Annals of Mathematics **179** (2014), 1041–1083
http://dx.doi.org/10.4007/annals.2014.179.3.4

Image of the Burau representation at d-th roots of unity

By T. N. Venkataramana

Abstract

We show that the image of the braid group under the monodromy action on the homology of a cyclic covering of degree d of the projective line is an arithmetic group provided the number of branch points is sufficiently large compared to the degree d. This is deduced by proving the arithmeticity of the image of the braid group on $n+1$ letters under the Burau representation evaluated at d-th roots of unity when $n \geq 2d$.

Contents

1. **Introduction**

This paper is concerned with the question of whether some natural monodromy groups are arithmetic. These questions were first considered by Griffiths and Schmid [GS75]. Following [GS75, pp. 123–124], we say that a subgroup $\Gamma \subset \mathrm{GL}_N(\mathbb{Z})$ is an *arithmetic group* if Γ has finite index in the integral points of its Zariski closure in GL_N. If Γ is an arithmetic group, then by a result of Borel and Harish-Chandra, Γ is a lattice in the group of real points of the Zariski closure. In [GS75], the groups Γ arise as follows. Let $\pi : X \to S$ be an algebraic family of algebraic manifolds, which is a fibration. Write $V_{s_0} = \pi^{-1}(\{s_0\})$ for a typical fibre and $\Gamma \subset \mathrm{Aut}(H^m(V_{s_0}))$ for the *monodromy group*; i.e., the image of the action of $\pi_1(S)$ on the cohomology group (with integral coefficients) of the fibre V_{s_0}. Griffiths and Schmid then raise the question: is the monodromy group an arithmetic group?

The foregoing question has a negative answer in general, as was shown by Deligne and Mostow ([DM86]). (There are examples of monodromy groups

which are not even finitely presented in [Nor86] — arithmetic groups are finitely presented by a result of Raghunathan.) Let us recall the basic set-up of [DM86]. Let $d \geq 2$ be an integer. For the family S, take the space of complex $n+1$-tuples $a = (a_1, \ldots, a_{n+1})$ whose entries are all distinct. Fix integers $k_1, \ldots, k_{n+1}$ with $1 \leq k_i \leq d-1$. Assume that the g.c.d. of $\{d, k_1, \ldots, k_{n+1}\}$ is 1. Given $a \in S$, consider the set $X_{a,k}$ of solutions (x, y) of the equation

$$y^d = (x - a_1)^{k_1}(x - a_2)^{k_2} \cdots (x - a_{n+1})^{k_{n+1}}.$$

The space $X_{a,k}$ has a natural structure of a compact Riemann surface $X^*_{a,k}$ with finitely many punctures. We then get a map $\pi : X \to S$ described on the "affine part" by $(x, y, a) \mapsto a$, where $(x, y) \in X_{a,k}$ and $a \in S$ and where X is the family of the compact Riemann surfaces $X^*_{a,k}$; we can then consider the monodromy action on $H^1(X^*_{a,k}, \mathbb{Z})$ for a typical fibre $X^*_{a,k}$.

The fundamental group of the space S is well known to be the pure braid group P_{n+1} on $n+1$ strands; thus the fibration $X \to S$ yields a monodromy representation

$$\rho^*_M(k, d) : P_{n+1} \to \mathrm{GL}(H^1(X^*_{a,k}, \mathbb{Z}))$$

of P_{n+1} on the integral cohomology of the fibre $X^*_{a,k}$. If N is the rank of the abelian group $H_1(X^*_{a,k}, \mathbb{Z})$, then the image Γ of P_{n+1} is a subgroup of $\mathrm{GL}_N(\mathbb{Z})$. Form the Zariski closure $\mathcal{G}$ of Γ in GL_N; this is a linear algebraic group defined over $\mathbb{Q}$.

We now give only a qualitative description of the results of [DM86]. Deligne and Mostow prove that for special choices of the integers d, n and $k_1, \ldots, k_{n+1}$, the monodromy group Γ does not have finite index in $\mathcal{G}(\mathbb{Z})$. Hence this gives a negative answer to the question of Griffiths-Schmidt mentioned before. It can be shown that the group $\mathcal{G}(\mathbb{R})$ of real points of the Zariski closure is a product $\prod_j U(p_j, q_j)$ of unitary groups $U(p_j, q_j)$. (The unitary structure on $H^1(C, \mathbb{C})$ of the curve $C = X^*_{a,k}$ comes from the intersection form $h(\alpha, \beta) = \int_C \alpha \wedge \overline{\beta}$.) As we mentioned before, $\mathcal{G}(\mathbb{Z})$ is a discrete subgroup of $\mathcal{G}(\mathbb{R})$, and hence so is Γ. However, the projection of Γ to one of these factors $U(p_j, q_j)$ may not be discrete. In [DM86] (see also [Mos86]) it is shown — using their INT and Σ-INT criteria — that for a finite number of special choices of k_i, d, n, one of these $U(p_j, q_j)$ is $U(n-1, 1)$ and that the *projection* of the monodromy group Γ to this factor $U(n-1, 1)$ continues to be discrete. Once the projection is discrete, it follows (see [McM13, Th. (10.3)], for example) that the image of the projection is a lattice in $U(n-1, 1)$; if there is one more noncompact factor isomorphic to $U(p, q)$ in $\mathcal{G}(\mathbb{R})$, then it follows (see [McM13, §10, p. 48]) that the image of the projection of the Γ in $U(n-1, 1)$ is a nonarithmetic *lattice*. In particular, the monodromy group Γ does not have finite index in $\mathcal{G}(\mathbb{Z})$. (If the monodromy were to have finite index, then the

projection to $U(n-1,1)$ would either be nondiscrete or an arithmetic lattice; this is discussed in more detail in [McM13, Cor. 10.4].)

In view of the Margulis arithmeticity theorem (that irreducible lattices in linear semi-simple Lie groups of real rank at least two are arithmetic), the above strategy to produce nonarithmetic lattices cannot work if $U(n-1,1)$ is replaced by $U(p,q)$ with $p,q \geq 2$; if we are to have $U(n-1,1)$ as a factor, it may be shown that the number $n+1$ of branch points $a_1,\ldots,a_{n+1}$ must not exceed $2d$. (See the proof of Theorem 2, where we prove this in the special case when all the k_i are 1.) However, if we take $n \geq 2d$, it is still of interest — in view of the question of Griffiths and Schmid — to know whether the monodromy $\Gamma \subset \mathcal{G}(\mathbb{Z}) \subset \mathrm{GL}_N(\mathbb{Z})$ has finite index in $\mathcal{G}(\mathbb{Z})$. In this paper, we prove that if $n \geq 2d$ and all the k_i are 1, then Γ does have finite index in $\mathcal{G}(\mathbb{Z})$. (See Theorem 26 for the statement of a more general case.)

Consider the compactification X_a^* of the affine curve X_a defined by

$$y^d = (x-a_1)(x-a_2)\cdots(x-a_{n+1}),$$

with $y \neq 0$ and $x \neq a_1,\ldots,a_{n+1}$. As before, there is the monodromy action of the pure braid group P_{n+1} on the cohomology of the fibre X_a^*. Since the equation of the curve is patently invariant under the action of the permutations of the a_i's, the action extends to an action of the full braid group B_{n+1} on $H_1(X_a^*,\mathbb{Z})$.

THEOREM 1. *Suppose $d \geq 3$. If $n \geq 2d$, then the image Γ of the monodromy representation $\rho(d) : B_{n+1} \to \mathrm{GL}(H^1(X_a^*,\mathbb{Z})) = \mathrm{GL}_N(\mathbb{Z})$ is an arithmetic group. Moreover, the monodromy is a product of irreducible lattices, each of which is a non co-compact arithmetic group and has $\mathbb{Q}$-rank at least two.*

Remark 1. The group $G = \mathbb{Z}/d\mathbb{Z}$, viewed as the group of d-th roots of unity, operates on each of the curves X_a^* for varying a and hence acts on the first cohomology $H^1(X_a^*,\mathbb{Z})$; therefore, one may view the first cohomology group of X_a^* as a module over the group algebra $\mathbb{Z}[G] = \mathbb{Z}[q]/(q^d-1)$. The action of G commutes with the monodromy action of the braid group, and therefore, the monodromy group lies in the space of endomorphisms of $H^1(X_a^*,\mathbb{Z})$ which are $\mathbb{Z}[G]$ module maps. Moreover, the monodromy group preserves the intersection form $(\alpha,\beta) \mapsto \alpha \wedge \beta$ on $H^1(X_a^*,\mathbb{Z})$ which extends as a Hermitian form on $V = H^1(X_a^*,\mathbb{C})$ given by $(\alpha,\beta) \mapsto \alpha \wedge \overline{\beta}$. Therefore, the monodromy lies in the unitary group of this Hermitian form and preserves the eigenspaces V_η (and hence the sum $W_\eta = V_\eta \oplus V_{\overline{\eta}}$) of the group G. Consequently, W_η is a Hermitian space and the monodromy representation restricted to W_η has its image in a unitary group of the form $U(r,s)$ with r,s depending on η. Since the cohomology group $H^1(X_a^*,\mathbb{C})$ is a direct sum of the spaces W_η, it follows that the image of the monodromy group lies in a product of the $U(r,s)$.

The image of Γ in the individual $U(r,s)$ may not be discrete, but Γ as a subgroup of the product will be discrete since it preserves the integral lattice $H^1(X_a^*,\mathbb{Z})$.

Remark 2. The arithmetic group is specified (up to finite index) in Proposition 24 in Section 7. It is a little complicated to describe when $n+1$ and d are not coprime, but Proposition 24 shows that the group of real points of the Zariski closure of the monodromy is a product of unitary groups $U(r,s)$.

Remark 3. If $n+1 \leq d$, then the group of integral points of the Zariski closure of the monodromy is a product of irreducible arithmetic lattices (the integral points of the Zariski closure are as described in Proposition 24), some of which form *co-compact* lattices of their real Zariski closures. The Zariski closure can in fact be shown to be a product of unitary groups of suitable Hermitian forms over certain totally real number fields, and one of these Hermitian forms is definite at one of the real completions of the number field. We give a more detailed analysis of the Hermitian form later.

A result of A'Campo [A'C87] says that Theorem 1 holds even when $d=2$. In the proof of Theorem 1, we use the fact that a certain central element in B_{n+1} acts by a *nontrivial* scalar on the Burau representation if n is of the form $kd-2$ in Lemma 17; it is here that we need that $d \geq 3$. The proof can be slightly modified to extend to the case $d=2$ (see the remark following Lemma 17), but we will not do so here.

Theorem 1 answers a question raised in [McM13] (see Question 11.1 in [McM13]) in the affirmative when $n \geq 2d$. When $n \leq d-2$, the monodromy is, in some cases, *not arithmetic*, as is shown by the examples of Deligne-Mostow; cf. the example of $d=18$ and $n=3$ of Corollary (11.8) of [McM13].

In a different direction ([ACT02]), the arithmeticity of the image of the braid group of type E_6 into $U(4,1)$ is proved; in [AH10] representations of the braid group on the homology of *noncyclic* coverings are considered. Arithmeticity results for cyclic coverings of compact surfaces are proved in [Loo97].

The monodromy representation of the braid group B_{n+1} considered in Theorem 1 is closely related to the reduced Burau representation of the group B_{n+1}. (See Section 7 for details.) Theorem 1 is deduced from the arithmeticity of the images of the Burau representation of the braid group B_{n+1} at d-th roots of unity (analogously, a more general result, namely Theorem 26, is deduced — in Section 9 — from the arithmeticity of the images of the Gassner representation of the pure braid group P_{n+1} evaluated at d-th roots of unity). In the rest of the introduction, we concentrate only on the Burau case; the case of the Gassner representation is much more involved and we postpone dealing with it to a future occasion.

1.1. *The braid group and the Burau representation.*

1.1.1. *Definition.* The braid group B_{n+1} on $(n+1)$-strands is the free group on n generators $s_1, s_2, \ldots, s_n$ modulo the relations

$$s_j s_k = s_k s_j \ (\mid j-k \mid \geq 2) \quad \text{and} \quad s_j s_k s_j = s_k s_j s_k \ (\mid j-k \mid = 1).$$

1.1.2. *The reduced Burau representations* ρ_n. Let $R = \mathbb{Z}[q, q^{-1}]$ be the Laurent polynomial ring in the variable q with integral coefficients. Let $M = R^n$ be the standard free R-module of rank n with standard generators $e_1, e_2, \ldots, e_n$. For each j, define the operator $T_j \in \mathrm{End}_R(M)$ by the formulae

$$T_j(e_j) = -qe_j, \quad T_j(e_{j-1}) = e_{j-1} + qe_j, \quad T_j(e_{j+1}) = e_{j+1} + e_j,$$

and

$$T_j(e_k) = e_k \ (\mid k-j \mid \geq 2).$$

In the above formulae, we do not attach any meaning to $T_1(e_0)$. Similarly $T_n(e_{n+1})$ is left undefined. The map $s_j \mapsto T_j$ defines a representation $\rho_n : B_{n+1} \to \mathrm{GL}_n(R)$. Denote by Γ_n the image of ρ_n. The representation ρ_n is the reduced *Burau representation in degree* n ([Bir74]).

1.1.3. *A Hermitian form on* R^n. The ring $R = \mathbb{Z}[q, q^{-1}]$ has an involution $f \mapsto \overline{f}$ given by $\overline{f}(q) = f(q^{-1})$. The sub-ring S of invariants in R under this involution is clearly $\mathbb{Z}[q + q^{-1}]$.

There is a unique map $h : R^n \times R^n \to R$, which is a bilinear map of S-modules, so that for all $v, w \in R^n$ and all $\lambda, \mu \in R$, we have

$$\overline{h(v,w)} = h(w,v), \quad h(\lambda v, \mu w) = \lambda \overline{\mu} h(v,w),$$

and

$$h(e_j, e_k) = 0 \quad (\mid j-k \mid \geq 2),$$

$$h(e_j, e_{j+1}) = -(q+1), \quad h(e_j, e_j) = \frac{(q+1)^2}{q}.$$

We denote this form by $h = h_n$. (When n is fixed, we drop the subscript, and write h.) Then Γ_n preserves the Hermitian form h on R^n. We can then talk of the unitary group of the Hermitian form h.

For a detailed description of a unitary group as an algebraic group defined over a field K, see the beginning of Section 3. The unitary group $U(h)$ of the Hermitian form h is an algebraic group scheme defined over S and

$$U(h)(S) = \{g \in \mathrm{GL}_n(R) : h(gv, gw) = h(v,w) \ \forall v, w \in R^n\}.$$

More generally, for any commutative S algebra A, $U(h)(A)$ is the group

$$U(h)(A) = \{g \in \mathrm{GL}_n(R \otimes_S A); h(gv, gw) = h(v,w) \ \forall v, w \in R^n \otimes_S A\}.$$

Remark 4. This Hermitian form h is essentially (up to a scalar multiple and equivalence of Hermitian forms) the one constructed by Squier [Squ84] where he uses a form with coefficients in a quadratic extension $R' = \mathbb{Z}[\sqrt{q}, \sqrt{q}^{-1}]$ of R. We have written it in this form since we need an algebraic group defined over S and not over R.

It is customary to use the notation $U(R, h)$ in place of $U(h)$ to denote a unitary group (see [PR94, §2.3.3]) in order to specify the quadratic extension R/S with respect to which the Hermitian form h is defined. Since our quadratic extension is fixed, we have used $U(h)$ to avoid complicating the notation.

1.2. *The Burau representations $\rho_n(d)$ at d-th roots of unity.* If $\mathfrak{a} \subset R$ is an ideal stable under the involution $f \mapsto \overline{f}$ and $A = R/\mathfrak{a}$ is the quotient ring, then on the A-module A^n we get a corresponding Hermitian form h_A and a corresponding representation $\rho_n(A) : B_{n+1} \to \mathrm{GL}_n(A)$, which maps B_{n+1} into $U(h_A)(B)$ where B is the quotient ring $S/\mathfrak{a} \cap S$.

We can take $\mathfrak{a}$ to be the principal ideal in R generated by $\Phi_d(q)$, where $\Phi_d(q)$ denotes the d-th cyclotomic polynomial in q. Then the quotient $R_d = R/\mathfrak{a}$ is an integral domain (the ring of integers in the d-th cyclotomic extension E_d of $\mathbb{Q}$). The reduction modulo the ideal $\mathfrak{a}$ of the representation ρ_n yields a representation $\rho_n(d)$ of the braid group B_{n+1}. This is referred to as the representation obtained by evaluating the representation ρ_n at (*all the*) primitive d-th roots of unity.

