INTEGRAL REPRESENTATIONS OF THE INFINITE DIHEDRAL GROUP

JAUME AGUADÉ, CARLES BROTO, AND LAIA SAUMELL

1. Introduction.

We want to study the representations of the infinite dihedral group D_∞ in $GL_2(R)$, where R is either the valuation ring $\mathbb{Z}_{(p)}$ of rational numbers with denominator prime to p or the ring of p-adic integers $\mathbb{Z}_p$ for some prime p.

The motivation for this research comes from the homotopy theory of classifying spaces of Kac-Moody groups. Associated to each generalized Cartan matrix (see, for instance, the introduction of [2]), one can define a (not necessarily finite dimensional) Lie algebra which can be integrated in some way which we will not discuss here (see [5]) to produce a topological group K called a Kac-Moody group. These topological groups, and their classifying spaces, have been studied from a homotopical point of view in several recent papers ([6],[3], [2], [1]). Like in the Lie group case, K has a maximal torus T and a Weyl group W which acts on the Lie algebra of T as a cristalographic group. However, in contrast to what happens in the Lie group case, this Weyl group can be infinite. If we start with a non-singular 2×2 Cartan matrix, we have a (non-afine) Kac-Moody group of rank two and then the Weyl group is infinite dihedral and we obtain a representation of D_∞ in $GL_2(\mathbb{Z})$ associated to K. In [1] we have investigated the cohomology of the classifying spaces of these rank two Kac-Moody groups and their central quotients and we have seen that this cohomology is intimately related to the representation theory of D_∞ over $\mathbb{Z}_p$. This research has lead us to investigate the representations of D_∞ from a purely algebraic point of view and the present paper, which can be read completely independently from [1] and which does not use any result from the theory of Kac-Moody groups, is the outcome of our research.

The set $\mathrm{Rep}(D_\infty)$ of rank two representations of D_∞ over R is first divided into different subsets according to the restriction of the representations to the two generating involutions of D_∞ (see sections 2 and 3). Then each of these subsets is described according to a system of numerical invariants, taking values in either R or $\mathbb{N}\cup\{\infty\}$, that classify and parametrize each of these subsets (see Theorems 2, 3, and 4).

While the homotopy theory of Kac-Moody groups of rank two has been the main motivation for the present paper, it is interesting to remark that the ideas behind our classification theorems (the invariants called Γ, δ, etc.) also come from [1]. Hence, this paper is a further example of the way in which cohomological invariants can lead to the solution of problems in pure algebra.

The authors acknowledge support from MCYT grant BFM2001-2035.

In a final section, we relate our results to those of [4], where one finds a classification of the representations of D_∞ over any field of characteristic $\neq 2$.

Through the paper we denote by ν_p the p-adic valuation on R.

2. Representations of $\mathbb{Z}/2\mathbb{Z}$.

We start understanding the representations of the group of two elements in $GL_2(R)$. Consider the matrices

$$A_0 = I, \quad A_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad A_3 = -I.$$

Proposition 1. *Up to conjugation, the matrices of order two in $GL_2(R)$ are A_1, A_2, A_3 for $p = 2$ and A_1, A_3 for $p > 2$.*

Proof. Let σ be a representation of $\mathbb{Z}/2$ in $GL_2(R)$ and let L be the corresponding $\mathbb{Z}/2$-lattice. Let r be the generator of $\mathbb{Z}/2$. There is an exact sequence of $\mathbb{Z}/2$-lattices

$$0 \longrightarrow L^{\mathbb{Z}/2} \longrightarrow L \longrightarrow L\big/L^{\mathbb{Z}/2} \longrightarrow 0\,.$$

$L\big/L^{\mathbb{Z}/2}$ is torsion free since for any $x \in L$ with αx invariant for some $\alpha \in R$, x itself is invariant. We can distinguish three cases according to the rank of $L^{\mathbb{Z}/2}$.

- $L^{\mathbb{Z}/2}$ **of rank 2:** In this case $L\big/L^{\mathbb{Z}/2}$ is of rank 0, hence trivial, and therefore $L = L^{\mathbb{Z}/2}$. The representation is trivial: $\sigma_0(r) = I$.
- $L^{\mathbb{Z}/2}$ **of rank 1:** Now $L^{\mathbb{Z}/2} = R$ with trivial action and then $L\big/L^{\mathbb{Z}/2} \cong \underline{R}$ is a copy of R with action of $\mathbb{Z}/2$ given by sign change. In fact, for any $x \in L$, $x + r(x) \in L^{\mathbb{Z}/2}$, hence $\overline{r(x)} = -\overline{x}$ in $L\big/L^{\mathbb{Z}/2}$.
- $L^{\mathbb{Z}/2}$ **of rank 0:** This is to say $L^{\mathbb{Z}/2} = 0$. Same argument as above shows that $r(x) = -x$ for all $x \in L$. The representation is given by sign change; that is, $\sigma_3(r) = -I$.

