, \alpha_n)\) are the parameters of \( f \) (i.e. the roots of \( f \) are \( e^{2\pi i \alpha_j} \), with \( 0 \leq \alpha_j < 1 \)), then \( m_j \) is the number of indices \( k \) such that \( \beta_k < \alpha_j \) (here \( \beta_1, \cdots, \beta_n \) are the parameters of \( g \)). The numbers \( \alpha_j, \beta_k \) 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 \( m_j = m_{j+1} \) (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 \(|p - q| \leq p + q - 2\).

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

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

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. \( \square \)

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 \( GL_3(\mathbb{Z}) \) 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 \( \leq 4 \): \( w = u_4x^4 + u_3x^3 + u_2x^2 + u_1x + u_0 \) with \( u_i \in \mathbb{Q} \). Denote by \( \lambda_0 \) 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 put $n = 6m + 5$. 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 co-prime 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 $v, Av, A^2v, A^3v, A^4v$. We have an injective linear map $i : V_0 \rightarrow V$ given on the basis elements $\{A^i_0v_0; 0 \leq k \leq 4\}$ by the formula $A^i_0v_0 \mapsto A^k v$.

**Lemma 4.** The above linear map $i$ is an isometry of the quadratic spaces $(V_0, h_0)$ and $(W, h_W)$. In particular, the restriction $h_W$ of $h$ to $W$ is non-degenerate; write the orthogonal decomposition $V = W \oplus W^\perp$. The group generated by the reflections $A^r_0C_0A_0^{-r}; 0 \leq r \leq 4$ is isomorphic to the group $\Delta$ generated by the reflections $A^rCA^{-r} : 0 \leq r \leq 4$. Moreover, $\Delta$ 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 $h_0(A^k_0v_0, A^l_0v_0)$ coincide if $0 \leq k,l \leq 4$. Using the invariance of $h, h_0$ under $A, A_0$ it is sufficient to check that the inner products $h(v, A^k v)$ and $h_0(v_0, A^k_0v_0)$ coincide. But these values are nothing but the $x^{n-1}$-coefficient of the vector $A^k Av = x^k(f-g)$, viewed as a linear combination of $1, x, \ldots, x^{n-1}$ (similarly $h_0(A^k_0v_0, v_0)$ is the $x^4$-th coefficient of the vector $A^k_0A_0v_0 = x^k(f_0-g_0)$ viewed as a linear combination of $1, x, x^2, x^3, x^4$).

It is trivial to check that $x^{n-1}$ coefficient of $x^k(f-g)$ is the same as $x^4$-th coefficient of $f_0-g_0$ since $f(x) = f_0(x)(P(x^6)$ and $g(x) = g_0(x)Q(x^6)$ and $f_0,g_0$ have degree 5. 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 an orthogonal decomposition, then $O(W)$ may be viewed as the subgroup of $V$ which fixes $W^\perp$ point-wise. 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 5.** If $\Gamma$ 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 $\Gamma$ has finite index in $SO(V, \mathbb{Z})$ provided $\mathbb{Q} - \text{rank}(W) = 2$.

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

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

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 $\Gamma$ 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 $p_0$ and $g$ of $P$ and $G$, decompose as follows ($\Phi^+$ is the system of positive roots, i.e. those roots occurring in $p_0$, and $\Phi$ is the system of all roots)

$$p_0 = g_0 \oplus_{\alpha \in \Phi^+} g_\alpha, \quad g_0 = g_0 \oplus_{\alpha \in \Phi^+} g_\alpha \oplus g_{-\alpha}.$$ 

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

Suppose that $\alpha, \beta$ are two roots which are not rational multiplies of each other. Then necessarily $\mathbb{Q} - \text{rank}(G) \geq 2$. In a group denote by $[x, y]$ the commutator element $xyzx^{-1}y^{-1}$. 


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
\[ P = \prod_{x \in X} g_x, \]
denote the product of $g_x$ where the product is taken in the sense that if $x < x' \in X$ then $g_x$ appears to the left of $g_{x'}$.