Note that there is no preferred embedding of the cyclotomic field $E_d = \mathbb{Q}[q]/(\Phi_d(q))$ into the field $\mathbb{C}$ of complex numbers since there is no preferred choice of a primitive d-th root of unity in $\mathbb{C}$. We will therefore not consider E_d as a sub-field of $\mathbb{C}$ but as being naturally embedded in the product $\prod_\mu \mathbb{C}$, where the product is over all the primitive d-th roots μ of unity. (The map into the product is obtained by evaluating q at *all* the primitive d-th roots of unity.)

Denote by $\Gamma_n(d)$ the image of the representation $\rho_n(d)$. The image goes into the group $U(h)(O_K)$ where $K = K_d$ is the (totally real) sub-field of E_d invariant under the involution $f \mapsto \overline{f}$: $K = \mathbb{Q}(2\cos(\frac{2\pi}{d}))$ and O_K is the ring of integers in K. We will consider arithmetic subgroups of (i.e., subgroups which have finite index in) $U(h)(O_K)$. (We refer to Section 2.2 for a discussion on why these are arithmetic groups in the sense of [GS75].)

Consider the group $\Gamma_n(d) \subset U(h)(O_K)$. The ambient Lie group in which $U(h)(O_K)$ is naturally a lattice (see the end of Section 2.2) is the product group $G_\infty = \prod_{v|\infty} U(h)(K_v)$, where the product runs through all the archimedean completions K_v of K. Since K is totally real, K_v is isomorphic to $\mathbb{R}$ for each v. The form h, however, may be different for different real embeddings of K. When h is nondegenerate, there exist nonnegative integers r_v and s_v with

$r_v + s_v = n$ such that the unitary group $U(h)(K_v)$ is isomorphic to $U(r_v, s_v)$ as an algebraic group over $\mathbb{R}$. (When h is degenerate, the unitary group $U(h)(K_v)$ has a unipotent radical and the quotient by the unipotent radical is of the form $U(r_v, s_v)$ with $r_v + s_v \leq n - 1$.) In the course of the proof of arithmeticity of monodromy, we never need to use the ambient group G_∞; we work directly with the arithmetic group $G(O_K)$ and the monodromy group $\Gamma \subset G(O_K)$. For these reasons, we do not specify the integers r_v, s_v and the ambient Lie group G_∞.

1.2.1. *Statement of results.* The main result of the paper is

THEOREM 2. *If $d \geq 3$ and $n \geq 2d$, then the image $\Gamma_n(d)$ of the Braid group B_{n+1} under the reduced Burau representation ρ_n evaluated at* all the *primitive d-th roots of unity — namely the image of representation $\rho_n(d) : B_{n+1} \to \mathrm{GL}_n(\mathbb{Z}[q, q^{-1}]/(\Phi_d(q)))$ — is an arithmetic group.*

More precisely, if h is the Hermitian form on A^n which $\Gamma_n(d)$ preserves, then $\Gamma_n(d)$ is a subgroup of finite index in $U(h)(O_K)$, where $K = \mathbb{Q}(\cos(\frac{2\pi}{d}))$ is the totally real sub-field of the d-th cyclotomic extension of $\mathbb{Q}$.

These arithmetic groups are of $\mathbb{Q}$-rank at least two and, in particular, are not co-compact lattices.

We now take $d = 3, 4, 6$. In these cases, the d-th cyclotomic extension $E_d = \mathbb{Q}(e^{2\pi i/d})$ is an imaginary quadratic extension of $\mathbb{Q}$ and the totally real sub-field $K_d = \mathbb{Q}(\cos(\frac{2\pi}{d}))$ is the field $\mathbb{Q}$ of rationals, $O_d = \mathbb{Z}$ and $\Gamma \subset U(h_n)(\mathbb{Z})$. Combining Theorem 2 with the results of Deligne-Mostow ([DM86], [McM13]) we will prove

THEOREM 3. *If $d = 3, 4, 6$, then* **for all n**, *the image of the Braid group B_{n+1} under the representation ρ_n evaluated at a primitive d-th root of unity is an arithmetic subgroup. More precisely, the image of $\rho_n(d)$ is an arithmetic subgroup of the integral unitary group $U(h)(\mathbb{Z})$.*

We refer to Section 6 for a proof of Theorem 3.

Now consider the ring $A = \mathbb{Z}[q, q^{-1}]/(q^d - 1)$, where $R = \mathbb{Z}[q, q^{-1}]$ as before. The free A module A^n of rank n may be viewed, in particular, as a free Abelian group of rank nd, and $\mathrm{GL}_n(A)$ can be viewed as a subgroup of $\mathrm{GL}_{nd}(\mathbb{Z})$. We say that a subgroup $\Gamma \subset \mathrm{GL}_n(A)$ is arithmetic if it has finite index in its integral Zariski closure in $\mathrm{GL}_{nd}(\mathbb{Z})$. A theorem of [A'C87] and Theorem 2 together imply the following:

THEOREM 4. *Consider the Burau representation*

$$\rho : B_{n+1} \to \mathrm{GL}_n(\mathbb{Z}[q, q^{-1}]/(q^d - 1)).$$

Then the image of ρ is an arithmetic group for all $d \geq 2$ and $n \geq 2d$.

1.3. *Description of the proof.* The proof of Theorem 2 is by showing that for $n \geq 2d$, the image $\Gamma_n(d)$ contains a large number of unipotent elements. (Precisely, $\Gamma_n(d)$ contains an arithmetic subgroup of the unipotent radical of a parabolic $\mathbb{Q}$-subgroup.) By using results of Bass-Milnor-Serre and Tits ([BMS67], [Tit76]) and their extensions to other groups ([Rag92], [Vas73], [Ven94]) on unipotent generators for noncocompact arithmetic groups of $\mathbb{R}$-rank at least two, we show (in Section 5) that such groups are arithmetic if $n \geq 2d$.

The proof that $\Gamma_n(d)$ contains sufficiently many unipotent elements (see Section 5) is by using induction. We first prove this in the case when $n \geq 2d$ and n is a multiple of d. Then we prove an inductive step that if we can get unipotents for m, then we get unipotents for $m+1$ ($m \geq 2d$). This will then cover all integers $n \geq 2d$.

The construction of sufficiently many unipotent elements is especially easy to describe when the representation is the Burau representation of B_{n+1} at d-th roots of unity and $n = 2d$ (or, more generally, when $n = kd$ is a multiple of d, with $k \geq 2$; see Section 4.5). We will exploit the fact that the representation $\rho_{2d-1}(d)$ is not irreducible but contains a nonzero invariant vector (see Proposition 16). Let s_1 be as before. Denote by Δ' the product element

$$\Delta' = (s_2 s_3 \cdots s_n)(s_2 s_3 \cdots s_{n-1}) \cdots (s_2 s_3)(s_2).$$

It can be shown that Δ'^2 is central in B'_n, the braid group generated by $s_2, s_3, \ldots, s_n$. Form the commutator $u = [s_1, (\Delta')^2]$. Consider the group $U \subset B_{n+1}$ generated by conjugates of u of the form $\{huh^{-1} : h \in B'_n\}$. We show (in Section 4.5) that the image of this group U under the Burau representation at d-th rots of unity is an arithmetic subgroup of the unipotent radical of a (maximal) parabolic subgroup of the unitary group $U(h)$. This is enough to prove that the image of B_{n+1} under $\rho_n(d)$ is arithmetic, by the criteria of Section 2.

In Section 7, we derive Theorem 1 from Theorem 2, by establishing the precise relationship between the monodromy representation of Theorem 1 and the Burau representation; although this connection is essentially well known (cf. [McM13, Th. 5.5]), we will give a more precise description of the connection in Section 7.

1.4. *Organisation of the paper.* This paper is organised as follows. In Section 2, we recall some basic notions from algebraic groups and state a criterion due to Bass-Milnor-Serre and others on unipotent generators for higher rank nonuniform lattices. In Section 3, we will apply this criterion to certain integral unitary groups.

The main section of the paper is Section 4, where we show that the image of the braid group B_{n+1} at a primitive d-th root of unity contains many unipotent

elements (more precisely, contains an arithmetic subgroup of the unipotent radical of a parabolic subgroup defined over the field K_d). The criteria of Section 3 then imply the arithmeticity when $n \geq 2d$ for all d.

In Section 8, we first consider (in Section 8.1) complex reflection groups corresponding to root systems of type A and show the arithmeticity of the images of the corresponding Artin groups $A_n(q)$ (see Section 8 for references to definitions), where q is a primitive d-th root of unity and $n \geq 2d$; the image of the group $A_n(q)$ turns out to be the same as the image of $\Gamma_n(d)$ into one of the factors of $U(h)(K \otimes \mathbb{R})$. Hence the arithmeticity of the image of $A_n(q)$ will be shown to be an immediate consequence of Theorem 2. This answers Question 5.6 in [McM13] in many cases.

In Section 8.2, we show that Theorem 2 implies the arithmeticity of the monodromy of certain one variable hypergeometric functions of type ${}_nF_{n-1}$, in some special cases of the parameters. The point here is that arithmeticity can be proved for an *infinite family* of parameters associated to the hypergeometric equations ${}_nF_{n-1}$.

Acknowledgements. I am very grateful to Madhav Nori for mentioning to me this problem of arithmeticity of the image of the braid group (Theorem 2); his formulation of the problem in purely algebraic terms was most helpful. I also thank him for generously sharing his insights on many of the questions addressed here and for very helpful remarks on many of the proofs and intermediate results (especially the remark that an earlier proof for the arithmeticity of the image of the Burau representation should also go through for the Gassner representation).

I thank Peter Sarnak for mentioning the monodromy problem of Section 8.2 and for very interesting discusions on the material of Section 8.2. I thank Curtis Mcmullen for helpful communications concerning Question 5.6 of [McM13], and pointing out some corrections on the material in Section 8.1. I extend to the referee my hearty thanks for a careful reading of the manuscript and for pointing out numerous corrections and suggestions for improving the exposition of the paper.

The support of the J. C. Bose fellowship for the period 2008–2013 is gratefully acknowledged.

2. **Algebraic groups**

For the facts on algebraic groups stated in this section, we refer to [BT65].

2.1. *Examples of algebraic groups.* If K is a number field and $G \subset \mathrm{GL}_n$ is a subgroup which is the set of zeroes of a collection of polynomials in the matrix entries of GL_n, such that the coefficients of these polynomials lie in K, then G is said to be an algebraic group defined over K.

For example, the groups SL_n and Sp_{2g} are algebraic groups defined over K. If E/K is a quadratic extension and $H : E^n \times E^n \to E$ is a K bilinear form which is Hermitian with respect to the nontrivial automorphism of E/K, then the unitary group of the Hermitian form h is an algebraic group defined over K.

2.2. *Arithmetic groups.* Let $\mathcal{G} \subset \mathrm{GL}_N$ be a linear algebraic group defined over $\mathbb{Q}$. A subgroup $\Gamma \subset \mathcal{G}(\mathbb{Z})$ is said to be an *arithmetic subgroup of* $\mathcal{G}(\mathbb{Q})$ if Γ has finite index in the intersection $\mathcal{G}(\mathbb{Z}) = \mathcal{G} \cap \mathrm{GL}_N(\mathbb{Z})$. (See [Rag72, Chap. X, Def. (10.12), p. 165] or [PR94, Chap. 4, (4.1), p. 171].) By a theorem of Borel and Harish-Chandra, Γ is a lattice (a discrete subgroup with finite covolume) in the group $\mathcal{G}(\mathbb{R})$ of real points of $\mathcal{G}$ provided the identity component $\mathcal{G}^0$ of the group $\mathcal{G}$ does not have nontrivial homomorphisms into the multiplicative group $\mathbb{G}_m$ defined over $\mathbb{Q}$. (For a reference, see [PR94, Th. 4.13, p. 213].) It is also a consequence of the result of Borel and Harish-Chandra that $\mathcal{G}(\mathbb{Z})$ is a co-compact lattice if and only if $\mathbb{Q}$-rank $(\mathcal{G}) = 0$. (See Section 2.3 for the notion of $\mathbb{Q}$-rank.)

Let O_K denote the ring of integers in K. The group $G(O_K)$ is by definition, the intersection $\mathrm{GL}_n(O_K) \cap G$. A subgroup $\Gamma \subset G(K)$ is said to be arithmetic if the intersection $\Gamma \cap G(O_K)$ has finite index in Γ and in $G(O_K)$. This definition appears to be different from the one given in the preceding paragraph. But these two definitions are equivalent. This is shown by replacing G by the Weil restriction of scalars $\mathcal{G} = R_{K/\mathbb{Q}}G$. (For a reference, see [PR94, 2.1.2, p. 49].) The theory of Weil restriction of scalars says that there exists a linear algebraic group $\mathcal{G}$ defined over $\mathbb{Q}$ (and unique up to isomorphism) with the following property: for any commutative $\mathbb{Q}$-algebra A, the group $\mathcal{G}(A)$ is naturally isomorphic to $G(K \otimes_{\mathbb{Q}} A)$, the group of $K \otimes_{\mathbb{Q}} A$-rational points of the K-algebraic group G.

Definition 1. The group $\mathcal{G}$ is called the Weil restriction of scalars from K to $\mathbb{Q}$, of the group G. It is denoted $\mathcal{G} = R_{K/\mathbb{Q}}(G)$.

We then have $R_{K/\mathbb{Q}}G(\mathbb{Z}) \simeq G(O_K)$, where the symbol $\simeq$ means that there is equality up to subgroups of finite index. (The two groups are *commensurable*.) Moreover, $\mathcal{G}(\mathbb{R}) \simeq \prod_{v|\infty} G(K_v)$, where the product is over all the inequivalent archimedean completions of K (see [PR94, 2.1.2, pp. 50–51]). Thus, $G(O_K)$ is a lattice in the ambient Lie group $\prod G(K_v)$ where the product is over all the inequivalent nonarchimedean completions K_v of K. We recall that any number field has r_1 completions K_v which are isomorphic to $\mathbb{R}$ and up to complex conjugation, r_2 completions K_v which are isomorphic to $\mathbb{C}$ such that $r_1 + 2r_2$ is the degree of the extension K over $\mathbb{Q}$.

We will have occasion to deal with images of arithmetic groups under morphisms of $\mathbb{Q}$-algebraic groups (see Section 7.7). In particular, we will use the following result. Let $f : \mathcal{G} \to \mathcal{G}'$ be a morphism of algebraic groups defined over $\mathbb{Q}$. This induces a homomorphism, also denoted f, from $\mathcal{G}(\mathbb{Q})$ into $\mathcal{G}'(\mathbb{Q})$. It is elementary that if $\Gamma \subset \mathcal{G}(\mathbb{Z})$ is a suitable subgroup (a suitable "congruence subgroup") of finite index, then $f(\Gamma)$ lies in $\mathcal{G}'(\mathbb{Z})$. For a proof of the following lemma, see Corollary (10.14) of [Rag72].

LEMMA 5. *The image of* Γ *under* f *is an arithmetic subgroup of* $\mathcal{G}'(\mathbb{Z})$.

Let $\theta : V \to V'$ be a linear map of $\mathbb{Q}$-vector spaces and $\rho : \Delta \to \mathrm{GL}(V)$ be a representation of a group Δ. Then the composite $\theta \circ \rho$ is a representation of Δ. The following is immediate from Lemma 5.

PROPOSITION 6. *If the image of* ρ *is an arithmetic subgroup of* $\mathrm{GL}(V)$, *then the image of the composite* $\theta \circ \rho$ *is an arithmetic subgroup of* $\mathrm{GL}(V')$.

2.3. *K-rank.* In this subsection, we define the notion of the K-rank and $\mathbb{Q}$-rank of a linear algebraic group.

Definition 2. An algebraic group G is said to be K-isotropic if there exists an injective morphism $\mathbb{G}_m^r \to G$ of linear algebraic groups defined over K for some $r \geq 1$. The r-fold product $\mathbb{G}_m^r$ is called the K-split torus of dimension r and the embedding is called a K-embedding. The K-rank of G is by definition the *maximum*, call it r, of the dimensions of K-split tori which are K-embedded in G. Let T be a K-split torus of dimension r which is K-embedded in G. Then T is called a maximal K-split torus. It is known that all maximal K-split tori are conjugate under the group $G(K)$.