It remains to describe the possible representations with invariants of rank one. These $\mathbb{Z}/2$-lattices will be all possible extensions

$$0 \longrightarrow R \longrightarrow L \longrightarrow \underline{R} \longrightarrow 0$$

and such extensions are classified by $\operatorname{Ext}^1_{\mathbb{Z}/2}(\underline{R}\,, R)$. The exact sequence of $R[\mathbb{Z}/2]$-modules

$$0 \longrightarrow R \xrightarrow{f} R[\mathbb{Z}/2] \xrightarrow{g} \underline{R} \longrightarrow 0$$

with $f(1) = 1 + r$ and $g(1) = 1$, $g(r) = -1$ gives

$$\operatorname{Ext}^1_{\mathbb{Z}/2}(\underline{R}\,, R) \cong \begin{cases} \mathbb{Z}/2 & , p = 2 \\ 0 & , p > 2\,. \end{cases}$$

Hence, there is only one representation for p odd and two non equivalent representations for $p = 2$ given by

$$\sigma_1(r) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad \sigma_2(r) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

which are clearly non-conjugated because their mod 2 reductions are non-conjugated in $GL_2(\mathbb{Z}/2)$. $\square$

3. Representations of D_∞.

Recall that the infinite dihedral group D_∞ has a presentation with two generators r_1, r_2 of order two and no other relations: $D_\infty \cong \mathbb{Z}/2 * \mathbb{Z}/2$. D_∞ has an infinite cyclic subgroup D_∞^+ of index two generated by r_1r_2 and so we can se D_∞ as an extension of $\mathbb{Z}/2\mathbb{Z}$ by $D_\infty^+ \cong \mathbb{Z}$. On the other side, D_∞ has only one non trivial outer automorphism which interchanges the two generators r_1 and r_2.

A representation of D_∞ in $GL_2(R)$ gives two representations σ_1, σ_2 of $\mathbb{Z}/2$. These representations have been studied in proposition 1. Thus the set $\mathrm{Rep}(D_\infty)$ of representations of D_∞ in $GL_2(R)$ splits as a disjoint union

$$\mathrm{Rep}(D_\infty) = \coprod_{i,j\in \mathrm{Rep}(\mathbb{Z}/2)} \mathrm{Rep}_{i,j}\,,$$

where $\mathrm{Rep}_{i,j}$ stands for the subset of $\mathrm{Rep}(D_\infty)$ of representations that restrict to $i \in \mathrm{Rep}(\mathbb{Z}/2)$ on r_1 and to $j \in \mathrm{Rep}(\mathbb{Z}/2)$ on r_2. Notice that by proposition 1 the index set $\mathrm{Rep}(\mathbb{Z}/2)$ can be identified to $\{0,1,2,3\}$ for $p=2$ and to $\{0,1,3\}$ for $p>2$ (0 means the trivial representation). Given a matrix $M \in GL_2(R)$ and given representations σ_i, σ_j of $\mathbb{Z}/2$ given by matrices A_i, A_j, we can consider the representation $\rho \in \mathrm{Rep}_{i,j}$ given by $\rho(r_1) = A_i$ and $\rho(r_2) = M^{-1}A_jM$. This assignment yields a bijection

$$C(A_j)\backslash GL_2(R)/C(A_i) \cong \mathrm{Rep}_{i,j}$$

where $C(A)$ denotes the centralizer of A in $GL_2(R)$. After this identification, the non trivial outer automorphism of D_∞ interchanges $\mathrm{Rep}_{i,j}$ and $\mathrm{Rep}_{j,i}$ and acts on $\mathrm{Rep}_{i,i}$ by $M \mapsto M^{-1}$. Then, since the matrices A_0 and A_3 are central, in order to determine $\mathrm{Rep}(D_\infty)$ we only have to study $\mathrm{Rep}_{1,1}$ for any prime and $\mathrm{Rep}_{1,2}$ and $\mathrm{Rep}_{2,2}$ for $p=2$.

The abelianization of D_∞ is the non-cyclic group of order four. Hence, there are four one-dimensional representations of D_∞ which produce ten reducible two-dimensional representations. Eight of these belong to each of the eight sets $\mathrm{Rep}_{i,j}$ where i or j belongs to $\{0,3\}$. The other two representations are in $\mathrm{Rep}_{1,1}$ and they correspond to the matrices I and $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$.

4. Representations of type $(1,1)$.

The centralizer of A_1 is the subgroup $\mathcal{D}$ of diagonal matrices in $GL_2(R)$. Hence, $\mathrm{Rep}_{1,1} \cong \mathcal{D}\backslash GL_2(R)/\mathcal{D}$. Let α, β, $\Gamma_{1,1}$ be the functions defined on $GL_2(R)$ by

$$\alpha\begin{pmatrix}x & y\\ z & t\end{pmatrix} = \nu_p(xz),$$

$$\beta\begin{pmatrix}x & y\\ z & t\end{pmatrix} = \nu_p(yt),$$

$$\Gamma_{1,1}\begin{pmatrix}x & y\\ z & t\end{pmatrix} = \frac{xt}{xt-yz} \in R.$$

Theorem 2. *The functions* $\Gamma_{1,1}$*,* α *and* β *are well defined on* $\mathrm{Rep}_{1,1}$ *and are a complete system of invariants.*

Proof. One checks immediately that $\Gamma_{1,1}$, α and β are well defined on the double cosets of $\mathcal{D}\backslash GL_2(R)/\mathcal{D}$. By a complete system of invariants we mean that two matrices are in the same coset if and only if the invariants take the same value on both matrices. Let $M = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$. If $\Gamma_{1,1}(M) \not\equiv 0\,(p)$ then $M \sim \begin{pmatrix} 1 & y/x \\ z/t & 1 \end{pmatrix}$. If $M' = \begin{pmatrix} x' & y' \\ z' & t' \end{pmatrix}$ and $\Gamma_{1,1}(M) = \Gamma_{1,1}(M')$, $\nu_p(xz) = \nu_p(x'z')$ and $\nu_p(yt) = \nu_p(y't')$ then we see that $yz/xt = y'z'/x't'$ and yx'/xy' is a unit or $yz = 0$. In any case, we see that M and M' are in the same coset.