We have the Chevalley commutator relations:

**Lemma 7.** For every pair of integers $m, n \geq 1$ such that $ma + nb$ is a root, there exist one parameter unipotent groups $X_{ma+nb}$ such that for all $s, t \in G$ we have the commutator relation
\[ [X_{\alpha}(s), X_{\beta}(t)] = \prod X_{ma+nb}(s^m t^n), \]
where the product is of elements of the group $G$, and the roots $\theta_{m,n} = ma + nb$ are arranged in some arbitrary but fixed order (so that $m+n < m'+n'$ then $\theta_{m,n}$ appears before, i.e. to the left of $\theta_{m',n'}$ in the product).

**Lemma 8.** Fix an integer $N \geq 1$ and consider the group $U_N$ generated by commutators
\[ [X_{\alpha}(s), X_{\beta}(t)]; s, t \equiv 0 \pmod{N}. \]
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 $X_{ma+n\beta}(x)$ for $x \equiv 0 \pmod{M}$.

**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 $U_{ma+n\beta}: m, n \geq 1$ 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 $X_{ma+n\beta}$). Denote by $u_0$ and $u^*$ the Lie algebras of $U_0$ and of $U^*$. Denote by Log the inverse of the exponential map from $U^*$ onto $u^*$.

Taking the logs of the commutators in the commutator relations, we obtain that a polynomial $P$ in $t, s$ namely
\[ P(t, s) = \log(\prod_{m,n} (X_{m,n}(t^m s^n))) \]
takes values in the subspace $u_0$; hence the coefficient of $ts$ also does. This coefficient is nothing but $\log(X_{1,1})$; hence the first element $X_{1,1}$ in the ordering lies in $U_0$; now an easy induction in 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 1-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 $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5$ of $W$ such that $\varepsilon_1^2 = \varepsilon_2^2 = 0$, $(\varepsilon_3^*)^2 = (\varepsilon_1^*)^2 = 0$, $w_3^3 \neq 0$, $\varepsilon_1.w_3 = \varepsilon_1^*,w_3 = 0$ for $i = 1,2$ and $\varepsilon_i(\varepsilon_j^*) = \delta_{ij}$. With respect to this basis, $O(W)$ may be thought of as a subgroup of the group $GL_5$ of $5 \times 5$ matrices. We will informally denote $O(W)$ by $O(2,3)$.

The intersection of the diagonals with $H = O(W)$ is a two-dimensional split group $S = \{t_1,t_2\} \subset \mathbb{G}_m^2$ which acts by the characters $t_i$ on $\varepsilon_i$, $t_i^{-1}$ on $\varepsilon_i^*$ and trivially on $w_3$. Denote by $h_{x_1}$ (resp. $h_{x_1+x_2}$) 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 8, we have

**Lemma 9.** In the notation of the preceding subsection, for any integer $N \geq 1$, the group generated by the commutators

$$[X_{x_1}(s), X_{x_1+x_2}(t)]; s,t \equiv 0 \pmod{N}$$

contains the group $X_{x_2}(M\mathbb{Z})$ where the latter 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 8 to the roots $\alpha = x_1 + x_2$ and $\beta = x_1$.

3.4. **The group** $O(V)$. Since $\mathbb{Q}$ rank of $W$ is two, the $\mathbb{Q}$ rank $r$ of $V$ is at least two. There exists a basis $\varepsilon_1, \ldots, \varepsilon_r, v_1, \ldots, v_m, \varepsilon_1^*, \varepsilon_r^*, \ldots, \varepsilon_1^*$ of $V$ ($dim(V) = n = 2r + m$) such that (1) $\varepsilon_j, \varepsilon_j^* = \delta_{ij}$ (the Kronecker delta symbol) 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 $\varepsilon_3, \ldots, \varepsilon_r, \varepsilon_3^*, \ldots, \varepsilon_r^*$. Under the inclusion $O(W) \subset O(V) \subset GL_n$, 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 $\varepsilon_3, \ldots, \varepsilon_r, v_1, \ldots, v_m, \varepsilon_3^*, \ldots, \varepsilon_r^*$. Let $M$ 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, $U$ its unipotent radical. $M$ is a Levi subgroup of $P$ containing the torus $S$ and we have $P = MU$. It is easy to see that $M = GL_2, O(Y)$ where $S \subset GL_2$ and $GL_2$ is the subgroup of $M$ 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 is $\mathfrak{h}_{x_1+x_2}$. Moreover, the action of $M = GL_2, O(Y)$ on the direct sum $\mathfrak{g}_{x_1} \oplus \mathfrak{g}_{x_2}$ is simply the exterior tensor product $St \otimes St$ of the standard representations of $GL_2$ and $O(Y)$ (and in particular, is irreducible for the action of $M$). We note that $\mathfrak{h} \cap \mathfrak{g}_{x_1} \neq \{0\}$.