For example, for any K, one can compute the K-rank of the groups SL_n and Sp_{2g}: the K-rank of SL_n is $n-1$; the K-rank of Sp_{2g} is g. The K-rank may depend on K: if D is a quaternionic division algebra over $\mathbb{Q}$, let $G = \mathrm{SL}_2(D)$ be the algebraic group defined over $\mathbb{Q}$. Then $\mathbb{Q}$-rank $(G) = 1$; if $K \subset D$ is a quadratic extension of $\mathbb{Q}$, then as an algebraic group over K, G is isomorphic to SL_4 and K-rank $(G) = 3$.

It follows from definitions that K-rank (G)=$\mathbb{Q}$-rank $(\mathcal{G})$, where $\mathcal{G}$ is the Weil restriction of scalars from K to $\mathbb{Q}$.

2.4. *Parabolic subgroups.* Suppose now that $G \subset \mathrm{GL}_n$ is an algebraic group defined over a number field K; embed K in $\mathbb{C}$, and suppose that the Lie algebra of $G(\mathbb{C})$ is a simple Lie algebra over $\mathbb{C}$. Then G is said to be *absolutely almost simple.*

An algebraic subgroup $P \subset G$ is said to be a parabolic subgroup defined over K if P is defined over K and the quotient G/P is a projective variety.

For example, a subgroup $P \subset \mathrm{GL}_n = \mathrm{GL}(V)$ is a parabolic subgroup if and only if it is the subgroup preserving a partial flag

$$\{0\} \subset W_1 \subset W_2 \subset \cdots \subset W_{r-1} \subset V,$$

where W_i form a sequence of subspaces of V with $W_i \subset W_{i+1}$.

Let G be an absolutely almost simple algebraic group defined over K. The group G has positive K-rank if and only if G contains a proper parabolic subgroup P defined over K. Suppose that $r = K$-rank $(G) \geq 1$ and T a maximal K-split torus in G. Then there exists a parabolic K-subgroup P containing T. Furthermore, there exists a nontrivial maximal unipotent normal subgroup U of P, called the unipotent radical of P. The Lie algebra of U is stable under the action of the group T and splits into character spaces for the adjoint action of T.

The structure theory of parabolic subgroups says that there exists a parabolic subgroup P^- defined over K containing T, with a unipotent radical U^- such that the characters of T on $\mathrm{Lie}(U^-)$ are the inverses of the characters of T on $\mathrm{Lie}(U)$. The group P^- is said to be *opposite* to P, and U^- is said to be *opposed* to U. The intersection $M = P \cap P^-$ is called a Levi subgroup of P, and we have the Levi decomposition $P = MU$. The group M normalises both U and U^-.

A K-parabolic subgroup P_0 containing T is *minimal* if it is of the smallest dimension among the K-parabolic subgroups containing T. If $P \supset P_0$, then we have the (reverse) inclusion of the unipotent radicals $U \subset U_0$. There exists a minimal parabolic subgroup P_0^- opposed to P_0, with unipotent radical U_0^-.

2.5. *The real rank.* Suppose that G is an absolutely almost simple algebraic group defined over a number field K. Write G_∞ for the product group $G_\infty = \prod_{v \text{ arch}} G(K_v)$ (which is a real semi-simple group), where v runs over all the archimedean completions of K; we write

$$\infty\text{-rank}(G) = \mathbb{R}\text{-rank}(G_\infty) = \sum_{v \text{ arch}} K_v\text{-rank}(G),$$

and we call this the *real rank* of G_∞.

2.6. *A criterion for arithmeticity.* Bass, Milnor and Serre proved that for any $N \geq 1$, the N-th powers of the upper and lower triangular unipotent matrices in $\mathrm{SL}_n(\mathbb{Z})$ generate a subgroup of finite index in $\mathrm{SL}_n(\mathbb{Z})$ for $n \geq 3$. A similar result holds for $\mathrm{Sp}_{2g}(\mathbb{Z})$. In this subsection, we describe an analogous result for all higher $\mathbb{R}$-rank groups.

The following result is due to many people: for $G = \mathrm{SL}_n$ $(n \geq 3)$ or Sp_{2g} $(g \geq 2)$, this is due to Bass, Milnor and Serre [BMS67]; when G is split over K (i.e., when a maximal K -split torus is also a a maximal $\mathbb{C}$-split torus), to Tits [Tit76] and for classical groups G with K-rank ≥ 2 to Vaserstein [Vas73]. The case of a general G is handled in Raghunathan [Rag92] and [Ven94].

THEOREM 7. *Let G be an absolutely almost simple algebraic group defined over a number field K. Assume that K-rank$(G) \geq 1$, $\mathbb{R}$-rank$(G_\infty) \geq 2$ and that P_0, P_0^- are minimal parabolic K-subgroups of G with unipotent radicals U_0 and U_0^-. Then the following hold*:

(1) *For every integer $N \geq 1$, let Δ_N be the subgroup of $G(O_K)$ generated by N-th powers of the elements in $U_0(O_K)$ and $U_0^-(O_K)$. Then Δ_N has finite index in $G(O_K)$.*
(2) *If $\Delta'_N \subset \Delta_N$ is an infinite normal subgroup, then Δ'_N also has finite index in $G(O_K)$.*

The above theorem says that the integral points of two *maximal* opposing unipotent subgroups (i.e., the unipotent radicals of two minimal parabolic K-subgroups) generate a finite index subgroup in $G(O_K)$ if the ∞-rank is at least two. We need a strengthening of this, where we assume only that the unipotent radicals which are not necessarily maximal, of two opposing parabolic subgroups are involved. This is the following:

COROLLARY 1. *Suppose G is absolutely almost simple and K-rank$(G) \geq 2$. Let P and P^- be two opposite parabolic subgroups containing a maximal K-split torus, and let U, U^- be their unipotent radicals. For any integer $N \geq 1$, the group $\Delta_N(P^\pm)$ generated by N-th powers of $U(O_K)$ and $U^-(O_K)$ is of finite index in $G(O_K)$.*

Proof. In the notation above, let $M = P \cap P^-$. Then $M(O_K)$ normalises $U(O_K)$ and $U^-(O_K)$ and hence normalises the group $\Delta_N(P)$. Now the group generated by $M(O_K)$ and $\Delta_N(P^\pm)$ contains $(U_0 \cap M)(O_K)$ and $(U_0 \cap U)(O_K)^N = U(O_K)^N$; the decomposition $P = MU$ shows that $P(O_K) = M(O_K)U(O_K)$ and hence $U_0(O_K) = (U_0 \cap M)(O_K)U(O_K)$. (All these equalities are true only up to finite index; the decomposition $U_0 = (U_0 \cap M)U$ of algebraic groups is defined over the *field* K but not over the integers O_K. This implies that there are finite index subgroups $U_0' \subset U_0(O_K)$, $(U_0 \cap M)' \subset (U_0 \cap M)(O_K)$ and $U' \subset U(O_K)$ such that the product decomposition $U_0' = (U_0 \cap M)'U'$ holds for the smaller groups.)

Therefore the group generated by $M(O_K)$ and $\Delta_N(P^\pm)$ contains N-th powers of elements of $U_0(O_K)$ and $U_0^-(O_K)$. Consequently, the group $\Delta_N(P^\pm)$ is normalised by Δ_N. By the second part of the above theorem, $\Delta_N(P)$ is of finite index in $G(O_K)$. □

Remark 5. The second part of Theorem 7 is true for any irreducible lattice in a real semi-simple group of real rank at least two. (This is the normal subgroup theorem of Margulis.)

In the next section, we will state a special case of this corollary for certain unitary groups.

2.7. *Subgroups of products of higher rank groups.* In Section 5, we will prove the arithmeticity of the image of the braid group in a group of the form $U(h)(\mathbb{Z}[q]/(q^d-1))$. The latter is a product of the groups $U(h)(O_e)$ for certain rings of integers O_e. To deal with this case, we now prove a lemma which is a simple consequence of the super-rigidity theorem of Margulis.

LEMMA 8. *Suppose that K_e are number fields for each element e in a finite indexing set X. Suppose that G_e is an absolutely almost simple semi-simple algebraic group defined over K_e, and suppose that ∞-rank$(G_e) \geq 2$ for all $e \in X$. Suppose that $\Gamma \subset \prod G_e(O_e)$ is a subgroup such that the image of its projection to each $G_e(O_e)$ has finite index in $G_e(O_e)$. Assume, in addition, that either K_e and K_f are nonisomorphic or else, if K_e and K_f are isomorphic, the groups G_e and G_f (which may be thought of as groups defined over the same field K_e) are not isomorphic over $K_e = K_f$.*

Under these assumptions, the group Γ has finite index in the product $\prod_{e\in X} G_e(O_e)$.

Proof. Replacing the arithmetic groups $G_e(O_e)$ by subgroups of finite index, we may assume that these are torsion free and hence that Γ is torsion free. We prove the lemma by induction on the number of factors. Fix an element $p \in X$. By induction, the projection of Γ in the product $\prod_{e\in X, e\neq p} G_e(O_e)$ under the projection map $\mathrm{pr} : \prod_{e\in X} G_e(O_e) \to \prod_{e\in X, e\neq p} G_e(O_e)$ has finite index. Suppose N_p is kernel of restriction of this projection map to Γ. We will show that the kernel N_p cannot be trivial.

If N_p is trivial, then Γ projects injectively into the product of the groups $G_e(O_e)$ with $e \neq p$: $\Gamma \subset \prod_{e\in X, e\neq p} G_e(O_e)$ (and by the induction assumption, its image has finite index). Therefore, Γ is an arithmetic subgroup of the higher rank lattice $\prod_{e\neq p} G_e(O_e)$ and has a nontrivial representation (projection to the p-th factor) onto a finite index subgroup of the arithmetic group $G_p(O_p)$; replacing the image of Γ by a smaller subgroup of finite index if necessary, we may assume that the image of Γ in the "away from p" product is a product of finite index subgroups of $G_e(O_e)$ (with $e \neq p$). The Margulis normal subgroup theorem (applied to the image of Γ in $G_e(O_e)$) then implies that only one of the factors in this product maps isomorphically onto its image in $G_p(O_p)$ and that the other factors map to the identity. This contradicts the Margulis super-rigidity (or Mostow rigidity): we have an isomorphism of a finite index subgroup of $G_e(O_e)$ with a finite index subgroup of $G_p(O_p)$. Such an isomorphism, by the super-rigidity theorem, is induced by first an isomorphism of K_e with K_p and an isomorphism of G_e with G_p as groups over $K_e = K_p$. This contradicts our assumptions and therefore, the kernel N_p cannot be trivial.

Since the kernel N_p is nontrivial, it is infinite since Γ is assumed to be torsion free. The conjugation action of Γ on the p-th factor $G_p(O_p)$ factors

through its projection to the p-th factor; but the p-th projection map has image of finite index, and hence N_p is normalised by a subgroup of finite index in $G_p(O_p)$; by the Margulis normal subgroup theorem, N_p has finite index in $G_p(O_p)$; therefore, Γ maps onto a subgroup of finite index in the product of the "away from p" factors, and intersects the p-th factor in a subgroup of finite index. Therefore, Γ has finite index. □

Remark 6. A related result is proved in [GL09] and also in [Loo97]. At the time of writing the present paper, we were unaware of these papers. Moreover, the proof here is different from the cited papers.

3. **Unitary groups**

Notation. Suppose that E/K is a quadratic extension. Write $E = K \oplus K\sqrt{\alpha}$ for some nonsquare element α in K, and given $z \in E$, write $z = x + y\sqrt{\alpha}$ accordingly. Then x, y are called the "real" and "imaginary" parts, respectively. Denote by $\overline{z}$ the element $x - \sqrt{\alpha}y$.

Given $n \geq 1$, the vector space E^n may be viewed as a $2n$-dimensional vector space over K. Suppose $h : E^n \times E^n \to E$ is a map which is K-bilinear such that for all $v, w \in E^n$, we have

$$h(v, w) = \overline{h}(w, v).$$

Then h is said to be a Hermitian form with respect to E/K. By definition, the elements of the unitary group $U(h)$ satisfy the property that they commute with scalar multiplication by elements of E, viewed as K-linear endomorphisms of E^n; further, they preserve the real and imaginary parts of h. These properties characterise the elements of $U(h)$, and in this manner, the group $U(h)$ may be viewed as a K-algebraic subgroup of $\mathrm{GL}_K(K^{2n}) = \mathrm{GL}_{2n}(K)$. In particular,

$$U(h)(K) = \{g \in \mathrm{GL}_n(E) \subset \mathrm{GL}_{2n}(K) : h(gv, gw) = h(v, w)\}$$

for all vectors $v, w \in E^n$. More generally, if A is a commutative K algebra, then

$$U(h)(A) = \{g \in \mathrm{GL}_n(E \otimes_K A) : h(gv, gw) = h(v, w)\}$$

for all elements v, w of the E-module $E^n \otimes_K A$.

For example, if K and E are replaced by $\mathbb{R}$ and $\mathbb{C}$ and h is the standard Hermitian form on $\mathbb{C}^n$, then the group of *real* points of the unitary group $U(h)$ are given by the compact group

$$U(h)(\mathbb{R}) = \{g \in \mathrm{GL}_n(\mathbb{C}) : {}^t\overline{g}g = 1\},$$

and the group of *complex* points of the unitary group may easily be seen (from the above description) to be isomorphic to $\mathrm{GL}_n(\mathbb{C})$.

3.1. *Rank of a unitary group.* Let $h_2 : E^2 \times E^2 \to E$ be a Hermitian form with respect to E/K. Suppose that the Hermitian form h_2 can be written as

$$h_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

That is, if v, w are column vectors in E^2 with entries $v = (z_1, z_2)$ and $w = (w_1, w_2)$, then $h_2(v, w) = z_1\overline{w_2} + z_2\overline{w_1}$. Then h is called a *hyperbolic form.* The standard basis of E_2 may be written v, v^*, and the form h_2 is such that $h(v, v) = h(v^*, v^*) = 0$ and $h(v, v^*) = 1$.

Suppose h is a nondegenerate Hermitian form on E^n. Then (E^n, h) can be written as a direct sum of r copies of the hyperbolic form (E^2, h_2) and a form (E^{n-2r}, h_0) which does not represent a zero in E^{n-2r}. Then h_0 is said to be *anisotropic.* Let $U(h)$ be the unitary group of the Hermitian form h. It can be shown that K-rank $(U(h)) = r$.

With respect to this decomposition $h = h_2 \oplus \cdots \oplus h_2 \oplus h_0$, write the standard basis of the j-th copy of (E^2, h_2) as v_j, v_j^*. We may rearrange the basis of E^n in the form

$$v_1, v_2, \ldots, v_r, w_1, \ldots, w_s, v_r^*, \ldots, v_2^*, v_1^*,$$

where $w_1, \ldots, w_s$ is a basis of (E^{n-2r}, h_0). Let $Av_1 \subset W \subset V = E^n$, where W is the E-submodule spanned by

$$v_1, \ldots, v_r, w_1, \ldots, w_s, v_r^*, \ldots, v_2^*.$$

In the terminology of the preceding section, if $n \geq 2$, then $\mathrm{SU}(h)$ is an absolutely almost simple algebraic group defined over K; the subgroup P of $\mathrm{SU}(h)$ which preserves the flag $Ev_1 \subset W \subset V$ is a parabolic subgroup defined over K. Let U be the subgroup of $\mathrm{SU}(h)$ which preserves this flag and acts trivially on successive quotients. Then U is the unipotent radical of P.

The partial flag $Ev^* \subset Ev^* \oplus W \subset V$ defines a parabolic subgroup P^- of $U(h)$, and U^- is the subgroup of P^- which acts trivially on the successive quotients of this flag. This parabolic subgroup P^- is opposite to P, and U^- is its unipotent radical opposed to U, in the sense of Section 2.4.

Corollary 2. *Along with the preceding notation and hypotheses, suppose that $r \geq 2$. Then the group generated by the N-th powers of $U(O_K)$ and $U^-(O_K)$ is an arithmetic subgroup of* $\mathrm{SU}(h)(O_K)$. *The same conclusion holds if the K-rank of* $\mathrm{SU}(h)$ *is* 1 *but ∞-rank* $(\mathrm{SU}(h))$ *is* ≥ 2.