If $\Gamma_{1,1}(M) \equiv 0\,(p)$ then, since $\det(M)$ is a unit, we have $yz \not\equiv 0\,(p)$ and we can repeat the same argument above, after interchanging the two columns. □

One can check easily that the table 1 gives a complete set of representatives for $\mathrm{Rep}_{1,1}$ without repetition.

				$\Gamma_{1,1}$	α	β
$\Gamma_{1,1} \not\equiv 0\,(p)$	1	$\begin{pmatrix} 1 & 0 \\ p^r & 1 \end{pmatrix}$	$r = 0, \ldots, \infty$	1	r	∞
	2	$\begin{pmatrix} 1 & p^s \\ x & 1 \end{pmatrix}$	$s \geq 0,\ x \in R,\ p^s x \not\equiv 1\,(p)$	$\frac{1}{1-p^s x}$	$\nu_p(x)$	$s \neq \infty$
$\Gamma_{1,1} \equiv 0\,(p)$	3	$\begin{pmatrix} 0 & 1 \\ 1 & p^r \end{pmatrix}$	$r = 0, \ldots, \infty$	0	∞	r
	4	$\begin{pmatrix} p^s & 1 \\ 1 & x \end{pmatrix}$	$s \geq 0,\ x \in R,\ p^s x \not\equiv 1\,(p)$ $s = 0 \Rightarrow x \equiv 0\,(p)$	$\frac{p^s x}{p^s x - 1}$	$s \neq \infty$	$\nu_p(x)$

TABLE 1. $\mathrm{Rep}_{1,1}$

One sees also that the range of the invariants $\Gamma_{1,1}$, α, β is $R \times \{0, 1, \ldots, \infty\}^2$, subject only to the restrictions:

$$\begin{aligned} \alpha + \beta = \infty \ &\Rightarrow\ \Gamma_{1,1} = 0,\ 1 \\ 0 < \alpha + \beta < \infty \ &\Rightarrow\ \nu_p(\Gamma_{1,1} - 1) = \alpha + \beta - \nu_p(\Gamma_{1,1}) \\ \alpha + \beta = 0 \ &\Rightarrow\ \nu_p(\Gamma_{1,1}) = \nu_p(\Gamma_{1,1} - 1) = 0 \end{aligned}$$

The non-trivial outer automorphism of D_∞ leaves $\Gamma_{1,1}$ invariant. It also leaves α and β invariant in the types 1 and 2 in the table and permutes α and β in the types 3 and 4. Recall also that the two reducible representations in $\mathrm{Rep}_{1,1}$ are precisely those with $\alpha = \beta = \infty$.

5. Representations of type $(1,2)$.

We can assume from now on that $p=2$. The centralizer of A_2 in $GL_2(R)$ is the subgroup

$$\mathcal{S}=\left\{\begin{pmatrix} a & b \\ b & a\end{pmatrix}\in GL_2(R)\right\}.$$

Hence

$$\mathcal{S}\backslash GL_2(R)/\mathcal{D} \xrightarrow{\cong} \mathrm{Rep}_{1,2}$$

Let $\Gamma_{1,2}$, γ be the functions defined on $GL_2(R)$ by

$$\Gamma_{1,2}\begin{pmatrix} x & y \\ z & t\end{pmatrix}=\frac{zt-xy}{xt-yz}\in R.$$

$$\gamma\begin{pmatrix} x & y \\ z & t\end{pmatrix}=\begin{cases}0 & yt \text{ even}\\ 1 & yt \text{ odd.}\end{cases}$$

Theorem 3. *The functions* $\Gamma_{1,2}$ *and* γ *are well defined on* $\mathrm{Rep}_{1,2}$ *and are a complete system of invariants.*

Proof. An easy direct computation shows that $\Gamma_{1,2}$ and γ are well defined on the double cosets in $\mathcal{S}\backslash GL_2(R)/\mathcal{D}$. Assume now that $\Gamma_{1,2}\left(\begin{smallmatrix} x & y \\ z & t\end{smallmatrix}\right)=\lambda$. Since $\left(\begin{smallmatrix} x & y \\ z & t\end{smallmatrix}\right)\sim\left(\begin{smallmatrix} z & t \\ x & y\end{smallmatrix}\right)$ we can assume that $xt\equiv 1\,(2)$. If y is even then

$$\begin{pmatrix} 1 & -\frac{y}{t} \\ -\frac{y}{t} & 1\end{pmatrix}\begin{pmatrix} x & y \\ z & t\end{pmatrix}\begin{pmatrix} \frac{t}{xt-yz} & 0 \\ 0 & \frac{t}{t^2-y^2}\end{pmatrix}=\begin{pmatrix} 1 & 0 \\ \lambda & 1\end{pmatrix}.$$

If y is odd then z is even and then

$$\begin{pmatrix} 1 & -\frac{z}{x} \\ -\frac{z}{x} & 1\end{pmatrix}\begin{pmatrix} x & y \\ z & t\end{pmatrix}\begin{pmatrix} \frac{x}{x^2-z^2} & 0 \\ 0 & \frac{x}{xt-yz}\end{pmatrix}=\begin{pmatrix} 1 & -\lambda \\ 0 & 1\end{pmatrix}.$$