**Lemma 10.** 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 $uv^Mvu^{-1}u'^{-M}$ lies in $X_{x_1+x_2}(NZ)$.

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

### 3.5. Proof of the Proposition

Let $\mathcal{U}$ denote the open Bruhat cell $Pw_0U$ where $w_0$ is the longest Weyl group element. Since $\Gamma$ is Zariski dense in $G = O(V)$, it follows that $\Gamma \cap \mathcal{U}$ is also Zariski dense in $G$. Given $\gamma \in \Gamma \cap \mathcal{U}$ write $\gamma = pw_0u$ accordingly. Then the elements $p$ (as $\Gamma$ varies) consist of 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 $p(h)_{x_1}p^{-1}$ 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 $u/\mathfrak{g}_{x_1+x_2}$ 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 $\Gamma$ contains a finite index subgroup of $H(Z)$ it contains the congruence group $(U \cap H)(NZ)$ for some integer $N$. In particular, there exists an element $v \in (U \cap H)(MZ)$ with the integer $M$ large such that for all $\gamma \in F$ the finite set of the previous paragraph, the elements $uvu^{-1}v^{-1}$ lies in $U_{x_1+x_2}(NZ) \subset \Gamma$. Consider the commutator set

$$E = \gamma(vX_{x_1+x_2}(MZ), X_{x_1+x_2}(MZ)).$$

Since $\gamma = pw_0u$ it follows from Lemma 10 that this set contains the commutator set

$$[pw_0(v), X_{x_1+x_2}(MZ)].$$

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

$$p([pw_0(v), X_{x_1+x_2}(NZ)]).$$
Since \( w_0(v) \) lies in \( X_{-2}(NZ) \), it follows from Lemma 9 that the group generated by the latter commutator contains \( X_{x_2}(MZ) \) for some integer \( M \) divisible large powers of \( N \) and the denominators of the rational matrix \( p \). Since the \( p \) conjugates of \( X_{x_1}(MZ) \) 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 contain \( U_{x_1}(MZ) \) and \( U_{x_2}(MZ) \). These generate a finite index subgroup of \( U(Z) \). Therefore, \( \Gamma \) contains a finite index subgroup of \( U(Z) \).

Now \( U \) is the unipotent radical of the parabolic subgroup \( P \) and \( G \) has real rank (even rational rank) at least two. By Theorem 6, it follows that \( \Gamma \) is arithmetic.

4. The arithmeticity of \( \Gamma \)

4.1. Arithmeticity of \( \Delta \). 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 \( \mathbb{Q} - \text{rank}(W) = 2 \). To ease the notation, we drop the subscript \( 0 \) in \( v_0, A_0 \) and simply write \( v, A \) etc.

Lemma 11. We have
\[
\begin{align*}
v.v &= 2, Av.v = 1, A^2v.v = 2, A^3v.v = 2, A^4v.v = 1.
\end{align*}
\]
The vector \( \varepsilon = v - A^2v \) is isotropic and the orthogonal complement \( \varepsilon^\perp \) is the span of the four vectors \( \varepsilon, v, Av, A^3v + A^4v - v \). Moreover, the reflections about the three vectors \( v, Av, A^3v + A^4v - v \) lie in \( \Gamma \) and fix \( \varepsilon \).

Proof. We view \( V \) as the space of polynomials of degree \( \leq 4 \). We need only compute the coefficient of \( x^4 \) of 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 \( Av = x^5 + 2x^4 + 2x^3 + x^2 + 2x = 2x^4 + 2x^3 + x^2 + 2x + 1 \) (since \( x^5 - 1 = 0 \) in \( V \)). Therefore, the \( x^4 \) coefficient of \( A^2v \) is 2. The others are proved similarly.