Proof. We have already noted that K-rank $(\mathrm{SU}(h))$ is the number of hyperbolic 2-planes in the decomposition of h. Therefore, the K-rank of $\mathrm{SU}(h)$ is ≥ 2. Then the corollary follows from Corollary 1 of the preceding section.

The second part follows by Theorem 7. (The group has higher real rank but $\mathbb{Q}$-rank one.) $\square$

3.2. *The Heisenberg group and the group P.* Assume now that (V, h) is an $n = m + 1$-dimensional E vector space with a *nondegenerate* Hermitian form h. Assume that there exists a E-vector subspace X of V of codimension two such that h is nondegenerate on X and that there exist isotropic vectors v, v^* in V which are orthogonal to X such that $h(v, v^*) \neq 0$. We have a partial flag

$$0 \subset Ev \subset Ev \oplus X \subset V = Ev \oplus X \oplus Ev^*.$$

The subgroup of the unitary group $U(h)$ of V which preserves this flag and acts trivially on successive quotients is called the Heisenberg group $H(X)$ of X. We write P for the subgroup of $U(h)$ which preserves this flag. It is easily seen that P is a maximal parabolic subgroup of the unitary group $U(h)$ defined over K. The Heisenberg group $H(X)$ is the unipotent radical of P. (We sometimes denote $H(X)$ by U, to be consistent with the notation of the preceding section.) Since we have an orthogonal decomposition $V = X \oplus (Ev \oplus Ev^*)$ with respect to the Hermitian form h, it follows that the unitary group $M = U(h_{|X})$ of the restriction of h to X is the subgroup of $U(h)$ which fixes the vectors v, v^*. We have $P = H(X)M = UM$, and this gives a Levi decomposition of the parabolic subgroup P. Since the Hermitian form h is the same on X and V, we sometimes write $U(X)$ and $U(V)$ in place of $U(h_{|X})$ and $U(h)$.

The direct sum $W = Ev \oplus X$ has the property that the Hermitian form on W is *degenerate* with $W^{\perp} = Ev$. The quotient map $W \to W/Av = X$ preserves the Hermitian structure on both sides since Ev is orthogonal to W. This induces a surjective map $U(W) \to U(X)$ of unitary groups, with kernel U_0, say. Consider the abelian vector group $X^* = \mathrm{Hom}(X, Ev)$. We may view X^* as a vector space over K and hence as the group of K-rational points of a unipotent algebraic group which is isomorphic to U_0: $U_0(K) \simeq X^*$. Hence we refer to U_0 as a vector group. We have a split short exact sequence

$$0 \to U_0 \to U(W) \to U(X) \to 1,$$

and we may write $U(W) = U(X)U_0$. An element α of $U(W)$ may accordingly be written as a pair $\alpha = (g, x)$ with $g \in U(X)$ and $x \in U_0$. If $g \in U(X)$, then g gives a transformation on the vector group U_0 defined by $x \mapsto xg$ (the transpose of g). With this notation, if $\beta = (h, y) \in U(W)$, then

$$\alpha\beta = (gh, xh + y).$$

Therefore, $\alpha^{-1} = (g^{-1}, -xg^{-1})$.

Suppose that $m \in U(X) \subset U(W)$ is of the form $(\lambda, 0)$, which is the multiplication by the scalar λ on X and acting by 0 on v. Given $a, b \in U(h)$, denote by $[a, b]$ the commutator $aba^{-1}b^{-1}$.

LEMMA 9. *If $\alpha = (g, x)$ and $m = (\lambda, 0)$, then the commutator $[\alpha, m]$ is of the form*

$$[\alpha, m] = (1, (1 - \lambda^{-1})xg^{-1}).$$

In particular, if $x \neq 0$ and $\lambda \neq 1$, then the commutator $[\alpha, m]$ is a nonzero element of the vector space U_0.

Recall that the abelian vector group $X^* = \mathrm{Hom}(X, Ev)$ may be viewed is a vector space over K and hence as the group of K-rational points of a unipotent algebraic group U_0: $U_0(K) \simeq X^*$. The nondegenerate Hermitian form h_X on X gives a Hermitian form on X^* as well, which we again denote $h_X = h_{|X^*}$.

The group $U = H(X)$ is nonabelian with centre equal to the one-dimensional vector space $\mathbb{G}_a$ over K, and we have an exact sequence of unipotent K-algebraic groups

$$\{0\} \to \mathbb{G}_a \to U \to U_0 \to \{1\}.$$

This in turn gives a short exact sequence

$$\{0\} \to K \to U(K) \to U_0(K) = X^* \to \{1\}$$

at the level of K-rational points. (We have written $\{0\}$ and $\{1\}$ for the trivial group since one of them is written additively and the other multiplicatively.) Moreover, if $x, y \in U(K)$, and x^*, y^* their images in $U_0(K)$, then the commutator $[x, y]$, as an element of K, is simply the imaginary part of $h(x^*, y^*)$.

Now, P is a semi-direct product of U with $M \simeq P/U$ and M is isomorphic to $U(X)$ as in the preceding. Moreover, the centre $Z = \mathbb{G}_a$ of U is normal in P and secondly the quotient U/Z is isomorphic to U_0. We may write, using the decomposition $P = MU$, an element α of P in the form $\alpha = (g, x)$ with $g \in M$ and $x \in U$. Let $\lambda \in U(X)$ be a scalar transformation.

LEMMA 10. *If $\alpha = (g, x)$ with $x \in U$, x has nonzero image in U_0 (i.e., does not lie in the centre of U), and $m = (\lambda, 0) \in M$, then the commutator $[\alpha, m]$ is a* **noncentral** *element of U.*

The proof is immediate from Lemma 9 since the image of the commutator $[\alpha, m]$ in $U_0 = U/Z$ is already nontrivial by Lemma 9.

We now state another simple observation as a lemma.

LEMMA 11. *If $U \to U_0$ is the quotient map, then a subgroup $N \in U(O_K)$ has finite index if and only if its image N_0 has finite index in $U_0(O_K)$.*

3.3. *An inductive step for integral unitary groups.* In this subsection, we prove a result which will be used in the inductive proof of Theorem 2. This says that a subgroup of the integral unitary group which contains finite index subgroups of smaller integral unitary groups has finite index.

Notation. Let $V = (V, h)$ be a nondegenerate Hermitian space over E such that K-rank$(U(h)) \geq 2$. Let W, W' be codimension one subspaces such that the restriction of h to W, W' and the intersection $W \cap W'$ are all nondegenerate. We denote by U_V the unitary group $U(h)$, and we similarly define $U_W, U_{W'}, U_{W\cap W'}$. If Y is one of the subspaces W, W' and $W \cap W'$, then by the nondegeneracy assumption, we have an orthogonal decomposition $V = Y \oplus Y^{\perp}$. Hence U_Y may be thought of as the subgroup of U_V which acts trivially on $Y^{\perp}$.

Suppose that $\Gamma \subset U_V(O_K)$ is a subgroup such that its intersection with $U_W(O_K)$ has finite index in $U_W(O_K)$ and such that its intersection with $U_{W'}(O_K)$ has finite index in $U_{W'}(O_K)$. Assume further that $W \cap W'$ contains a nonzero isotropic vector v.

LEMMA 12. *With the preceding notation* (*and under the assumption that* K*-rank*$(U(h)) \geq 2$), *the group* Γ *has finite index in* $U_V(O_K)$.

Proof. Since $W \cap W'$ has codimension two in V and h is nondegenerate on $W \cap W'$, it follows that V is the direct sum of $W \cap W'$ and its orthogonal complement $(W \cap W')^{\perp}$ in V. The orthogonal complement is also a nondegenerate unitary space (of dimension two); by assumption, $W \cap W'$ contains an isotropic vector v, say. The nondegeneracy of h on $W \cap W'$ shows that there exists a vector $v^* \in W \cap W'$ such that $h(v, v^*) \neq 0$; by replacing v^* by $v^* + \lambda v$ for a suitable scalar λ if necessary, we may assume that $v^* \in W \cap W'$ is also an isotropic vector. Write $V = (Ev + Ev^*) \oplus X$, an orthogonal decomposition. Consider the filtration

$$0 \subset Ev \subset E \oplus X \subset Ev \oplus X \oplus Ev^* = V.$$

Denote the corresponding integral Heisenberg group (the unipotent subgroup of $U(V)$ which preserves the flag and acts trivially on successive quotients) by $H_V = H(X)(O_K)$. Similarly define the smaller Heisenberg groups $H_W = H(X \cap W)(O_K)$ and $H_{W'} = H(X \cap W')(O_K)$.

By assumption, $H_W \cap \Gamma$ has finite index in H_W; similarly for $H_{W'}$. The two Heisenberg groups generate H_V up to finite index since two distinct vector subspaces of codimension one span the whole space. We thus find that the intersection of Γ with the integral unipotent radical of a parabolic K subgroup $H_V = H(X)(O_K)$ has finite index in H_V.

Similarly, we find a finite index subgroup of an opposite integral unipotent radical which lies in Γ; therefore, Γ is arithmetic, by the Corollary 1 to Theorem 7. □

4. **Properties of the Burau representations ρ_n and $\rho_n(d)$**

4.1. *Notation.* As observed in the introduction, the representation $\rho_n : B_{n+1} \to \mathrm{GL}_n(\mathbb{Z}[q, q^{-1}])$ preserves the Hermitian form

$$h = h_n = \begin{pmatrix} \frac{(q+1)^2}{q} & -(1+q) & 0 & \cdots & \cdots \\ -(1+q^{-1}) & \frac{(q+1)^2}{q} & -(q+1) & \cdots & \cdots \\ 0 & -(1+q^{-1}) & \frac{(q+1)^2}{q} & -(q+1) & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}.$$

(Note that h_{kk} is fixed under the involution $q \mapsto q^{-1}$.) Denote by D_n the determinant of h_n.

LEMMA 13. *The determinant D_n of the matrix h_n is*

$$D_n = \det(h) = \left(\frac{q+1}{q}\right)^n \left(\frac{q^{n+1}-1}{q-1}\right).$$

Proof. Expanding the determinant of h_{n+1} using the first row, we see that

$$D_{n+1} = \frac{(q+1)^2}{q} D_n - (1+q)(1+q^{-1}) D_{n-1}.$$

Now an easy induction implies the lemma. □

4.2. *Nondegeneracy of the representation* $(A^n, \rho_n(d))$. Consider the ring $A = R/(\Phi_d(q)) \subset E = \mathbb{Q}[q]/(\Phi_d(q))$ (q evaluated at *all* the primitive roots of unity). We then have a corresponding Hermitian form on A^n which we again denote by $h_n = h_n(d)$. We will say that elements $v_1, \ldots, v_k$ are basis elements of A^n if there exist vectors $v_{k+1}, \ldots, v_n$ in A^n such that A^n is the free module generated by $v_1, \ldots, v_n$. We have a representation $\rho_n(d) : B_{n+1} \to U(h) \subset \mathrm{GL}_n(A)$ as before.

LEMMA 14. *Let A be as in the preceding. Assume that $d \geq 3$, so that $q \neq \pm 1$. Then*

(1) *The Hermitian form h_n on the module A^n is nondegenerate if and only if n is not congruent to -1 modulo d.*
(2) *If d divides $n+1$, define k by the formula $n = kd-1$. Then the vector*

$$v = e_1 + \left(\frac{q^2-1}{q-1}\right) e_2 + \left(\frac{q^3-1}{q-1}\right) e_3 + \cdots \left(\frac{q^{kd-1}-1}{q-1}\right) e_{kd-1}$$

is a basis vector and generates the null space of the degenerate Hermitian form h in $V_A = A^n$. Moreover, on the quotient module V_A/Av, the form h is nondegenerate.
(3) *The vector v is fixed by the elements s_j under the representation $\rho_n(d)$. We therefore get the "quotient" representation $\overline{\rho_n(d)}$ of B_{n+1} on the quotient V_A/Av which again preserves the (nondegenerate) Hermitian form h on V_A/Av.*

Proof. Part (1) is obvious because of Lemma 13: the determinant of h on A^n vanishes if and only if $q^{n+1}-1=0$, where now q is a primitive d-th root of unity; therefore, this happens if and only if $n+1$ is divisible by d.

In part (2), the orthogonality of v with the vectors e_j ($j=1,2,\ldots,kd-1$) follows from an explicit computation; it is clear that $v, e_2, \ldots, e_{kd-1}$ form a basis of A^{kd-1}. The matrix of the Hermitian form h_{kd-1} on the quotient A^{kd-1}/Av with respect to the basis $e_2, \ldots, e_{kd-1}$ is clearly h_{kd-2}; this is nondegenerate by part (1). Thus part (2) follows.

Since v is orthogonal to e_k, it follows that s_k fixes v: for any $x \in A^n$, we have

$$s_k(x) = x - \frac{qh(x,e_k)}{q+1}e_k,$$

as can be easily checked by evaluating both sides of this equality on the basis elements e_l. Therefore (3) follows. □

LEMMA 15. *Suppose n is an integer not congruent to -1 modulo d, and as before let $\Gamma_n(d)$ be the image of B_{n+1} under the representation $\rho_n(d)$ on A^n. If $0 \neq W \subset V_A = A^n$ is a subgroup which is stable under $\Gamma_n(d)$, then W contains $\lambda(A^n)$ for some nonzero $\lambda \in A$; in particular, W has finite index in A^n.*

If $F \supset A$ is a field containing the integral domain A and $W_F \subset F^n$ is a nonzero F-subspace stable under the action of $\rho_n(d)$, then $W_F = F^n$.

Proof. Since $n \neq -1 \pmod d$, h is nondegenerate; since $W \neq 0$, W has a nonzero vector x, and there exists a k such that $h(x,e_k) \neq 0$. The formula

$$s_k(x) = x - \frac{qh(x,e_k)}{q+1}e_k$$

shows that a nonzero multiple v_k of e_k lies in W; applying $s_k^{\pm 1}$ to this multiple of e_k shows that $(-q)^{\pm 1}v_k \in W$, where q is a primitive root of unity; hence the $\mathbb{Z}[q,q^{-1}]$-module generated by v_k lies in W. Thus $Av_k \subset W$.

Applying the elements $s_{k\pm 1}$ to Av_k it follows that W contains a nonzero multiple v_l of e_l for every $l \leq n$, and by the preceding paragraph, $Av_l \subset W$ for each l. Therefore the first part of the lemma follows.

The second part of the lemma is proved in the same way, by replacing A by the field F. □

PROPOSITION 16.

(1) *The representation $\rho_n(d)$ is irreducible unless $n \equiv -1 (\text{mod } d)$.*
(2) *If $n \equiv -1 \pmod d$, then $\rho_n(d)$ contains a vector v fixed under B_{n+1} and the quotient A^n/Av yields a representation $\overline{\rho_n(d)}$ of B_{n+1}. Restricted to the subgroup of B_{n+1} generated by $s_2, \ldots, s_n$, the representation $\overline{\rho_n(d)}$ is equivalent to $\rho_{n-1}(d)$. Hence $\overline{\rho_n(d)}$ is irreducible.*

(3) *Suppose n is not congruent to -1 modulo d. Consider the representation $\rho_n(d)$ over an algebraically closed field $\overline{E}$ containing the ring $S = \mathbb{Z}[q+q^{-1}]$, and denote it $\rho_n(\overline{E})$. Then $\rho_n(\overline{E})$ is irreducible over $\overline{E}$.*

Proof. Part (1) of the proposition (the irreducibility) is the second part of Lemma 15. The second part is obvious. The third part again follows from the second part of Lemma 15: $\rho_n(\overline{E})$ is irreducible. □

Let $n \equiv -1 \pmod{d}$. Then the Hermitian space $V = (A^n, h)$ contains the span Av of v as its orthogonal complement and $\overline{V} = V/Av$ has a nondegenerate Hermitian form $\overline{h}$ induced by h. Let $U(h)$ and $U\overline{h})$ denote the unitary groups. We then have a split exact sequence of groups

$$\{0\} \to \mathrm{Hom}_A(\overline{V}, Av) \to U(h) \to U(\overline{V}) \to \{1\}.$$

As before, $\{0\}$ is the trivial group written additively and $\{1\}$ is the trivial group written multiplicatively.

Here, the dual W of $\overline{V}$ may be identified with $\mathrm{Hom}_A(\overline{V}, Av)$. Thus $U(h)$ may be written as a semi-direct product $U(h) = U(\overline{h})W$ with W normal in $U(h)$ and the conjugation action of $U(\overline{h})$ on W is just the dual of the standard representation of $U(\overline{h})$.