We have hence proved that

$$\Gamma_{1,2}^{-1}(\lambda)=\begin{cases}\left[\left(\begin{smallmatrix} 1 & 0 \\ \lambda & 1\end{smallmatrix}\right)\right], & \lambda \text{ even}\\ \left\{\left[\left(\begin{smallmatrix} 1 & 0 \\ \lambda & 1\end{smallmatrix}\right)\right],\left[\left(\begin{smallmatrix} 1 & -\lambda \\ 0 & 1\end{smallmatrix}\right)\right]\right\}, & \lambda \text{ odd.}\end{cases}$$

And the proposition follows. □

As representatives for the double cosets in $\mathrm{Rep}_{1,2}$ one can take the matrices

$$\begin{pmatrix} 1 & 0 \\ z & 1\end{pmatrix},\ z\in R;\quad \begin{pmatrix} 1 & y \\ 0 & 1\end{pmatrix},\ y\in R^*.$$

6. Representations of type $(2,2)$.

Here the situation is more involved that in the two previous cases. We know that $\mathrm{Rep}_{2,2}$ is equivalent to the double cosets

$$\mathcal{S}\backslash GL_2(R)/\mathcal{S}.$$

As before, we introduce some invariants. We define functions $\Gamma_{2,2}$, ϵ, $\bar{\epsilon}$ and δ on a matrix $\left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right)$ as follows

$$\begin{aligned} \Gamma_{2,2} &= \frac{x^2+t^2-y^2-z^2}{xt-yz} \in R; \\ \epsilon &= \nu_2(y+t-x-z); \\ \bar{\epsilon} &= \nu_2(y+t+x+z); \\ \delta &= \min\left\{\nu_2(x^2+z^2-y^2-t^2), \nu_2(xz-yt)\right\}. \end{aligned}$$

It is relatively straightforward to show by a direct calculation that these functions are well defined on $\mathrm{Rep}_{2,2}$. Actually, the only thing that needs some more careful check is the invariance of δ under left multiplication by a matrix in $\mathcal{S}$, but this is not difficult. Then:

Theorem 4. *The functions $\Gamma_{2,2}$, ϵ, $\bar{\epsilon}$ and δ are a complete system of invariants for* $\mathrm{Rep}_{2,2}$.

The proof of this result is quite lengthy. We start with a criterion to decide if two matrices are in the same coset.

Proposition 5.

(1) *Any coset $[\left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right)]$ has a representative of the form $\left(\begin{smallmatrix} 1 & u \\ 0 & v \end{smallmatrix}\right)$. If we assume (no loss of generality) that x is odd and z is even then we can take*

$$u = \frac{xy-zt}{x^2-z^2}, \qquad v = \frac{xt-yz}{x^2-z^2}.$$

(2) *Two different matrices $M = \left(\begin{smallmatrix} 1 & u \\ 0 & v \end{smallmatrix}\right)$ and $M' = \left(\begin{smallmatrix} 1 & u' \\ 0 & v' \end{smallmatrix}\right)$ are in the same coset if and only if $\Gamma_{2,2}(M) = \Gamma_{2,2}(M')$ and either $\nu_2(v-v') \neq \nu_2(vu'+uv')$ or $\nu_2(u-u') \neq \nu_2(uu'+vv'-1)$. In particular, if uu' is odd then M and M' are in the same coset if and only if $\Gamma_{2,2}(M) = \Gamma_{2,2}(M')$.*

Proof. Since we can permute rows and columns, there is no loss of generality in assuming that x is odd and z is even. Then

$$\begin{pmatrix} \frac{x^2}{x^2-z^2} & \frac{-zx}{x^2-z^2} \\ \frac{-zx}{x^2-z^2} & \frac{x^2}{x^2-z^2} \end{pmatrix} \begin{pmatrix} x & y \\ z & t \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & x^{-1} \end{pmatrix} = \begin{pmatrix} 1 & u \\ 0 & v \end{pmatrix}$$

which shows (1). To prove (2) notice that M and M' are equivalent if and only if there are matrices $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} c & d \\ d & c \end{smallmatrix}\right)$ with a^2-b^2 and c^2-d^2 both odd and such that

$$\begin{pmatrix} 1 & u \\ 0 & v \end{pmatrix} \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} 1 & u' \\ 0 & v' \end{pmatrix}.$$

This equation implies $a = c + ud$, $b = vd$ and c and d must be solutions of the linear system of equations

$$\left.\begin{array}{rcl}(u'-u)\,c + (uu'+vv'-1)\,d &=& 0\\ (v'-v)\,c + (vu'+uv')\,d &=& 0\end{array}\right\}$$

The vanishing of the determinant of this linear system is equivalent to both matrices $\left(\begin{smallmatrix}1 & u\\ 0 & v\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & u'\\ 0 & v'\end{smallmatrix}\right)$ having the same value of the $\Gamma_{2,2}$ invariant. We also require that c and d have opposite parity. This is possible if and only if $\nu_2(v-v') \neq \nu_2(vu'+uv')$ or $\nu_2(u-u') \neq \nu_2(uu'+vv'-1)$. Notice that the two inequalities are essentially equivalent, unless $v = v'$ or $u = u'$. The proposition is proven. $\square$