The second part follows immediately from the first: as an illustration, we compute
\[
\begin{align*}
\varepsilon.v &= A^2v.v - v.v = 2 - 2 = 0 \quad \text{and} \\
\varepsilon.A^2v &= A^2v.A^2v - v.A^2v = v.v - A^2v.v = 2 - 2 = 0.
\end{align*}
\]
Note that we have used the invariance of the “dot product” under the action of \( A, B \). The others are proved similarly.
We denote by $\Delta(\varepsilon)$ the subgroup of $\Delta$ which fixes the line through $\varepsilon$. It is the intersection of $\Delta$ with the parabolic subgroup $P = P(\varepsilon)$ of $G$ which fixes the isotropic vector $\varepsilon$. Since the vectors $v, Av, v'$ are in the orthogonal complement of $\varepsilon$ it follows that the reflections $C_v, C_{Av}, C_{v'}$ about the vectors $v, Av, v'$ fix the vector $\varepsilon$ and in particular, lie in $P$. Since the reflections about $v$ and $Av$ are the elements $C$ and $ACA^{-1}$, it follows that $C_v$ and $C_{Av} = ACA^{-1}$ lie in $\Delta(\varepsilon)$, since $\Delta$ is the group generated by $A, C$. We need only prove that $C_{v'}$ lies in $\Delta$.

In a group, denote $x(y) = xyx^{-1}$. 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
\[ C_{A^3v}C_v(C_{A^4v}) = C_{A^3v}(C_{A^4v-v}v) = C_{A^4v-v-A^4v+2Av} = C_{v'} \]

The extreme left hand side term of the above equalities lies in $\Delta$ since each of the reflections about $v, A^3v, A^4v$ does. Therefore, $C_{v'}$ lies in $\Delta$. $\square$

**Notation.** The element $\varepsilon$ of the Lemma 11 is isotropic. Hence we have the partial flag $Q \varepsilon \subset \varepsilon \perp \subset V$. 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 $\varepsilon$ by Lemma 11. 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 $w \in \varepsilon \perp$, $w(A^2v - v) = 0$ i.e.
\[ C_{A^2v}C_v(w) = C_{A^2v}(w - (w.v)v) = \\
\quad = w - (w.A^2v)A^2v - (w.v)v + (w.v)(A^2v.v)A^2v = \\
\quad = w - (w.v)A^2v - (w.v)v + 2(w.v)A^2v = w + (w.v)(A^2v - v), \]

since $A^2v.v = 2$ (Lemma 11). That is
\[ C_{A^2v}C_v(w) = w + (w.v)(Av - v) \quad \forall w \in \varepsilon \perp. \]

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

**Lemma 12.** 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 $M = O(\varepsilon \perp/Q\varepsilon)$. By Lemma 11, the image of $\Delta(\varepsilon)$ in the quotient $M$ contains the reflections about the basis elements.
HYPERGEOMETRIC GROUPS OF ORTHOGONAL TYPE

$v, A^2v, v' = A^3v + A^4v - v$. Moreover, these basis elements are mutually non-orthogonal. Hence the group generated by these three reflections acts irreducibly on the standard representation $Q^3$ of $M$. However, the conjugation action of $M$ on $U$ is clearly the standard representation of $M$. 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 spans $U(Q) = Q^3$. That is, $U \cap \Delta(\varepsilon)$ contains a spanning set of $Q^3$. Hence $U \cap \Delta(\varepsilon)$ contains a finite index subgroup of $Z^3$.

**Proposition 13.** 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, $Q - \text{rank}(V_0) = 2$.

**Proof.** Consider the vector $\varepsilon' = A^3v + A^4v - Av$. By Lemma 11, $\varepsilon'$ lies in $\varepsilon^\perp$. We compute the dot product of $\varepsilon'$ with itself (we write $w^2$ for $w.w$):

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

Using the formulae for the dot product in Lemma 11, this is $6 + 2v.Av - 2.2 = 6 + 2 - 4 = 0$. Hence $\varepsilon, \varepsilon'$ are linearly independent mutually orthogonal isotropic vectors. Hence $Q - \text{rank}(V_0) \geq 2$. Since $h = h_0$ is non-degenerate ([2]) and is a quadratic form in 5 variables, it follows that $Q - \text{rank}(V)$ is exactly 2.