4.3. *A central element of the braid group.* Consider the braid group B_{n+1} with generators $s_1, s_2, \ldots, s_n$. consider the element

$$\Delta = (s_1 s_2 \cdots s_n)(s_1 \cdots s_{n-1}) \cdots (s_1 s_2)(s_1)$$

of B_{n+1}. It is elementary to check that for every $k \leq n$ we have: $\Delta s_{n+1-k} = s_k \Delta$. Hence Δ^2 is in the centre of B_{n+1}.

If E is an algebraically closed field containing $\mathbb{Z}[q+q^{-1}]$ and n is not congruent to -1 mod d, then by part (3) of Proposition 16, $\rho_n(E)$ is irreducible; therefore, by Schur's Lemma, the element Δ^2 acts by a scalar δ, say. Since the determinant of each s_i is $-q$ in the representation $\rho_n(E)$, we see that the determinant of Δ^2 is $(-q)^{n(n+1)} = \delta^n$. Therefore, $(\delta/(-q)^{n+1})^n = 1$. On the other hand, the entries of $\rho_n(E)(\Delta^2)$ are Laurent polynomials in q with integral coefficients. Hence the scalar δ lies in the ring $\mathbb{Z}[q, q^{-1}]$. Therefore, the above equation means that $\rho_n(\Delta^2) = \delta = (\pm 1)q^{n+1}$.

LEMMA 17. *If $d \geq 3$ and $n = kd-2$, then the element Δ^2 acts by a scalar $\lambda \neq 1$ on the space A^n of the representation $\rho_n(d)$.*

Proof. By Proposition 16, the representation ρ_{kd-2} is irreducible. By the conclusion of the preceding paragraph, the central element Δ^2 acts by a scalar $\lambda = \pm q^{n+1} = \pm q^{kd-1} = \pm q^{-1}$ since q is now a d-th root of unity. This shows

that $\lambda \neq 1$ since, otherwise, we get

$$q^{-2} = (\pm 1)^2 = 1.$$

This is impossible since $d \geq 3$ and q is a primitive d-th root of unity. Hence $\lambda \neq 1$. □

Remark 7. It can be shown, by examining the action of the Braid Group ([Bir74]) on the free group on $n+1$ generators that the scalar in question is actually q^{n+1}. (This is a special case of Proposition 27 of the present paper, which we do not prove.) In particular, if $n = kd - 2$ and q is a primitive d-th root of unity, then $q^{n+1} = q^{-1} \neq 1$, even when $d = 2$.

We have already mentioned in the introduction that the proof of Theorem 2 is by induction. We will prove Theorem 2 directly when $n \geq 2d$ is congruent to $-1 \pmod{d}$. Then we will prove that induction may be applied, which will prove Theorem 2 for all $n \geq 2d$. To achieve this, we need to exhibit sufficiently many unipotent elements in the image of B_{n+1} under the representation $\rho_n(d)$ for the values $n \equiv -1$ or $0 \pmod{d}$. This will be done in the next two subsections.

4.4. *Constructing unipotent elements when $n = kd - 1$.* Assume that $n = kd - 1$. Since $\dim X = kd - 2$, Lemma 17 and Proposition 16 imply that the square of the element

$$\Delta' = (s_2 s_3 \cdots s_n)(s_2 s_3 \cdots s_{n-1})(\cdots)(s_2 s_3)(s_2)$$

lies in the subgroup generated by $s_2, \ldots, s_n$ in B_{n+1} and acts by a nontrivial scalar $\lambda \neq 1$ on $\overline{\rho_{kd-1}(d)}$.

Denote the element $[s_1, \Delta'^2]$ of B_{n+1} by u. (As before, we denote by $[g, h]$ the commutator $ghg^{-1}h^{-1}$ of g and h.) The image of this element u under the reducible representation $\rho_{kd-1}(d)$ lies in the vector group A^n, where $U(h) = \mathrm{Hom}_A(A^n, Av) \rtimes U(\overline{h})$ is a semi-direct product as before.

PROPOSITION 18. *Let $n = kd - 1$. Under the representation $\rho_n(d)$, the commutator element $u = [s_1, (\Delta')^2]$ has the property that its image $u' = \rho_{kd-1}(u)$ is a* **nontrivial** *unipotent element in the vector part A^{n-1} of $U(h)$.*

Proof. This follows from Lemma 9. Note that (A^n, h) is a degenerate Hermitian form with an isotropic vector v such that the quotient V/Av is nondegenerate; moreover, if X is the A-span of the vectors $e_2, e_3, \ldots, e_n$, then A^n is the direct sum $Av \oplus X$. Hence (V, h) satisfies the hypotheses of Lemma 9.

Since $\mathrm{Dim}\,(X) = kd-2$, Lemma 17 implies that the element $m = \rho_n((\Delta')^2)$ acts by a scalar $\lambda \neq 1$ on X and acts trivially on v; the element $p = \rho_n(s_1)$

takes the element $e_2 \in X$ into the element

$$e_2 + e_1 = -qe_2 + v - \sum_{k=3}^{n} \left(\frac{q^k - 1}{q - 1} \right) e_k \notin X,$$

which shows that p does not lie in $M = U(X)$. Therefore, Lemma 9 applies, and u' is a nonzero vector in the vector part of $U(h)$ and, in particular, is a nontrivial unipotent element. □

PROPOSITION 19. *Suppose that $n = kd - 1$. The subgroup U_n of B_{n+1} generated by the conjugates huh^{-1} where h runs through the elements of the group generated by $s_2, s_3, \ldots, s_n$ has the property that under the representation $\rho_n(d)$, it preserves the flag*

$$Av \subset Av + Ae_2 + \cdots + Ae_{n-1} \subset A^n$$

and acts trivially on successive quotients of this flag.

Further, if U_0 denotes the subgroup of $U(h)$ which preserves the above flag and acts trivially on successive quotients, then the image of U_n is a subgroup N_0 of finite index in the integral points $U_0(O_K)$.

Proof. We need only prove the last part since the image of u lies in the normal subgroup U_0 and is preserved under conjugation by elements of $U(h)$. The conjugation action of M on U_0 becomes the action of $M = U(X)$ on the dual $X^* = \mathrm{Hom}(X, Av)$. By Lemma 15, N_0 is of finite index provided it contains a nonzero element of U_0; but it was already shown (Proposition 18) that the image of u is nontrivial in U_0. The proposition follows. □

4.5. *Constructing unipotents when $n = kd$ with $k \geq 1$.* The space $V = A^n$ may be written as a direct sum

$$V = Av \oplus X \oplus Av^*,\ v = e_1 + \sum_{k=2}^{n-1} x_k e_k,\ v^* = e_n + \sum_{k=1}^{n-1} y_k e_{n-k}$$

as in the preceding subsection. Then $M = U(X)$ is the Levi part of the parabolic subgroup P of $U(h)$ which preserves the flag

$$0 \subset Av \subset Av \oplus X \subset V,$$

and U is the subgroup of P which acts trivially on successive quotients of this flag.

Let Δ' be as in the previous subsection; then $m = \rho_n((\Delta')^2)$ lies in M since it acts trivially on v^* and v (v^* and v are orthogonal to all the vectors $e_2, e_3, \ldots, e_{n-1}$, and hence they are fixed by $s_2, \ldots, s_{n-1}$). Therefore, v, v^* are fixed by Δ', and Δ' preserves the space X. By Lemma 17 , $(\Delta')^2$ acts by a scalar $\lambda \neq 1$ on X.

PROPOSITION 20. *Assume $n = kd$. Then the following hold*:

(1) *The element $u = [s_1, (\Delta')^2]$ acts by a* **nontrivial** *unipotent element on A^n under the representation $\rho_n(d)$. More precisely, the element $\rho_n(d)(u)$ lies in $U(O_K) \setminus Z$, i.e., preserves the flag $Av \subset Av \oplus X \subset V$, acts trivially on the successive quotients, and does not preserve the subspace X.*

(2) *The group N generated by the conjugates huh^{-1} with $h \in \Gamma_{n-1}$ (the group generated by the elements $\rho_n(s_2), \ldots, \rho_n(s_{n-1})$) is a subgroup of finite index in $U(O_K)$; in particular, Γ_n intersects the unipotent radical $U(O_K)$ in a subgroup of finite index.*

Proof. The element u clearly preserves the flag of the proposition, as was verified in the preceding proposition. Since u acts by a unipotent element on W and is a commutator, it follows that u acts trivially on the one-dimensional space V/W, and hence u acts unipotently on V.

By the preceding proposition, u does not preserve the space X: it takes the basis element $e_2 \in X$ into a sum of av and elements of X, with $a \neq 0$ a scalar. By Lemma 10, u does not lie in the centre of U.

Let B be the group generated in $U(O_K)$ by the conjugates $huh^{-1} : h \in H$, where H is the group generated by $s_2, \ldots, s_{n-1}$. Under the quotient map $U \to U_0$, B maps onto B_0, and by the preceding proposition, B_0 has finite index in $U_0(O_K)$.

Now the proposition follows, by appealing to Lemma 11. □

5. **Proof of Theorem 2**

5.1. *Proof of Theorem* 2. We prove the main theorem (Theorem 2) by induction on $n \geq 2d$; we will prove Theorem 2 directly for all n which are multiples of d and are at least $2d$. Then by induction, Theorem 2 follows.

5.1.1. *Proof when $n = kd$, with $k \geq 2$.* The representation ρ_{n-1} is not irreducible. Let $Av \subset V_{n-1}$ be the subspace of invariants. The quotient V_{n-1}/Av is an irreducible representation of the braid group $B(s_2, \ldots, s_{n-1})$. Hence the commutator element

$$u = [s_1, \Delta(s_2, \ldots, s_{n-1})^2]$$

is a *nontrivial* unipotent element under ρ_{n-1} and lies in the vector group $\mathrm{Hom}_A(V_{n-1}/Av, Av)$. Therefore, u preserves the flag $0 \subset Av \subset V_{n-1} \subset V$ and acts unipotently on V since u, being a commutator, has determinant one and is unipotent on V_{n-1}.

Therefore, by Proposition 20, the group generated by the elements huh^{-1} with $h \in B(s_2, \ldots, s_{n-1})$ generate a subgroup commensurable with $U(O_K)$, where U is the unipotent group preserving the flag $Av \subset V_{n-1} \subset V$ and acting

trivially on successive quotients of the flag. We have therefore proved that $\Gamma_n \supset U(O_K)^N$ for some integer N.

Similarly, $\Gamma_n \supset U^-(O_K)^N$ for some integer N, where U^- is opposite to U. Therefore, Γ_n is an arithmetic group since $n \geq 2d$, and hence $U(V_n)$ has K-rank at least two: the space V_{d-1} spanned by $e_1, \ldots, e_{d-1}$ has an isotropic vector v by Lemma 14. The subspace V'_{d-1} spanned by $e_{d+1}, \ldots, v_{2d-1}$ also has the same Hermitian form h_{d-1} and contains an isotropic vector v' by Lemma 14. Clearly, V_{d-1} and V'_{d-1} are mutually orthogonal since the indices j of the bases e_j differ by at least two. Thus we have produced two mutually orthogonal independent isotropic vectors, and hence the K-rank of the unitary group $U(V_n)$ is at least two. Therefore, Theorem 2 follows for $n = kd \geq 2d$ from Corollary 2.

5.1.2. *Proof that Theorem* 2 *for* $n-1$ *implies Theorem* 2 *for* n *when* $kd < n \leq kd+d-2$. In this case, ρ_n and ρ_{n-1} are irreducible. Then V_n contains both the subspace V_{n-1} and the span W_{n-1} of $e_2, e_3, \ldots, e_n$; moreover, both these subspaces V_{n-1} and W_{n-1} are nondegenerate under h. The intersection $V_{n-1} \cap W_{n-1}$ contains an isotropic vector since the intersection contains the span of $e_2, \ldots, e_{d+1}$; recall that $n \geq 2d$, hence $n-2 \geq d$.

By the induction assumption, there exists an integer N such that $U(V_{n-1})^N \subset \Gamma_{n-1}$ and $U(W_{n-1})^N \subset \Gamma_{n-1} \simeq \langle s_2, \ldots, s_n \rangle$. It follows from Lemma 12 that Γ_n is arithmetic.

5.1.3. *Proof that Theorem* 2 *for* $n-1$ *implies Theorem* 2 *for* n *when* $n = kd-1$. By the previous subsection, Γ_{n-1} is arithmetic. Since n is congruent to -1 modulo d, the Hermitian form h_n is degenerate. Then, Proposition 19 implies that Γ_n intersects the vector part in an arithmetic group.

Since the Hermitian form is degenerate, the unitary group $U(V_n)$ of V_n is a semi-direct product of its reductive part $U(V_{n-1})$ and its unipotent part $\mathrm{Hom}(V_{n-1}, Av)$. Then, the decomposition

$$U(V_n)(O_K) = U(V_{n-1})(O_K)\mathrm{Hom}_A(V_{n-1}, Av)$$

shows that Γ_n is also arithmetic.

Combining the above subsections together, we obtain a proof of our main result, namely Theorem 2, for all $n \geq 2d$.

6. **Proof of Theorems 3 and 4**

6.1. *Proof of Theorem* 3. In this subsection we prove that if d is one of the numbers $3, 4, 6$, then for *every* integer $n \geq 1$, the image of the Burau representation $\rho_n(d)$ is an arithmetic group. First note that in these cases $d = 3, 4, 6$, the d-th cyclotomic extension $E_d = \mathbb{Q}[q]/(\Phi_d(q)) \simeq \mathbb{Q}(e^{2\pi i/d})$ is an imaginary quadratic extension of $\mathbb{Q}$, and the totally real sub-field $K_d = \mathbb{Q}$; the ring of integers O_d is the ring $\mathbb{Z}$ of rational integers. Therefore, we have $\Gamma \subset U(h)(\mathbb{Z})$ and the ambient Lie group is $U(h)(\mathbb{R})$ since $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}$. Note

that $U(h)(\mathbb{R})$ is of the form $U(r,s)$ and there is only one factor involved, since $\mathbb{Q}$ has only one archimedean completion, namely $\mathbb{R}$.

We divide the proof into three cases.

Case 1: $n \geq 2d$. In this case, this is exactly Theorem 2, and this was already proved.

Case 2: $n \leq d-2$ *or* $d \leq n \leq 2d-1$. We refer to Table 9 on page 32 of [McM13]. In these cases, the group $\mathrm{SU}(h)(\mathbb{R})$ is either compact or is isomorphic to $U(n-1,1)$. If $U(h)$ is compact, then Γ is finite and is hence "arithmetic"; this is the trivial case. If $U(h) = U(n-1,1)$, then by Theorem (10.3) in [McM13] (which is actually a special case of a result of Deligne-Mostow), the image $\Gamma = \rho_n(d)(B_{n+1})$ is a lattice, i.e., Γ has finite index in $U(h)(\mathbb{Z})$.

Case 3: $n = d-1$ *or* $n = 2d-1$. Since n is congruent to -1 modulo d, Part (2) of Proposition 16 tells us that $\rho_n(d)$ contains a trivial sub-representation and that the quotient is isomorphic to $\overline{\rho_{n-1}(d)}$; moreover, the unitary group $U(h) = U(h_n)$ has a unipotent radical U_0 and a smaller group $U(h_{n-1})$ as a Levi supplement. By the preceding paragraph, the image of Γ in $U(h_{n-1})(\mathbb{Z})$ is arithmetic; moreover, by Proposition 19 (note that n is of the form $kd-1$ with $k = 1$ or 2), the image of a subgroup $U_n \subset B_{n+1}$ under the representation $\rho_n(d)$ is a subgroup of finite index in the integral unipotent radical $U_0(\mathbb{Z})$. Hence Γ has finite index in the integral points of the semi-direct product group $U(h)$.