Proof of theorem 4. The theorem is proven by contradiction. We assume that we have a counterexample which, by proposition 5, is not restrictive to suppose that it is given by two matrices of the form $\left(\begin{smallmatrix}1 & u\\ 0 & v\end{smallmatrix}\right)$. More precisely, we assume that there are u, v, u', v' such that the matrices $\left(\begin{smallmatrix}1 & u\\ 0 & v\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1 & u'\\ 0 & v'\end{smallmatrix}\right)$ have the same invariants $\Gamma_{2,2}$, ϵ, $\bar{\epsilon}$ and δ:

$$\begin{array}{rcl}v'(1+v^2-u^2) &=& v(1+v'^2-u'^2)\\ \nu_2(u+v-1) &=& \nu_2(u'+v'-1)\\ \nu_2(u+v+1) &=& \nu_2(u'+v'+1)\\ \min\left\{\nu_2(u), \nu_2(u^2+v^2-1)\right\} &=& \min\left\{\nu_2(u'), \nu_2(u'^2+v'^2-1)\right\}\end{array}$$

and we assume also that the criterion for non-equivalence given by proposition 5 holds:

$$\begin{array}{rcl}\nu_2(u-u') &=& \nu_2(uu'+vv'-1)\\ \nu_2(v-v') &=& \nu_2(uv'+u'v)\,.\end{array}$$

Then, we will investigate which properties should u, v, u', v' have till we conclude that $u = u'$ and $v = v'$, which ends the proof.

$\boxed{u \text{ and } u' \text{ are even}}$

Notice that u is odd if and only if $\Gamma_{2,2}$ is odd, but if both u and u' are odd then $\Gamma_{2,2}$ classifies the coset of the matrix (cf. proposition 5).

$\boxed{\nu_2(u) = \nu_2(u')}$

Assume this were not true. Then, let us write $u = 2^a\lambda$, $u' = 2^{a'}\lambda'$ with $1 \leq a < a'$ and $\lambda\lambda'$ odd (or $u' = 0$). Then we can write

$$\begin{array}{rcl}v &=& 2^b\mu - 2^a\lambda \pm 1\\ v' &=& 2^b\mu' - 2^{a'}\lambda' \pm 1\end{array}$$

with $\mu\mu'$ odd and $b > 1$. To see this, notice that either ϵ or $\bar{\epsilon}$ is > 1. If $\epsilon > 1$ then we take $b = \epsilon$ and the plus sign in both equations; If $\epsilon = 1$ then we take $b = \bar{\epsilon}$ and the minus sign in both equations.

Then:

$$\begin{array}{rcl}u^2+v^2-1 &=& 2^{2a+1}\lambda^2 + 2^{2b}\mu^2 - 2^{a+b+1}\lambda\mu \pm 2^{b+1}\mu \mp 2^{a+1}\lambda\\ u'^2+v'^2-1 &=& 2^{2a'+1}\lambda'^2 + 2^{2b}\mu'^2 - 2^{a'+b+1}\lambda'\mu' \pm 2^{b+1}\mu' \mp 2^{a'+1}\lambda'.\end{array}$$

If we check now the values of the invariant δ we see easily that the cases $b \geq a' > a$ and $a' > b \geq a$ are impossible. Hence, we have $1 < b < a < a'$ and we can write

$$\begin{aligned} v &= 2^b\tau \pm 1 \\ v' &= 2^b\tau' \pm 1 \end{aligned}$$

with $\tau\tau'$ odd and $\tau \neq \tau'$ (notice that $\tau = \tau'$ would imply $u' = \pm u$ and $a = a'$). Then

$$b + \nu_2(\tau - \tau') = \nu_2(v - v') = \nu_2(uv' + u'v) = a$$

and we can write $\tau' = \tau + 2^{a-b}\rho$ for some odd ρ. Let us consider now the equality $v'(1 + v^2 - u^2) = v(1 + v'^2 - u'^2)$ as a quadratic equation on τ. It yields

$$\begin{aligned} &[2^{b-1}\rho]\tau^2 + [2^{a-1}(\lambda^2 + \rho^2) - 2^{2a'-a-1}\lambda'^2 \pm \rho]\tau \\ &\qquad + [2^{2a-b-1}\lambda^2\rho \pm 2^{a-b-1}(\lambda^2 + \rho^2) \mp 2^{2a'-a-b-1}\lambda'^2] = 0 \end{aligned}$$

which is absurd, since the quadratic term and the independent term are both even while the linear term is odd.

Since the case $u = u' = 0$ is trivial, we can write $u = 2^a\lambda$, $u' = 2^a\lambda'$, $u+v = 2^b\mu\pm 1$, $u' + v' = 2^b\mu' \pm 1$ with $b > 1$ and $\lambda\lambda'\mu\mu'$ odd.

$\boxed{b \leq a}$

If $b > a$ then $u - u' = 2^a(\lambda - \lambda')$ while

$$uu' + vv' - 1 = 2^{2a+1}[\lambda\lambda' + 2^{2b-2a-1}\mu\mu' - 2^{b-a-1}(\lambda\mu' + \mu\lambda')] \pm 2^b(\mu + \mu') \mp 2^a(\lambda + \lambda').$$

Since $\nu_2(\lambda - \lambda') = 1$ if and only if $\nu_2(\lambda + \lambda') > 1$, one sees easily that $uu' + vv' - 1$ cannot have the same ν_2-valuation that $u - u'$, a contradiction.

$\boxed{b = a}$

Assume $b < a$ and write, as we did before,

$$\begin{aligned} v &= 2^b\tau \pm 1 \\ v' &= 2^b\tau' \pm 1 \end{aligned}$$

with $\tau\tau'$ odd. The case in which $\tau = \tau'$ leads easily to a contradiction in the following way. If $v = v'$ then the existence of the invariant $\Gamma_{2,2}$ implies $u' = \pm u$. But $u = -u'$ and $b < a$ contradict $\nu_2(u - u') = \nu_2(uu' + vv' - 1)$.