By Lemma 12, the intersection $\Delta \cap U$ has finite index in $U(Z)$ and $U$ is the unipotent radical of a parabolic $Q$-subgroup of $H = O(V_0, h_0)$. By [2], the monodromy group $\Delta$ is Zariski dense in $H$. By the preceding paragraph, $Q$ rank of $H$ is at least two. Therefore, by Theorem 6, $\Delta$ is an arithmetic subgroup of $H(Z)$.

**4.2. Proof of the Main Theorem.** We now return to the situation of Lemma 4. We have the spaces $V_0$ 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 leave $W$ stable and act trivially on $W^\perp$. The reflections with respect to the vectors $\{A^k v : 0 \leq k \leq 4\}$ lie in $O(W)$ since they act trivially on $W^\perp$. By Proposition 13, these reflections generate an arithmetic subgroup of $O(W)$.

Now $\Gamma$ is Zariski dense in $O(V)$ by [2]. By Proposition 5, and by the last sentence of the preceding paragraph, $\Gamma$ 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 2.

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 $g(0) = 1$. Put $V = \mathbb{Q}[x]/(f(x))$; let $v, Av$ be as before and and normalise the inner product $h$ so that $v.v = 2$.

**Lemma 14.** Suppose there exists $g \in \Gamma$ such that $\varepsilon = g(v) + v \in V$ 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 $\mathbb{R}-\text{rank}(V) = 2$. Then $\Gamma$ is arithmetic.

**Proof.** We only work out the case $\varepsilon = g(v) - v$, the other being similar. The isotropy of $\varepsilon$ 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 $C_{g(v)}(w) = w - (w.v)v$. 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 $C_{g(v)}(v)$ 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 $2\varepsilon$. Hence $\theta = C_{v}^{-1}C_{g(v)}(v)$ lies in the unipotent radical $U$ of the parabolic subgroup $P$ which fixes $\varepsilon$.

The Levi part of this parabolic is $O(Q)$ where $Q$ is the quotient $\varepsilon^\perp/\mathbb{Q}\varepsilon$. 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 identity: it contains $\theta$. The irreducibility of the action of $R$ on $\mathbb{Q}^3$ implies that the conjugates by elements of $R$ of $\theta$ generate a finite index subgroup of $U(\mathbb{Z})$.

Now, $\mathbb{R} - \text{rank}(G) = 2$ and $\Gamma$ is Zariski dense in $G$ by [2]. By the conclusion of the preceding paragraph, $\Gamma$ contains a finite index subgroup of $U(\mathbb{Z})$. The arithmeticity of $\Gamma$ follows from Theorem 6. □

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

**Example 1.** $f = (x - 1)(x^2 + 1)^2$ and $g = (x + 1)(x^2 - x + 1)^2$. 

We will show that the hypergeometric group $\Gamma$ is arithmetic and that $\mathbb{Q}$ 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 we have

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

In other words,

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

We will view $V$ is the space of polynomials of degree $\leq 4$. 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 $Av.v = 0$.

The element $A^2v = x(Av) = -x^4 + 3x^3 - 2x^2 + 2x$ and $A^2v.v = -1$. Similarly, $A^3v = -x^5 + 3x^4 - 2x^3 + 2x^2 = (-x^4 + 3x^3 - 2x^2 + x - 1) + 3x^4 - 2x^3 + 2x^2 = 2x^4 + x - 1$.

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 $\varepsilon$. We have:

$$\varepsilon.v = A^4v.v - v.v = 0,$$

$$\varepsilon.Av = A^4v.Av - v.Av = A^3v.v - Av.v = 2 - 0 = 2,$$


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

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

and therefore also lies in $\Gamma(\varepsilon)$. By lemma 14 $\Gamma$ is arithmetic in $O(2,3)$; we have already shown that the $\mathbb{Q}$-rank is two.
Example 2. \( f = (x - 1)(x^2 + 1)^2 \) and \( g = (x + 1)^{\frac{x^5}{x+1}} - 1 \).