6.2. *Proof of Theorem* 4. We will now prove Theorem 4. Let $\mathfrak{a}$ (resp. $\mathfrak{a}_e$) denote the principal ideal in $R = \mathbb{Z}[q, q^{-1}]$ generated by the polynomial (q^d-1) (resp. by the e-th cyclotomic polynomial $\Phi_e(q)$). Let $A = R/\mathfrak{a}$. By the Chinese remainder theorem, the $\mathbb{Q}$-algebra $A \otimes \mathbb{Q}$ is the product ring $A \otimes \mathbb{Q} = \prod_{e|d} \mathbb{Q}[q, q^{-1}]/(\mathfrak{a}_e \otimes \mathbb{Q}) \simeq \prod E_e$ where the product runs over all the divisors of d. Here E_e is the e-th cyclotomic extension. Consequently, the reduced Burau representation $\rho_n(A)$ on the rational vector space $A^n \otimes \mathbb{Q} \simeq E_e^n$ is the direct sum $\oplus_{e|d}\rho_n(e)$. Hence the image Γ of the braid group under the Burau representation $\rho_n(A)$ lies in the product $\prod U(h)(O_e)$, where O_e is the ring of integers in the totally real sub-field $K_e = \mathbb{Q}(\cos\frac{2\pi}{d})$, as in the introduction.

(1) We first prove Theorem 4 in the case that d and $n+1$ are coprime. In that case, every divisor e of d is coprime to $n+1$. By Proposition 16, the Hermitian form h on E_e^n is nondegenerate and the representation $\rho_n(e)$ is irreducible. Since $n \geq 2d$, Theorem 2 implies that the image of Γ under $\rho_n(e)$ is a subgroup of finite index in $G_e(O_e)$, where $G_e = U(h)$ is the unitary group of h with respect to Hermitian form h corresponding to the quadratic extension E_e/K_e, provided $e \geq 3$. Moreover, there exists a subgroup, namely $\mathrm{SU}(h)(O_e)$, of finite index in $G_e(O_e)$ which is an arithmetic subgroup of a higher rank semi-simple Lie group, namely $\mathrm{SU}(h)(K_e \otimes_{\mathbb{Q}} \mathbb{R})$.

If $e = 2$, then $E_e = \mathbb{Q}[q]/(\Phi_2(q)) = \mathbb{Q}$ and the image of q in the field $E_e = \mathbb{Q}$ is -1. The form h vanishes identically since $q+1$ divides all entries; we replace this zero form by first dividing h by $q+1$ for a variable q and then taking the resulting form evaluated at $q = -1$. This "divided" form is symplectic. Therefore, G_e is the symplectic group; then by the result of A'Campo [A'C87], the image of Γ in $G_e(O_e) = \mathrm{Sp}(h, \mathbb{Z})$ is a higher rank arithmetic group.

If $e = 1$, then the Burau representation is evaluated at 1; i.e., the representation of the braid group B_{n+1} lies in the symmetric group S_{n+1} which is a finite group and may be ignored in questions on arithmeticity. Lemma 8 now implies that the image Γ in $U(h)(A) = \prod_{e\geq 2} U(h)(O_e)$ is an arithmetic group in the product, under the assumption that $n \geq 2d$.

(2) Suppose $n + 1$ and d are not coprime, and let $r \geq 2$ be the greatest common denominator of d and $n+1$. If a divisor e of d does not divide r, then it does not divide $n + 1$ either, and hence $U(h)(O_e)$ is an arithmetic group in a higher rank semi-simple group (up to finite index) and the projection to the e-th factor of the group Γ has finite index in $U(h)(O_e)$.

If e does divide $n + 1$, then $U(h)$ as an algebraic group over K_e is not reductive; suppose V_e is the unipotent radical of $U(h)$ viewed as a group over E_e. By Theorem 2 applied to this case, the projection of Γ to the e-th factor contains a subgroup of finite index in $V_e(O_e)$. (See the proof of Theorem 2, the subsection where $n + 1$ is divisible by e.)

Putting the above cases together, and using Lemma 8, we get Theorem 4 in all cases.

7. Relation with a cyclic covering of $\mathbb{P}^1$ and proof of Theorem 1

In this section, we relate the monodromy representation of the braid group B_{n+1} considered in Theorem 1 to the Burau representation and use this relation to prove Theorem 1.

7.1. *Generalities.* Suppose

$$\{1\} \to N \to F \to Q \to \{1\}$$

is an exact sequence of abstract groups. Suppose B is a subgroup of the group of automorphisms of F which stabilises the kernel N. Then B acts on the quotient Q also by automorphism and acts on the abelianisation $N^{\mathrm{ab}} = N/[N, N]$; hence B acts on the exact sequence

$$1 \to N/[N, N] \to F/[N, N] \to Q \to \{1\},$$

whose kernel is abelian. Moreover, the conjugation action of F on the abelianisation $N/[N, N]$ is trivial on N and descends to an action of the quotient Q on N^{ab}. If N^{ab} is written additively, then we have a $\mathbb{Z}[Q]$ module structure on N^{ab}.

If we now assume that B acts trivially on the quotient Q, we then have an action of the product group $B \times Q$ on the abelianisation N^{ab}. Therefore, the action of B on N^{ab} is by $\mathbb{Z}[Q]$ module endomorphisms.

7.2. *Action of the braid group on the free group.* Suppose F_{n+1} is a free group on $n+1$ generators, $x_1, x_2, \ldots, x_{n+1}$. Recall that the braid group on $n+1$ strands was given by generators s_i and relations given in the introduction. A theorem of E. Artin ([Bir74, Cor. 1.8.3]) says that the braid group B_{n+1} acts on F_{n+1} as follows. If $j \leq i-1$ or if $j \geq i+2$, then $s_i(x_j) = x_j$. If $j = i, i+1$, then the action is

$$s_i(x_i) = x_{i+1}, \quad s_i(x_{i+1}) = x_{i+1}^{-1} x_i x_{i+1}.$$

(In [Bir74, Cor. 1.8.3], the action is on the right; to get the left action, one can make a slight modification of the formulae.)

The action of B_{n+1} on F_{n+1} gives an action of the braid group on the abelianisation $F_{n+1}^{\mathrm{ab}} = \mathbb{Z}^{n+1}$ of the free group; the images of x_i form the standard basis of $\mathbb{Z}^{n+1}$. From the equations in the preceding paragraph, it is clear that the element s_i acts by the permutation matrix interchanging i and $i+1$ and fixing the rest of the basis. It is also clear that the image of B_{n+1} in the automorphisms of $\mathbb{Z}^{n+1}$ is the permutation group S_{n+1} on $n+1$ symbols.

The kernel, denoted P_{n+1}, of the map $B_{n+1} \to S_{n+1}$ is called the *pure braid group.*

7.3. *Realisation of the Burau representation on homology.* Write $G = \mathbb{Z}^{n+1}$ for the abelianisation of the free group F_{n+1}, where G is written multiplicatively. We have a map $G \to \mathbb{Z} \simeq q^{\mathbb{Z}}$ given by

$$x_1^{m_1} x_2^{m_2} \cdots x_{n+1}^{m_{n+1}} \mapsto q^{-(m_1+m_2+\cdots+m_{n+1})}.$$

The group S_{n+1} (and hence the braid group B_{n+1}) acts on $\mathbb{Z}^{n+1}$ by permutations on the standard basis and acts trivially on $q^{\mathbb{Z}}$. The above map is equivariant with respect to this action. Moreover, the braid group B_{n+1} acts on F_{n+1} and the map $F_{n+1} \to \mathbb{Z}^{n+1}$ is equivariant with respect to this action. We now have an exact sequence

$$1 \to K_{n+1} \to F_{n+1} \to q^{\mathbb{Z}} \to 1$$

with kernel K_{n+1} stable under the action of the braid group B_{n+1}.

The group F_{n+1} has the standard generators $x_1, x_2, \ldots, x_{n+1}$. *As a normal subgroup of* F_{n+1}, the group K_{n+1} is s generated by the elements

$$y_1 = x_1^{-1} x_2, \quad y_2 = x_2^{-1} x_3, \ldots, y_n = x_n^{-1} x_{n+1}.$$

As was observed in the preceding paragraph, B_{n+1} acts on K_{n+1}; we compute its action on the "standard basis" $y_1, y_2, \ldots, y_n$ of K_{n+1}. The braid group is

generated by s_i, and the action of s_i on F_{n+1} was described before. Hence, we have $s_i(y_{i-1}) = x_{i-1}^{-1}x_{i+1} = y_{i-1}y_i$,

$$s_i(y_j) = s_i(x_{j-1}^{-1}x_j) = y_j \ (j \leq i-2 \text{ or } j \geq i+2),$$
$$s_i(y_i) = x_{i+1}^{-1}x_{i+1}^{-1}x_ix_{i+1} = x_{i+1}^{-1}y_i^{-1}x_{i+1} = {}^{x_{i+1}^{-1}}(y_i^{-1}),$$

and

$$s_i(y_{i+1}) = x_{i+1}^{-1}x_i^{-1}x_{i+1}x_{i+2} = x_{i+1}^{-1}x_i^{-1}x_{i+1}^2y_{i+1} = {}^{x_{i+1}^{-1}}(y_i)y_{i+1}.$$

We now consider the commutator subgroup $K_{n+1}^{(1)}$ of K_{n+1}; it is a normal subgroup of F_{n+1} and is stabilised by the action of the braid group. Therefore, we have an exact sequence of groups

$$1 \to M_n = K_{n+1}/K_{n+1}^{(1)} \to F_{n+1}/K_{n+1}^{(1)} \to q^{\mathbb{Z}} \to 1,$$

with abelian kernel M_n (namely the abelianisation of K_{n+1}) written additively. Since K_{n+1} is generated by the y_i as a normal subgroup of F_{n+1} and the conjugation action of F_{n+1} on the abelian group M_n descends to the action of $q^{\mathbb{Z}}$, it follows that M_n is generated as a $q^{\mathbb{Z}}$-module, by the images y_i' (under the quotient map $K_{n+1} \to M_n$) of y_i. Since the group law on M_n is written additively, for each x_i, the conjugation action on M_n is simply multiplication by the element q^{-1}. We are in the situation of Section 7.1 with $N^{\mathrm{ab}} = M_n$, $Q = q^{\mathbb{Z}}$ and $B = B_{n+1}$.

The action of the braid group on the basis y_i of the group K_{n+1} was computed above; this gives a description of the action of s_i on the basis y_i' of M_n as follows. We have the formulae

$$s_i(y_j') = y_j' \ (j \leq i-2 \text{ or } j \geq i+2), \quad s_i(y_{i-1}') = y_{i-1}' + y_i',$$
$$s_i(y_i') = -qy_i', \quad s_i(y_{i+1}') = y_{i+1}' + qy_i'.$$

Now write $y_i = q^ie_i$. In the basis $\{e_i\}$, we get

$$s_i(e_j) = e_j \ (\mid j-i \mid \geq 2), \quad s_i(e_{i-1}) = e_{i-1} + qe_i,$$
$$s_i(e_i) = -qe_i, \quad s_i(e_{i+1}) = e_{i+1} + e_i,$$

which is exactly the reduced Burau representation defined in the introduction. We therefore have

THEOREM 21 (Burau). *Let K_{n+1} be the kernel of the map $F_{n+1} \to q^{\mathbb{Z}}$ defined above. Then, the action of the braid Group B_{n+1} on the first homology of K_{n+1} with integral coefficients is isomorphic to the reduced Burau representation.*

7.4. *Realisation of the Burau representation at d-th roots of unity.* Consider now the quotient map $q^{\mathbb{Z}} \to q^{\mathbb{Z}}/q^{d\mathbb{Z}} \simeq \mathbb{Z}/d\mathbb{Z}$. We have a surjective map $F_{n+1} \to q^{\mathbb{Z}} \to q^{\mathbb{Z}}/q^{d\mathbb{Z}}$. This defines an exact sequence

$$1 \to K_{n+1}(d) \to F_{n+1} \to \mathbb{Z}/d\mathbb{Z} \to 1,$$

of groups, with $Z/d\mathbb{Z}$ written multiplicatively. Clearly, $K_{n+1}(d)$ is generated (as a *normal* subgroup of F_{n+1}) by the elements $y_1, y_2, \ldots, y_n$ and x_1^d where, as before, $y_i = x_i^{-1}x_{i+1}$. Therefore, $K_{n+1}(d)$ is generated by the elements x_1^d and the collection $\{x_1^j y_i x_1^{-j} : 0 \leq j \leq d-1,\ i \leq n\}$.

Being a subgroup of F_{n+1}, $K_{n+1}(d)$ is also free and if n' denotes the minimal number of generators of this free group, we have the formula

$$1 - n' = d(1 - (n+1)) = -dn,\ n' = 1 + dn.$$

Since the cardinality of the system of generators we have exhibited is exactly $1 + nd$, it follows that the above generators x_1^d and $x_1^j y_i x_1^{-j}$ *freely* generate $K_{n+1}(d)$.

Therefore (Section 7.1), the abelianisation $K_{n+1}(d)^{\mathrm{ab}}$ is a direct sum of a *free* module over the ring $\mathbb{Z}[G] = \mathbb{Z}[q]/(q^d - 1) = A$ with generators $y_1', y_2', \ldots, y_n'$ and the trivial module $\mathbb{Z}(x_1^d)'$. Here the prime denotes the image of the element under the quotient map $K_{n+1}(d) \to K_{n+1}(d)^{\mathrm{ab}}$. The map $K_{n+1}^{\mathrm{ab}} \to K_{n+1}(d)^{\mathrm{ab}}$ is equivariant for the action of the braid group. We have an exact sequence of B_{n+1} modules:

$$0 \to \mathrm{Image}(K_{n+1}^{\mathrm{ab}}) \to K_{n+1}(d)^{\mathrm{ab}} \to \mathbb{Z} \to 0.$$

Therefore, it follows from Theorem 21 that the braid group acts on the abelianisation $K_{n+1}(d)^{\mathrm{ab}}$ and that the latter is an extension of the reduced Burau representation $\rho_n(A)$ by the trivial representation. It follows from Theorem 4 that the image of the representation $B_{n+1} \to \mathrm{GL}(K_{n+1}(d)^{\mathrm{ab}})$ is an arithmetic group.

7.5. *Some cyclic coverings of* $\mathbb{P}^1$. Let $a_1, a_2, \ldots, a_{n+1}$ be distinct complex numbers; write S_a for the complement in $\mathbb{C}$ of these points: $S_a = \mathbb{C} \setminus \{a_1, a_2, \ldots, a_{n+1}\}$. The fundamental group of S_a, once a base point is chosen, may be identified with the free group on F_{n+1} generated by small circles x_i going around the point a_i counterclockwise once (and joined to the preferred base point by an arc which avoids all the other points a_j and has zero winding number around all the points a_j with $j \neq i$). The map $S_a \to \mathbb{C}^*$ defined by

$$x \mapsto (x - a_1)(x - a_2)\cdots(x - a_{n+1}) = P_a(x)$$

induces a homomorphism $F_{n+1} \to q^{\mathbb{Z}}$, which sends each x_i to q^{-1}. Here, q^{-1} is a small circle around zero in $\mathbb{C}^*$ which runs counterclockwise exactly once.

For future reference, note that the loop around infinity lying in S_a represents the product element $x_1x_2\cdots x_{n+1}$ and that this element is invariant under the action of the braid group B_{n+1} on the free group F_{n+1}.

The affine variety $\mathbb{C}^* = \mathbb{G}_m$ admits a cyclic covering of order d given by $z \mapsto z^d$ from $\mathbb{G}_m$ to $\mathbb{G}_m$. The covering may be realised as the space $\{(x,y) \in \mathbb{C}^* \times \mathbb{C}^* : y^d = x\}$ where the covering map is the first projection. Pulling back this covering to S_a we get a cyclic covering of S_a, realised as the space

$$X_a = \{(x,y) \in \mathbb{C}^* \times S_a : y^d = (x-a_1)(x-a_2)\cdots(x-a_{n+1})\},$$

with the first projection being the covering map from X_a onto S_a. Therefore, under the identification of the fundamental group of S_a with F_{n+1}, the fundamental group of X_a is identified with $K_{n+1}(d)$.

As the collection a varies, we get a collection $\mathcal{P}$ of monic polynomials P_a of degree $n+1$ which have distinct roots, and if $\mathcal{Q}$ denotes the variety

$$(w,x,P) \in \mathbb{C}^* \times \mathbb{C} \times \mathcal{P} : w = P(x),$$

then the projection on to the third coordinate gives a fibration over $\mathcal{P}$ with fibre at P being S_a. (Here a is the collection of roots of P.) The fibration over $\mathcal{P}$ has a continuous section (as can be easily seen) and hence the fundamental group of $\mathcal{P}$ may be thought of as a subgroup of the total space $\mathcal{Q}$ of the fibration. We therefore get a monodromy action of the fundamental group of $\mathcal{P}$ on the fundamental group F_{n+1} of the fibre. We have the following fundamental theorem of E. Artin ([Bir74, 1.8]):

THEOREM 22 (Artin). *The fundamental group of $\mathcal{P}$ is the braid group B_{n+1}, and the monodromy action on F_{n+1} is the action of B_{n+1} on F_{n+1} defined in Section* 7.2.