Hence, we can write $\tau' = \tau + 2^c\rho$ for some odd ρ. Like before, let us write the equality $v'(1 + v^2 - u^2) = v(1 + v'^2 - u'^2)$ as a quadratic equation on τ. It yields

$$\begin{aligned} &[2^{b-1}\rho]\tau^2 + [2^{2a-b-c-1}(\lambda^2 - \lambda'^2) + 2^{b+c-1}\rho^2 \pm \rho]\tau \\ &\qquad + [2^{2a-b-1}\lambda^2\rho \pm 2^{2a-2b-c-1}(\lambda^2 - \lambda'^2) \pm 2^{c-1}\rho^2] = 0 \end{aligned}$$

Now,

$$b + c = \nu_2(v - v') = \nu_2(uv' + vu') = \nu_2(2^a(\lambda + \lambda')v + 2^{a+b+c}\lambda\rho)$$

implies $\nu_2(\lambda + \lambda') = b + c - a$ (and, in particular, $c > 1$). Then we see that both the quadratic and the independent term in the quadratic equation above are even, while the linear term is odd, which is absurd.

Hence, we have $a = b$ and, in particular, $a > 1$ and we can write

$$\begin{aligned} v &= 2^d\eta \pm 1 \\ v' &= 2^{d'}\eta' \pm 1 \end{aligned}$$

with $\nu\nu'$ odd and $1 < a < d \leq d'$.

$\boxed{d = d'}$

The equation $v\Gamma_{2,2} = 1 + v^2 - u^2$ yields

$$2^{2a}\lambda^2 = 2^{2d}\eta^2 - v(\Gamma_{2,2} \mp 2)$$

and, if we write $\Gamma_{2,2} \mp 2 = 2^{2a}\gamma$ with γ odd, we get

$$\lambda^2 = 2^{2(d-a)}\eta^2 - (2^d\eta \pm 1)\gamma$$

and this yields

$$(\dagger) \qquad \lambda^2 - \lambda'^2 = 2^{2(d-a)}\eta^2 - 2^{2(d'-a)}\eta'^2 - 2^d\eta\gamma + 2^{d'}\eta'\gamma.$$

If we assume $d < d'$ we get

$$(\ddagger) \qquad d = \nu_2(v - v') = \nu_2(uv' + u'v) = a + \nu_2(2^{d'}\lambda\eta' + 2^d\lambda'\eta \pm (\lambda + \lambda')).$$

If this last term in brackets has ν_2-valuation 1, then $d = a + 1$ and ($\dagger$) implies that $\nu_2(\lambda^2 - \lambda'^2) = 2$, which is absurd. Hence, $d - a > 1$ and $\nu_2(\lambda + \lambda') > 1$ and $\nu_2(\lambda^2 - \lambda'^2) = \nu_2(\lambda + \lambda') + 1$.

Let us consider now the equations ($\dagger$) and ($\ddagger$), according to the relative values of a and d.

- If $d > 2a$ then ($\dagger$) implies $\nu_2(\lambda + \lambda') = d - 1$ and ($\ddagger$) yields $d = a + d - 1$, which is absurd.
- If $d < 2a$, then ($\dagger$) implies that $\nu_2(\lambda + \lambda') = 2d - 2a - 1 < d$ and ($\ddagger$) yields $d - a = 1$ which we have already seen that is not possible.
- If $d = 2a$ then ($\dagger$) implies $\nu_2(\lambda + \lambda') \geq 2a$ which contradicts ($\ddagger$).

$\boxed{v = v'}$

Like in the previous case, we have the equality

$$(\S) \qquad \lambda^2 - \lambda'^2 = (\eta - \eta')[2^{2(d-a)}(\eta + \eta') - 2^d\gamma].$$

Now, if $v \neq v'$, we can write $\eta' = \eta + 2^e k$ for some odd k and $e \geq 1$. This yields

$$(\P) \qquad d + e = \nu_2(v - v') = \nu_2(vu' + uv') = a + \nu_2((\lambda + \lambda')(2^d\eta \pm 1) + 2^{d+e}\lambda k).$$

This implies immediately $\nu_2(\lambda + \lambda') > 1$ and therefore $\nu_2(\lambda - \lambda') = 1$. Also, ($\P$) implies $\nu_2(\lambda + \lambda') < d + e$ and we have

$$d + e = a + \nu_2(\lambda + \lambda').$$

But ($\S$) implies

$$d + e - a + 1 = \nu_2(\lambda + \lambda') + 1 = e + \nu_2(2^{2(d-a)}(\eta + \eta') - 2^d\gamma)$$

which is impossible.

$\boxed{u = u'}$

Since $v = v'$, we have $u = \pm u'$. If $u' = -u$ then we notice that

$$a + 1 = \nu_2(u + u) = \nu_2(-u^2 + v^2 - 1) = \nu_2(-2^{2a}\lambda^2 + 2^{2d}\eta^2 \pm 2^{d+1}\eta)$$

with $d > a > 1$, which is absurd.

This ends the proof of the theorem. □

The above result provides an effective classification of representations of D_∞ of type $(2, 2)$. However, unlikely to what happens in $\mathrm{Rep}_{1,1}$ or $\mathrm{Rep}_{1,2}$, we see no obvious way to select a complete list of coset representatives. To give a hint of the kind of phenomena that occur, we include here a sample of results about matrices which have simple coset representatives.