In this case, we show that \( \mathbb{Q} \text{-rank of } V \) is one and that \( \Gamma \) 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 \( A^2v = 3 \). 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 \( \varepsilon \) is isotropic. We compute the inner products \( \varepsilon.A^kv \):

\[ \varepsilon.v = A^4v.v + v.v = 0, \varepsilon.A^4v = (A^4v)^2 + v.A^4v = 2 - 2 = 0, \]
\[ \varepsilon.Av = A^4.Av + Av.v = A^3v.v + Av.v = -3 + 3 = 0, \]
\[ \varepsilon.A^3v = A^4v.A^3v + v.A^3v = Av.v + A^3v.v = 3 - 3 = 0. \]

Consequently, the orthogonal complement \( \varepsilon \perp \) is spanned by \( \varepsilon, v, Av, A^3v \).

Since the reflections about these vectors \( v, Av, A^3v \) already lie in \( \Gamma(\varepsilon) \), it follows from Lemma 14 that \( \Gamma \) is arithmetic.

It remains to show that the \( \mathbb{Q} \)-rank of \( V \) is one. Since \( \varepsilon \) 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 of the form

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

(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 \( \mathbb{Q} \)-rank of \( V \) is one but the group \( \Gamma \) is arithmetic.

Example 3. \( f = (x - 1)(x^2 + x + 1)^2 \), \( g = \frac{x^5}{x+1}(x + 1) \).
We show that $\Gamma$ 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 $f = x^5 + x^4 + x^3 - x^2 - x - 1 \equiv 0$, $g = x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 1$. Therefore,

$$Av = g - f = x^4 + x^3 + 3x^2 + 3x + 2,$$

and hence by the vectors $\varepsilon,v,A$.

Example 4. $f$ and hence $w$. Then by Lemma 14, $\Gamma$ is arithmetic.

Using $f \equiv 0$ we get

$$A^2v = x^5 + x^4 + 3x^3 + 3x^2 + 2 = 2x^3 + 4x^2 + 3x + 1,$$

and

$$A^2.v = 0.$$

We find that $\varepsilon,v,A$.

Example 5. $f$ and hence $w$. It follows that $\varepsilon, v, A$ and hence by the vectors $\varepsilon,v,A$.

Finally,

$$A^4v = 2x^4 + 3x^2 + 2x + 2$$

and $A^4.v = 2$.

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

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

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

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

Then by Lemma 14, $\Gamma$ is arithmetic.

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

$$w.w = (A^3v)^2 + (Av)^2 + v^2 + 2(A^3v.Av) - 2(A^3v) - 2(Av.v) =
\quad = 2 + 2 + 2.0 - 2.2 - 2.1 = 0$$

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

Example 4. $f = (x-1)(x^2+1)(x^2+x+1)$ $g = (x+1)(\frac{x^4-1}{x-1})$. The group $G$ has $\mathbb{R}$ rank two and $\mathbb{Q}$-rank one. The group $\Gamma$ is arithmetic.

Example 5. $f = x^5 - 1$, $g = (x+1)(x^2-x+1)^2$. The group $G$ has $\mathbb{Q}$-rank two and $\Gamma$ is arithmetic.

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 $\varepsilon,v,A^2v,A^3v-Av$. Since $A^2v-A^3v+Av \in \varepsilon^\perp$, and is isotropic, it follows that $\mathbb{Q} - \text{rank}(V) = 2$. Since $C_{A^4v}(C_Av) = C_{Av-A^4v}$, it follows that the reflections about these basis elements $v, A^2v, A^3v - A^4v$ of $\varepsilon^\perp/\varepsilon$ all lie in $\Gamma$ and fix $\varepsilon$. Hence (by arguments similar to Lemma 14), we get one non-trivial element $u$ of the integral unipotent radical.
$U(\mathbb{Z})$ of the parabolic $P(\varepsilon)$ fixing the line through $\varepsilon$ in $\Gamma$. To be specific, the element is $u = C_v C_{A^2 v} C_v C_{A^2 v}$, viewed as an element of $\Gamma(\varepsilon)$. The conjugates of $u$ by the reflections in $\Gamma(\varepsilon)$, generates a finite index subgroup of $U(\mathbb{Z})$ in $\Gamma(\varepsilon)$. Therefore, by Theorem 6, $\Gamma$ is arithmetic.