Consequently, the monodromy action on the fibre of the fibration

$$\{(y,x,P) \in \mathbb{C}^* \times \mathbb{C} \times \mathcal{P} : y^d = P(x)$$

over $\mathcal{P}$ is the action of B_{n+1} defined in Section 7.2 restricted to the subgroup $K_{n+1}(d) \simeq \pi_1(X_a)$; therefore, B_{n+1} acts on the first homology of X_a: $H_1(X_a) \simeq K_{n+1}(d)^{\mathrm{ab}}$ by (an extension by the trivial representation of) the Burau representation $\rho_n(A)$, and this gives the monodromy action of B_{n+1} on $H_1(X_a)$, with image Γ', say.

THEOREM 23. *If $n \geq 2d$, then the image of the representation $B_{n+1} \to \mathrm{GL}(H_1(X_a))$ is an arithmetic group.*

Proof. We have identified this representation with the extension by the trivial representation of the Burau representation $\rho_n(A)$, where

$$A = \mathbb{Z}[q,q^{-1}]/(q^d-1).$$

The theorem follows from the conclusion of the preceding Section 7.4. □

7.6. *The compactification of* X_a. Now X_a is a compact Riemann surface with finitely many punctures; denote by X_a^* the smooth projective curve obtained by filing in these punctures.

The covering map $X_a \to S_a$ is such that these punctures lie over the points a_i or else over the point at infinity of S_a. If a puncture lies over some a_i, then the image of a small loop around the puncture in F_{n+1} is x_i^d; if the puncture lies above infinity, then the image of a small loop around the puncture in F_{n+1} is a power of the element $x_1x_2\cdots x_{n+1}$ (represented by the loop around infinity); therefore, such an element is invariant under the action of the braid group.

The mapping of $\pi_1(X_a) \to \pi_1(X_a^*)$ is such that these loops around the punctures generate the kernel. (This is an easy consequence of the van Kampen theorem.) Note that the element s_j of the braid group B_{n+1} (under the action on the free group F_{n+1} defined in Section 7.2) takes the loop x_i to a conjugate of the loop x_k for some k. Therefore, the braid group leaves the kernel of the map $\pi_1(X_a) \to \pi_1(X_a^*)$ stable. Hence, by Artin's theorem (Theorem 22), the induced map $H_1(X_a) \to H_1(X_a^*)$ on homologies is equivariant under the monodromy action of the braid group.

7.7. *Proof of Theorem* 1. We can now prove Theorem 1. We are to prove that the image of the representation $B_{n+1} \to \mathrm{GL}(H^1(X_a^*))$ is arithmetic where $H^1(X_a^*)$ is the cohomology with integer coefficients. The B_{n+1} module $H_1(X_a^*)$ (*homology* of X_a^* with integral coefficients) is a quotient of the module $H_1(X_a)$. By Theorem 23, the image of the braid group in $\mathrm{GL}(H_1(X_a))$ is arithmetic. By Proposition 6, the image of the braid group in $\mathrm{GL}(H_1(X_a^*))$ is also arithmetic. By Poincaré duality, the image of the braid group in $\mathrm{GL}(H^1(X_a))$ is also arithmetic, proving Theorem 1.

7.8. *The representation* $H_1(X_a^*, \mathbb{Q})$. Denote by A and A' respectively the $\mathbb{Q}$-algebras $\mathbb{Q}[q]/(q^d-1)$ and $\mathbb{Q}[q]/(1+q+\cdots+q^{d-1})$. If M is an A module, denote by $(1+q+\cdots+q^{d-1})M$ the subspace of elements of the form $(1+q+\cdots+q^{d-1})m$ with $m \in M$, and let M' be the quotient module $M/(1+q+\cdots+q^{d-1})M$.

We have seen that $K_{n+1}(d)^{\mathrm{ab}}$ is an extension of the image of K_{n+1}^{ab} in $K_{n+1}(d)^{\mathrm{ab}}$, by the trivial module $\mathbb{Z}$; tensoring with $\mathbb{Q}$, we have the same statement, with $\mathbb{Z}$ replaced by $\mathbb{Q}$. Clearly, $\mathbb{Q}' = 0$. Therefore, we have the equality of the "primed" modules

$$K_{n+1}^{\mathrm{ab}} \otimes \mathbb{Q} \simeq \mathrm{Im}(K_{n+1}^{\mathrm{ab}} \otimes \mathbb{Q})'.$$

We have seen in the preceding subsection that the "primed" representation $H_1(X_a, \mathbb{Q})'$ of the braid group B_{n+1} is isomorphic to the Burau representation $\rho_n(A')$ on A'^n, where $A' = \mathbb{Q}[q, q^{-1}]/(1+q+\cdots+q^{d-1})$. Therefore, by Section 6.2, the Burau representation $\rho_n(A')$ on the $\mathbb{Q}$-vector space $(A')^n$ is the

direct sum

$$H_1(X_a, \mathbb{Q})' \simeq \rho_n(A') = \oplus_{e|d\ e\geq 2}\rho_n(e).$$

Recall from Proposition 16 that if $n \equiv -1 \pmod{e}$, then the representation $\rho_n(e)$ contains a one-dimensional space L_e, say, of invariants, and that the quotient $(A_e^n \otimes \mathbb{Q})/L_e$ is irreducible; in Proposition 16, this representation was denoted $\overline{\rho_n(e)}$. By an abuse of notation, if e does not divide $n+1$, we denote $\rho_n(e)$ also by $\overline{\rho_n(e)}$.

The embedding of the affine curve X_a into its compactification X_a^* induces a map $H_1(X_a, \mathbb{Q}) \to H_1(X_a^*, \mathbb{Q})$ on rational homology, which is equivariant for the action of the braid group. By analysing the map $H_1(X_a) \to H_1(X_a^*)$, one can show that (compare Theorem 5.5 of [McM13, pp. 24–25], where the case $e = d$ is treated) the monodromy representation $H_1(X_a^*, \mathbb{Q})$ has the decomposition

$$H_1(X_a^*, \mathbb{Q}) \simeq \bigoplus_{e|d,\ e\geq 2} \overline{\rho}_n(e).$$

We use the fact that loops around points in X_a which lie above ∞ in the curve $S_a \subset \mathbb{P}^1$ lie in the kernel of the map $H_1(X_a) \to H_1(X_a^*)$; one can show that the invariant vector in $\rho_n(e)$ (for e dividing $n+1$) is generated by these "infinity" loops and hence lies in the kernel of the map on homology.

The following proposition is an immediate consequence of the decomposition of the representation of B_{n+1} on $H_1(X_a^*)$ and Lemma 8.

PROPOSITION 24. *If $n \geq 2d$, then the image of the monodromy representation of B_{n+1} on $H_1(X_a^*)$ of Theorem 1 is a subgroup of finite index in the product $\prod \overline{G}_e(O_e)$, where the product is over all the divisors $e \geq 2$ of d and $\overline{G}_e$ is the unitary group of the Hermitian form $\overline{h}_n$ induced by $h = h_n$ on the quotient representation $\overline{\rho}_n(e)$ of the Burau representation $\rho_n(e)$.*

8. **Applications**

8.1. *Some complex reflection groups.* We will follow the notation of Section 5 of [McM13]. In Section 5 of [McM13], given the root system A_n (and therefore its graph), the Artin group $A(A_n)$ is defined; given a complex number $q = e^{2\pi i x}$ with $-1/2 \leq x < 1/2$, there exists a representation

$$\rho_q : A(A_n) \to \mathrm{GL}_n(\mathbb{C}),$$

with image denoted $A_n(q)$. The image preserves a Hermitian form and is a subgroup of a unitary group $U(r,s) \subset \mathrm{GL}_n(\mathbb{C})$. The image of the braid group B_{n+1} under the Burau representation $\rho_n : B_{n+1} \to \mathrm{GL}_n(\mathbb{Z}[q, q^{-1}])$ may be identified with the complex reflection group $A_n(q)$. Question 5.6 of [McM13] asks when the image $A_n(q)$ is a lattice in $U(r,s)$. In the notation of Question 5.6 of [McM13], the image group $\Gamma_n = \rho_n(d)(B_{n+1})$ is the group $A_n(q)$ where q

is a primitive d-th root of unity; therefore, question 5.6 asks whether $A_n(q)$ can be a lattice in the real unitary group $U(r,s)$; Theorem 2 answers this question in a large number of cases. We have the following corollary of Theorem 2 (and part (1) of the corollary follows from Theorem 3).

COROLLARY 3. (1) *If $q = e^{2\pi i/d}$, then $A_n(q)$ is a lattice in $U(r,s)$ when $d = 3,4,6$ for* **all n**. *If $d = 2$, then $A_n(q)$ is a lattice in $\mathrm{Sp}_n(\mathbb{Z})$.*

(2) *If d is not $2,3,4,6$ and $n \geq 2d$, then the image Γ_n under the Burau representation is an irreducible lattice in the product of unitary groups $U(h)(K_d \otimes_{\mathbb{Q}} \mathbb{R}) \simeq \prod_v U(r_v, s_v)$, where the product is over all the archimedean (real) completions $K_{d,v}$ of the totally real field K_d and the number of factors is at least two. Therefore, the projection of Γ_n to one of the factors is never a lattice if $d \neq 3,4,6$.*

In particular, the intersection $A_n(q) \cap \mathrm{SU}(r_v, s_v)$ is dense in $\mathrm{SU}(r_v, s_v)$ for each archimedean v.

Thus Question 5.6 of [McM13] is open only if $d \neq 3,4,6$ *and* if $n \leq 2d-1$.

8.2. *Application to hypergeometric monodromy of type ${}_nF_{n-1}$.*

Definition 3. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{C}^n$ be complex numbers such that $\alpha_j \neq \beta_k \pmod 1$ for any j and k. Denote by z a complex variable; write $\theta = z\frac{d}{dz}$. Consider the differential operator $D = D(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$ given by

$$D = (\theta + \beta_1 - 1)(\theta + \beta_2 - 1) \cdots (\theta + \beta_n - 1) - z(\theta + \alpha_1) \cdots (\theta + \alpha_n).$$

The equation

$$Du = 0$$

is called the *hypergeometric equation* with parameters α, β.

The differential operator D is of the form

$$D = a_n(z)\frac{d^n}{dz^n} + a_{n-1}(z)\frac{d^{n-1}}{dz^{n-1}} + \cdots + a_0(z),$$

where a_i are polynomials and $a_n(z) = z^n(1-z)$ is the highest coefficient.

This coefficient $a_n(z)$ vanishes at 0 and 1 (and also at infinity if we change coordinates from z to z^{-1}) but does not vanish anywhere in $C = \mathbb{P}^1 \setminus \{0, 1, \infty\}$. Using this property of the highest coefficient, it can be shown that the space of solutions is of dimension n and that the solutions are (locally) analytic on the Riemann surface C. Denote by $\pi_1(C, \frac{1}{2})$ the fundamental group of C based at the point $\frac{1}{2}$. Then it acts on the space ($\simeq \mathbb{C}^n$) of solutions u of the foregoing differential equation $Du = 0$. (Here u is analytic on C.) Denote by $\Gamma = \Gamma(\alpha, \beta)$ the image of the fundamental group $\pi_1(C, \frac{1}{2})$ in the group $\mathrm{GL}_n(\mathbb{C})$ of linear automorphisms of the n-dimensional space of solutions. Denote by $M_{\alpha,\beta}$ the resulting representation of $\pi_1(C, \frac{1}{2})$.

If $\alpha, \beta \in \mathbb{Q}^n$, then Γ may be conjugated into $\mathrm{GL}_n(O)$ where O is the ring of integers in a number field F. If $D = [F : \mathbb{Q}]$ is the degree of F over $\mathbb{Q}$, then $\Gamma \subset \mathrm{GL}_{nD}(\mathbb{Z})$. In [Sar12] the following question is considered: determine the pairs $\alpha, \beta \in \mathbb{Q}^n$ such that the associated monodromy group is arithmetic (i.e., has finite index in its integral Zariski closure in $\mathrm{GL}_{nD}(\mathbb{Z})$).

Fuchs, Meiri and Sarnak (see [Sar12]) give an infinite family of examples of pairs α, β for which the group Γ has a natural embedding in an integral orthogonal group $O_n(\mathbb{Z})$ with Zariski dense image and of *infinite index*. (In [Sar12], they are called *thin* groups.) Thus the monodromy Γ is not always arithmetic.

By using [A'C87], an infinite family of examples can be constructed, where the monodromy is an arithmetic subgroup of $\mathrm{Sp}_{2m}(\mathbb{Z})$. One can, using Theorem 2, give a more general formulation: let $d \geq 2$ be an integer and $1 \leq c \leq d$ be an integer coprime to d.

THEOREM 25. *Suppose that*

$$\alpha = \left(\frac{c}{d} + \frac{1}{n+1}, \ldots, \frac{c}{d} + \frac{n-1}{n+1}, \frac{c}{d} + \frac{n}{n+1}\right),$$
$$\beta = \left(\frac{c}{d} + \frac{1}{n}, \ldots, \frac{c}{d} + \frac{n-1}{n}, 1\right).$$

If $d = 2$ and $n = 2m$ is even, then the monodromy group Γ (is an arithmetic group and) has finite index in the integral symplectic group $\mathrm{Sp}_{2m}(\mathbb{Z})$.

If $d \in \{3, 4, 6\}$ and n is arbitrary such that $n + 1$ is coprime to d, then the monodromy Γ is an arithmetic group and is of finite index in the integral unitary group $U(h)(\mathbb{Z})$, where h is a suitable Hermitian form defined over the rationals.

If $d \geq 3$ and $n \geq 2d$ is such that $n + 1$ is coprime to d, then Γ is an arithmetic group. Γ has finite index in an integral unitary group of the form $U(h)(O_d)$, where h is a nondegenerate Hermitian form over the totally real number field $K_d = \mathbb{Q}(\cos(\frac{2\pi}{d}))$ and O_d is the ring of integers in K_d.

Among these examples, only the case $d = 2$ (treated in [A'C87]) has the property that the monodromy group Γ can be conjugated into $\mathrm{GL}_n(\mathbb{Z})$ (in fact it already lies in $\mathrm{Sp}_{2m}(\mathbb{Z})$ with respect to the natural representation given in [BH89]).

As we will see, Theorem 25 is an easy consequence of the fact that the image of the Burau representation of the braid group B_{n+1} on $n + 1$ strands at d-th roots of unity is an arithmetic group in the cases stated in the theorem. In case the image of the Burau representation is not arithmetic ([DM86], [McM13]), the image of the monodromy representation defines a *thin group* in the sense of Sarnak ([Sar12]).

That the image of the Burau representation for $d = 2$ is a finite index subgroup of the integral symplectic group is a well known theorem of A'Campo ([A'C87]). In the other cases, this is Theorem 2.

We now sketch the relationship between Theorem 25 and the Burau representation. Suppose D is the differential operator considered at the beginning of this section. Put $a_j = e^{2\pi i\alpha_j}$, and write $f(X) = \prod_{j=1}^{n}(X - a_j)$. Consider the ring $\mathbb{C}[X]/(f(X))$. This is a $\mathbb{C}$-vector space with the basis $1, X, \ldots, X^{n-1}$. The operator defined by multiplication by X on the ring $\mathbb{C}[X]/(f(X))$ gives a matrix A with respect to this basis and is called the companion matrix of f. Similarly, let B be the companion matrix of $g(X) = \prod_{j=1}^{n}(X - b_j)$, where $b_j = e^{2\pi i\beta_j}$. We will assume henceforth that $a_j \neq b_k$ for any j, k; i.e., f, g are coprime.

By results of Levelt ([BH89]), there exists a basis of solutions $\{u\} = \{u_1, \ldots, u_n\}$ of the equation $Du = 0$ on which the monodromy action of $\pi_1(C) = \pi_1(C, \frac{1}{2})$ is described as follows. Let h_0, h_1, h_∞ be small loops in C going counterclockwise around $0, 1, \infty$ exactly once. They generate $\pi_1(C, \frac{1}{2})$ and satisfy the relation $h_0h_1h_\infty = 1$. Under the monodromy representation $M_{\alpha,\beta}$, the matrix of h_0 is A, that of h_∞ is B^{-1}. (Then the matrix of h_1 is $A^{-1}B$.) It follows that $A^{-1}B$ is a *complex reflection*; i.e., the space of vectors fixed by $A^{-1}B$ is a codimension one subspace.