Proposition 6. *If $\Gamma_{2,2}(M)$ is odd, then $M \sim \left(\begin{smallmatrix} 1 & 1 \\ 0 & \Gamma_{2,2}(M) \end{smallmatrix}\right)$.*

Proof. Take $M \sim \left(\begin{smallmatrix} 1 & u \\ 0 & v \end{smallmatrix}\right)$. Then u is odd and we know that in this case the invariant $\Gamma_{2,2}$ suffices to classify M. □

The next results are only valid when the ground ring is the ring $\mathbb{Z}_2$ of the 2-adic integers. Let us recall that a 2-adic integer $x \neq 0$ is a square in R if and only if there exists $r \geq 0$ such that $x = 2^{2r}y$ with $y \equiv 1\,(8)$.

Proposition 7. *Assume $R = \mathbb{Z}_2$. If $\delta(M) = 1$ then $M \sim \left(\begin{smallmatrix} 1 & 2 \\ 0 & v \end{smallmatrix}\right)$ for some unique v.*

Proof. Take $M \sim \left(\begin{smallmatrix} 1 & u \\ 0 & v \end{smallmatrix}\right)$. Then, one sees easily that the condition on $\delta(M)$ is equivalent to $\nu_2(u) = 1$, so we write $u = 2\lambda$ with λ odd. If we want to look for a matrix $\left(\begin{smallmatrix} 1 & 2 \\ 0 & v' \end{smallmatrix}\right)$ with the same value of the invariant $\Gamma_{2,2}$ than the matrix M, we need to solve a quadratic equation on v':

$$vv'^2 + (u^2 - v^2 - 1)v' - 3v = 0.$$

This equation has a solution in $\mathbb{Z}_2$ if and only if the discriminant Δ is a square. If we write $v^2 = 8k + 1$ we see that

$$\Delta = 16(4k^2 + \lambda^4 - \lambda^2 + 8k - 4\lambda^2 k + 1),$$

which is, indeed, a square in $\mathbb{Z}_2$, $\Delta = (\pm 4\omega)^2$. Then, we have two possible values for v', given by

$$vv' = \frac{1 + v^2 - u^2}{2} \pm 2\omega.$$

To conclude that $M \sim \left(\begin{smallmatrix} 1 & 2 \\ 0 & v' \end{smallmatrix}\right)$ we need to check that $\nu_2(u - 2) \neq \nu_2(2u + vv' - 1)$, but it is easy to see that there is always a choice of the sign of ω which makes this inequality hold.

To see the uniqueness of v', notice that the invariant $\Gamma_{2,2}$ applied to $\left(\begin{smallmatrix} 1 & 2 \\ 0 & v \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} 1 & 2 \\ 0 & v' \end{smallmatrix}\right)$ yields $v' = v$ or $v' = -3/v$. But this second value of v' gives $\nu_2(v - v') = \nu_2(2v' + 2v)$. □

Proposition 8. *Assume $R = \mathbb{Z}_2$. If $\nu_2(u) > \nu_2(v^2 - 1)$ then $\left(\begin{smallmatrix} 1 & u \\ 0 & v \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} 1 & 0 \\ 0 & v' \end{smallmatrix}\right)$ for some unique v'.*

Proof. Like in the previous proposition, let us first look for a matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & v' \end{smallmatrix}\right)$ with the same value of $\Gamma_{2,2}$ than the original matrix $\left(\begin{smallmatrix} 1 & u \\ 0 & v \end{smallmatrix}\right)$. We need to solve the quadratic equation

$$vv'^2 + (u^2 - v^2 - 1)v' + v = 0$$

i.e. we need to prove that the discriminant Δ of this equation is a square in $\mathbb{Z}_2$. Let us write $u = 2^a\lambda$, $v^2 = 2^b\eta + 1$ with $\lambda\eta$ odd and $b \geq 3$. Then,

$$\Delta = 2^{2b}[2^{4a-2b}\lambda^4 + \eta^2 - 2^{2a-b+1}\lambda^2\eta - 2^{2a-2b+2}\lambda^2]$$

and we see that the condition $3 \leq b < a$ implies that Δ is a square, $\Delta = (\pm 2^b\omega)^2$ and

$$vv' = \frac{1 + v^2 - u^2}{2} \pm 2^{b-1}\omega = 2^{b-1}(\eta \pm \omega) - 2^{2a}\lambda^2 + 1.$$

Now, like in the preceding proposition, we can choose the sign of ω in a way that $\nu_2(u) \neq \nu_2(vv' - 1)$.

The uniqueness part is trivial. □

These two last propositions may induce the reader to believe that there are always coset representatives of the form $\left(\begin{smallmatrix} 1 & 2^r \\ 0 & v \end{smallmatrix}\right)$. The following example shows that this is not true.

Proposition 9. $\left(\begin{smallmatrix} 1 & 12 \\ 0 & \sqrt{17} \end{smallmatrix}\right) \not\sim \left(\begin{smallmatrix} 1 & 2^r \\ 0 & v \end{smallmatrix}\right)$ *for any r and any v.*

Proof. The invariant δ of the matrix $\left(\begin{smallmatrix} 1 & 12 \\ 0 & \sqrt{17} \end{smallmatrix}\right)$ has value 2, while the δ invariant of the matrix $\left(\begin{smallmatrix} 1 & 2^r \\ 0 & v \end{smallmatrix}\right)$ is equal to 2 only if $r = 2$. Then, $\Gamma_{2,2}\left(\begin{smallmatrix} 1 & 12 \\ 0 & \sqrt{17} \end{smallmatrix}\right) = \Gamma_{2,2}\left(\begin{smallmatrix} 1 & 4 \\ 0 & v \end{smallmatrix}\right)$ if and only if v satisfies the quadratic equation $v^2 - \frac{126}{\sqrt{17}}v - 15 = 0$, which has no roots in $\mathbb{Z}_2$ because its discriminant is not a square. □

7. Representations over a field

The representations of D_∞ over a field k of characteristic $\neq 2$ have been studied by Đokovič in [4]. Although our aim in this paper has been to study the *integral* representations of D_∞, it seems worthwhile, in order to present a more complete view of the representation theory of the dihedral group, to relate our results to those of [4]. We point out that the main result of [4] is slightly inaccurate in the two-dimensional case, which is the case we are dealing here with.