**Example 6.** $f = x^5 - 1$, $g = (x + 1)^3(x^2 - x + 1)$

The group has $Q$-rank two and $\Gamma$ is arithmetic.

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

\[
C_{a^2 v} C_v (C_{A^4 v}) = C_{a^2 v} (C_{A^4 v - 2v}) = C_{A^4 v - 2v + a^2 v} = C_v,
\]

and lies in $\Gamma(\varepsilon)$; the elements $C_v, C_{A^3 v}$ also do. Hence, by Lemma 14, the group is arithmetic.

Example 7. $f = (x - 1)(x^2 + x + 1)^2$, $g = (x + 1)(x^2 - x + 1)^2$

The group has $Q$-rank two and $\Gamma$ is arithmetic.

We have $Av.v = 0, A^2 v.v = 2, A^3 v.v = -2, A^4 v.v = 2$. Take $\varepsilon = A^2 v - v$; then $\varepsilon^\perp$ is the span of $\varepsilon, v, Av, A^4 v$ and hence by Lemma 14, the group $\Gamma$ is arithmetic. Since $A^4 v - v$ is perpendicular to $\varepsilon$ and is isotropic, the $Q$-rank is two.

**Example 8.** $f = (x - 1)(x^2 + x + 1)^2$, $g = (x + 1)(x^4 - x^2 + 1)$.

The group has $Q$-rank two and $\Gamma$ is arithmetic.

We have $Av.v = 0, A^2 v.v = 2, A^3 v.v = -2, A^4 v.v = 2$. Take $\varepsilon = A^2 v - v$; then $\varepsilon^\perp$ is the span of $\varepsilon, v, Av, A^4 v$ and hence by Lemma 14, the group $\Gamma$ is arithmetic. Since $A^4 v - v$ is perpendicular to $\varepsilon$ and is isotropic, the $Q$-rank is two.

Example 9. $f = x^5 - 1$, $g = (x + 1)(x^4 - x^2 + 1)$.

The group $G$ has $Q$-rank two and $\Gamma$ is arithmetic.

We have $Av.v = 1, A^2 v.v = -1, A^3 v.v = -1, A^4 v.v = 1$. It follows that $\varepsilon = A^2 v - Av + v$ 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 \( \mathbb{Q} \)-rank of $G$ is two. Moreover, $A^4v - A^3v = CA^2v (C_A^3v)$ and hence by Lemma 14 (to check that Lemma 14 applies, note that $\varepsilon = A^2v - Av - v$ is of the form $g(v) - v$ where $g = C_Av. A^2 = AC_v A$), $\Gamma$ is arithmetic.

**Example 10.** $f = (x - 1)(x^2 + 1)^2$, $g = (x + 1)(x^4 - x^2 + 1)$.

$\Gamma$ is arithmetic and \( \mathbb{Q} \)-rank of $G$ is two.

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 $\varepsilon' = v, A^2v, v' = Av + A^3v = C_A^3v(Av) > .$

The formula for $v'$ shows from Lemma 14, that $\Gamma$ is arithmetic. Moreover, if $\varepsilon' = v + A^2v - Av - A^3v = v + A^2v - v'$ then $\varepsilon'$ is isotropic and orthogonal to $\varepsilon$; hence \( \mathbb{Q} - rank(G) = 2. \)

6. Complements
Acknowledgements:

I thank Peter Sarnak for some very helpful communications concerning hypergeometric groups.

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. I thank Herbert Abels for his invitation to visit and the Bielefeld University for its hospitality.

References

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


T.N. Venkataramana, School of Mathematics, TIFR, Homi Bhabha Road, Colaba, Mumbai 400005, India
E-mail address: venky@math.tifr.res.in