Moreover, suppose $X, Y \in \mathrm{GL}_n(\mathbb{C})$ are such that (1) the characteristic polynomial of X is f, and the characteristic polynomial of Y is g, (2) the matrix $X^{-1}Y$ is a complex reflection. We then get a representation M' of $\pi_1(C)$ by sending h_0 to X and h_∞ to Y^{-1}. The result of Levelt is that the representation M' is equivalent to $M_{\alpha,\beta}$ for some α, β such that $e^{2\pi i\alpha_j}$ for varying j give all the roots of f; β is chosen similarly for g.

Now consider the Burau representation $\rho_n : B_{n+1} \to \mathrm{GL}_n(\mathbb{Z}[q, q^{-1}])$. The braid group B_{n+1} is generated by the two elements $t_0 = s_1s_2\cdots s_n$ and $t_1 = s_n^{-1}$. Write $t_\infty = (s_1s_2\cdots s_{n-1})^{-1}$. We then get $t_0t_1t_\infty = 1$. Therefore, we have a surjection from $\pi_1(C, \frac{1}{2}) \to B_{n+1}$ given by $h_0 \mapsto t_0$ and $h_\infty \mapsto t_\infty$. Composition of this map with the Burau representation ρ_n gives a representation $r : \pi_1(C, \frac{1}{2}) \to \mathrm{GL}_n(\mathbb{Z}[q, q^{-1}])$. Put $X = r(h_0)$ and $Y = r(h_\infty^{-1})$. Then $X^{-1}Y = r(h_1) = \rho_n(t_1) = \rho_n(s_n^{-1})$, and the formula for the Burau representation shows that the latter matrix is a complex reflection. Secondly, with respect to the standard basis e_i of the Burau representation, the element h_0 has the matrix form

$$X = \rho_n(q)(h_0) = \begin{pmatrix} 0 & 0 & 0 & \cdots & -q \\ q & 0 & 0 & \cdots & -q \\ 0 & q & 0 & \cdots & -q \\ \cdots & \cdots & \cdots & \cdots & -q \\ 0 & \cdots & \cdots & q & -q \end{pmatrix}$$

and its characteristic polynomial is of the form

$$\mathrm{Ch}(t, X) = \prod_{j=1}^{n} (t - q\ e^{2\pi ij/(n+1)}) = f(t),$$

say. Similarly, if $Y = \rho_n(q)(h_0^{-1})$, then the characteristic polynomial is of the form

$$\mathrm{Ch}(t, Y) = (t-1) \prod_{k=1}^{n-1} (t - q\ e^{2\pi ik/n}) = g(t),$$

say. It is clear that the two characteristic polynomials do not have a common root. Therefore, by Levelt's result, r is equivalent to the monodromy representation $M_{\alpha,\beta}$ of a suitable hypergeometric equation associated to parameters α_j, where $a_j = qe^{2\pi ij/(n+1)} = e^{2\pi\alpha_j}$ and $b_j = e^{2\pi i\beta_j} = qe^{2\pi ij/n}$ or 1. Specialise q to any primitive d-th root of unity $e^{2\pi ic/d}$. The resulting representation r of the group $\pi(C, \frac{1}{2})$ is equivalent to the monodromy representation associated to the parameters α, β in the theorem, and therefore, it has the same image (up to conjugacy) as the Burau representation $\rho_n(d)$. Therefore, the arithmeticity of $M_{\alpha,\beta}$ follows from Theorem 2.

In Theorem 25, we have proved that a very special case of the representation $M_{\alpha,\beta}$ coincides with the monodromy of the Burau representation; therefore, its arithmeticity follows from Theorem 2 and from [A'C87].

9. **Theorem 26 and its proof**

Let $d \geq 2$ and $k_1, k_2, \ldots, k_{n+1}$ be integers with $1 \leq k_i \leq d-1$. Let $a_1, \ldots, a_{n+1}$ be distinct complex numbers. Consider the affine curve $X_{a,k} = \{(x, y) \in \mathbb{C}^2\}$ given by the equation

$$y^d = (x - a_1)^{k_1} \cdots (x - a_{n+1})^{k_{n+1}}.$$

$X_{a,k}$ is a compact Riemann surface $X^*_{a,k}$ with finitely many punctures. The space S of $a = (a_1, \ldots, a_{n+1}) \in C^{n+1}$ with distinct co-ordinates has fundamental group isomorphic to the "pure braid group" denoted P_{n+1}. It is the kernel to the map $B_{n+1} \to S_{n+1}$. (See the last paragraph of Section 7.2.) As before, we have a family $X \to S$ with the fibre over a being the compact Riemann surface $X^*_{a,k}$ and we have the monodromy representation of P_{n+1} on the cohomology group $H^1(X^*_{a,k}, \mathbb{Z})$.

THEOREM 26. *If all the k_i are co-prime to d and if $n \geq 2d$, then the image Γ of the monodromy representation is an arithmetic group.*

We only sketch the proof. (The proof is much more involved than that of Theorem 1.) The proof of Theorem 1 used the properties of the Burau representation, which were established in Section 4. The proof of Theorem 26 is quite similar, but it uses properties of the reduced *Gassner* representation.

(See [Bir74, p. 119] for the definition of the reduced Gassner representation.) This is a representation

$$g_n(X) : P_{n+1} \to \mathrm{GL}_n(\mathbb{Z}[X_1^{\pm 1}, \ldots, X_{n+1}^{\pm 1}])$$

of the pure braid group P_{n+1} on the free module of rank n over the ring of Laurent polynomials with integral coefficients in $n+1$ variables $X_1, \ldots, X_{n+1}$. If $z_1, \ldots, z_{n+1}$ are complex numbers, then we get a specalisation $g_n(z)$ of the reduced Gassner representation, called the *reduced Gassner representation evaluated at* $z_1, \ldots, z_{n+1}$.

The properties of Gassner representation which we will use are the following. (For the second part of the proposition, see [Abd97].)

PROPOSITION 27. *The reduced Gassner representation is has a nondegenerate skew Hermitian form H preserved by P_{n+1}. It is absolutely irreducible. The centre of B_{n+1} (which lies in P_{n+1} and is generated by Δ^2) acts by scalars, and Δ^2 acts by the scalar $X_1 X_2 \cdots X_{n+1}$ on the Gassner representation.*

If we specialise $X_i \mapsto z_i = q^{k_i}$, where k_i are coprime to d and q is a generator of the cyclic group $\mathbb{Z}/d\mathbb{Z} = q^{\mathbb{Z}}/q^{d\mathbb{Z}}$, then the reduced Gassner representation evaluated at these d-th roots of unity is irreducible unless $z_1 z_2 \cdots z_{n+1} = 1$.

If $z_1 \cdots z_{n+1} = 1$, then reduction of the Hermitian form H is degenerate and its null space is one dimensional. Moreover, the quotient is irreducible.

In the Burau case, we used the fact that if $n \equiv -1 \pmod{d}$, then the Hermitian form is degenerate (Proposition 16) to produce (many) unipotent elements. We similarly use the last part of Proposition 27 to obtain unipotent elements in the Gassner case.

The analogue of Theorem 2 is the following. As in the introduction, let $A_d = \mathbb{Z}[q, q^{-1}]/(\Phi_d(q))$; it is isomorphic to the ring of integers in the d-th cyclotomic extension E_d of $\mathbb{Q}$. Let O_d denote the ring of integers of the totally real sub-field $K_d = \mathbb{Q}[q + q^{-1}]/(\Phi_d(q))$ of E_d.

THEOREM 28. *Let $g_n(d) : P_{n+1} \to \mathrm{GL}_n(A_d)$ denote the reduced Gassner representation evaluated at $X_i = q_0^{k_i}$, where k_i are coprime to d and $q_0 \in A_d$ is the image of q. If $n \geq 2d$, then the image of $g_n(d)$ is an arithmetic subgroup of a suitable unitary group.*

The proof of Theorem 28 is similar to that of Theorem 2. In the case of the Burau representation, after we constructed sufficiently many unipotent elements, Theorem 2 could be proved using the fact (see the section on the proof of Theorem 2) that the K-rank of the associated unitary group was ≥ 2, provided $n \geq 2d$. The argument was as follows. Write $n + 1 = d + m + d$, where $m \geq 1$. Then the span of the first d basis elements $e_1, \ldots, e_d$ of the Burau representation contains an isotropic vector v, and similarly the span of the last d basis elements $e_n, \ldots, e_{n-d+1}$ contains an isotropic vector v'. If

$m \geq 1$, then the two sets of basis elements are orthogonal and hence v, v' are orthogonal for the hermitian form h_n. Hence the K rank of the unitary group is at least 2.

We argue similarly in the case of the Gassner representation. As was remarked at the end of Proposition 27, we can get unipotent elements if there are subsets X of the indexing set $1, 2, \ldots, n$ such that $\prod_{i \in X} z_i = 1$. Put $z_i = q^{k_i}$; an argument using the pigeon-hole principle implies that if $n \geq 2d$, then there are two disjoint subsets X, Y of the set $\{1, 2, \ldots, n\}$ such that $\prod_{i \in X} z_i = 1$ and $\prod_{j \in Y} z_j = 1$. (In the Burau case, $X = \{1, 2, \ldots, d\}$ and $Y = \{n, n-1, \ldots, n-d+1\}$ will suffice.) By the third part of Proposition 27, it follows that the span of e_i for $i \in X$ contains an isotropic vector v_X. Similarly, the span of e_j for $j \in Y$ contains an isotropic vector v_Y. The Hermitian form preserved by the image of the Gassner representation is such that if X, Y are disjoint and their union is a proper subset of $\{1, 2, \ldots, n\}$, then v_X, v_Y are orthogonal, and hence the K-rank of the associated unitary group is at least two. Moreover, Proposition 27 applied to the set X (in place of the set $1, 2, \ldots, n$) implies that we have many unipotent elements in the image of the Gassner representation. By appealing to Theorem 7, we then deduce Theorem 28.

The proof of Theorem 26 is deduced from Theorem 28, by relating the monodromy representation, to the Gassner representation. The proof of this relationship is very similar to the proof in Section 7 relating monodromy and the Burau representation (but is much more involved and we omit the details).

References

[Abd97] M. N. Abdulrahim, Complex specializations of the reduced Gassner representation of the pure braid group, *Proc. Amer. Math. Soc.* **125** (1997), 1617–1624. MR 1422839. Zbl 0872.20035. http://dx.doi.org/10.1090/S0002-9939-97-04081-1.

[A'C87] N. A'Campo, Tresses, monodromie et groupes symplectique, *Comment. Math. Helv.* **54** (1987), 318–327. Zbl 0441.32004.

[ACT02] D. Allcock, J. A. Carlson, and D. Toledo, The complex hyperbolic geometry of the moduli space of cubic surfaces, *J. Algebraic Geom.* **11** (2002), 659–724. MR 1910264. Zbl 1080.14532. http://dx.doi.org/10.1090/S1056-3911-02-00314-4.

[AH10] D. Allcock and C. Hall, Monodromy groups of Hurwitz-type problems, *Adv. Math.* **225** (2010), 69–80. MR 2669349. Zbl 1080.14532. http://dx.doi.org/10.1016/j.aim.2010.02.013.

[BMS67] H. Bass, J. Milnor, and J.-P. Serre, Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$), *Inst. Hautes Études Sci. Publ. Math.* **33** (1967), 59–137. MR 0244257. Zbl 0174.05203. Available at http://www.numdam.org/item?id=PMIHES_1967__33__59_0.

[BH89] F. Beukers and G. Heckman, Monodromy for the hypergeometric function ${}_nF_{n-1}$, *Invent. Math.* **95** (1989), 325–354. MR 0974906. Zbl 0663.30044. http://dx.doi.org/10.1007/BF01393900.

[Bir74] J. S. Birman, *Braids, Links, and Mapping Class Groups*, **82**, Princeton Univ. Press, Princeton, N.J., 1974, Ann. of Math. Stud. MR 0375281. Zbl 0305.57013.

[BT65] A. Borel and J. Tits, Groupes réductifs, *Inst. Hautes Études Sci. Publ. Math.* **27** (1965), 55–150. MR 0207712. Zbl 0145.17402. http://dx.doi.org/10.1007/BF02684375.

[DM86] P. Deligne and G. D. Mostow, Monodromy of hypergeometric functions and nonlattice integral monodromy, *Inst. Hautes Études Sci. Publ. Math.* **63** (1986), 5–89. MR 0849651. Zbl 0615.22008. http://dx.doi.org/10.1007/BF02831622.

[GS75] P. A. Griffiths and W. Schmid, Recent developments in Hodge theory: a discussion of techniques and results, in *Discrete Subgroups of Lie Groups and Applications to Moduli* (Intern. Colloq., Bombay, 1973), Oxford Univ. Press, Bombay, 1975, pp. 31–127. MR 0419850. Zbl 0355.14003.

[GL09] F. Grunewald and A. Lubotzky, Linear representations of the automorphism group of a free group, *Geom. Funct. Anal.* **18** (2009), 1564–1608. MR 2481737. Zbl 1175.20028. http://dx.doi.org/10.1007/s00039-009-0702-2.

[Loo97] E. Looijenga, Prym representations of mapping class groups, *Geom. Dedicata* **64** (1997), 69–83. MR 1432535. Zbl 0872.57018. http://dx.doi.org/10.1023/A:1004909416648.

[McM13] C. T. McMullen, Braid groups and Hodge theory, *Math. Ann.* **355** (2013), 893–946. MR 3020148. Zbl 06149478. http://dx.doi.org/10.1007/s00208-012-0804-2.

[Mos86] G. D. Mostow, Generalized Picard lattices arising from half-integral conditions, *Inst. Hautes Études Sci. Publ. Math.* **63** (1986), 91–106. MR 0849652. Zbl 0615.22009. http://dx.doi.org/10.1007/BF02831623.

[Nor86] M. V. Nori, A nonarithmetic monodromy group, *C. R. Acad. Sci. Paris Sér. I Math.* **302** (1986), 71–72. MR 0832040. Zbl 0602.14025.

[PR94] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, *Pure and Applied Mathematics* **139**, Academic Press Inc., Boston, MA, 1994, translated from the 1991 Russian original by Rachel Rowen. MR 1278263. Zbl 0841.20046.

[Rag72] M. S. Raghunathan, *Discrete Subgroups of Lie Groups*, *Ergeb. Math. Grenzgeb.* **68**, Springer-Verlag, New York, 1972. MR 0507234. Zbl 0254.22005. http://dx.doi.org/10.2140/pjm.1992.152.365.

[Rag92] M. S. Raghunathan, A note on generators for arithmetic subgroups of algebraic groups, *Pacific J. Math.* **152** (1992), 365–373. MR 1141802. Zbl 0793.20045. http://dx.doi.org/10.2140/pjm.1992.152.365.

[Sar12] P. Sarnak, Notes on thin groups, 2012, MSRI Hot Topics Workshop. Available at http://www.msri.org/attachments/workshops/652_Sarnak-notes.pdf.

[Squ84] C. C. Squier, The Burau representation is unitary, *Proc. Amer. Math. Soc.* **90** (1984), 199–202. MR 0727232. Zbl 0542.20022. http://dx.doi.org/10.2307/2045338.

[Tit76] J. Tits, Systèmes générateurs de groupes de congruence, *C. R. Acad. Sci. Paris Sér. A-B* **283** (1976), Ai, A693–A695. MR 0424966. Zbl 0381.14005.

[Vas73] L. N. Vaserštein, Structure of the classical arithmetic groups of rank greater than 1, *Mat. Sb.* **20** (1973), 465–492. MR 0349864. Zbl 0291.14016. http://dx.doi.org/10.1070/SM1973v020n03ABEH001885.

[Ven94] T. N. Venkataramana, On systems of generators of arithmetic subgroups of higher rank groups, *Pacific J. Math.* **166** (1994), 193–212. MR 1306038. Zbl 0822.22005. http://dx.doi.org/10.2140/pjm.1994.166.193.

(Received: May 25, 2012)
(Revised: October 8, 2012)

School of Mathematics, Tata Institute of Fundamental Research, Mumbai, India
E-mail: venky@math.tifr.res.in