The irreducible representations of D_∞ in $GL_2(k)$, k a field of characteristic $\neq 2$, are the following:

(I): For any $\alpha \in k^*$, $\alpha \neq \pm 1$, the representation ρ_α given by

$$\begin{aligned} \rho_\alpha(r_2 r_1) &= \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \\ \rho_\alpha(r_1) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

with $\rho_\alpha \sim \rho_{\alpha^{-1}}$.

(II): For any $\beta \in k$ such that β^2-1 is either 0 or a non-square, the representation τ_β given by

$$\begin{aligned} \tau_\beta(r_2 r_1) &= \begin{pmatrix} 0 & -1 \\ 1 & 2\beta \end{pmatrix} \\ \tau_\beta(r_1) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

This follows from [4] in a quite straightforward way. Notice, however, that some of the representations which appear in the main theorem of [4] are redundant, because they become equivalent when the dimension is two.

In our case, k is the field of fractions of R, i.e. k is either the rational field $\mathbb{Q}$ or the field of p-adic numbers $\mathbb{Q}_p$. All irreducible representations are in $\mathrm{Rep}_{1,1}$. Hence, in the set of irreducible representations of D_∞ in $GL_2(k)$ we have the k-valued function $\Gamma = \Gamma_{1,1}$. This function classifies the representations:

Proposition 10. *Γ is a one-to-one correspondence between the set of irreducible representations of D_∞ in $GL_2(k)$ and k.*

Proof. The only thing that needs to be proved now is that each representation ρ_α, τ_β in the list above yields a different value of Γ.

First of all, a straightforward computation which we leave to the reader shows that

$$\begin{aligned} \Gamma(\rho_\alpha) &= \frac{(\alpha+1)^2}{4\alpha} \\ \Gamma(\tau_\beta) &= \frac{1+\beta}{2} \end{aligned}$$

Then, it is obvious that $\Gamma(\tau_\beta) = \Gamma(\tau_{\beta'})$ implies $\beta = \beta'$ and $\Gamma(\rho_\alpha) = \Gamma(\rho_{\alpha'})$ implies $\alpha' = \alpha, \alpha^{-1}$ and $\rho_\alpha \sim \rho_{\alpha'}$. On the other hand, if $\Gamma(\tau_\beta) = \Gamma(\rho_\alpha)$ then $\alpha \neq \pm 1$ is a root of the quadratic equation

$$X^2 - (4\Gamma(\tau_\beta) - 2)X + 1 = 0$$

and this implies that $\beta^2 - 1$ is a non-zero square and so τ_β is not in the list. □

Finally, we would like to be able to distinguish which of these representations are faithful and which are not. Clearly, this depends only on the representation over k. We have the following partial result:

Proposition 11. *Let $\rho : D_\infty \to GL_2(\mathbb{Z}_p)$ (p odd) be an irreducible representation with $\Gamma \equiv 0, 1\,(p)$. Then $\rho(D_\infty)$ has finite order if and only if $p = 3$ and $\Gamma = 3/4,\ 1/4$.*

Proof. It is clear that $\rho(D_\infty)$ has finite order if and only if the matrix $\omega = r_1 r_2$ is nilpotent. ω is a two-by-two matrix of determinant one. If we assume that ω is nilpotent then it has to be diagonalizable in $\mathbb{Q}_p$ or in some quadratic extension of $\mathbb{Q}_p$. If ζ, ζ^{-1} are the eigenvalues of ω then ζ is an m-th root of unity for some minimal m. Let us discuss in which cases this can happen.

If m is coprime to p then $\mathbb{Q}_p(\zeta)$ is unramified over $\mathbb{Q}_p$. The hypothesis on Γ implies that the mod p reduction of the characteristic polynomial of ω is $(x \pm 1)^2$ and so $\mathbb{Q}_p(\zeta)$

is totally ramified over $\mathbb{Q}_p$. Hence, $\mathbb{Q}_p(\zeta) = \mathbb{Q}_p$ and so ζ is an m-th root of unity in $\mathbb{Q}_p$ such that $\zeta \equiv \pm 1\,(p)$. Hence, we have $\zeta = \pm 1$, $\omega = \pm I$ and the representation is reducible.

Put $m = p^r n$ with n coprime to p and $r \geq 1$. Then ζ^n is a primitive p^r-th root of unity and we have

$$p^{r-1}(p-1) = [\mathbb{Q}_p(\zeta^n) : \mathbb{Q}_p] \leq [\mathbb{Q}_p(\zeta) : \mathbb{Q}_p] \leq 2.$$

Hence, $p = 3$ and $r = 1$. Moreover, as above, $\zeta^3 = \pm 1$. Since the characteristic polynomial of ω is $X^2 - 2(2\Gamma - 1)X + 1$, we obtain that $\Gamma = 3/4,\ 1/4$.

The converse is easy. □

References

[1] J. Aguadé, C. Broto, N. Kitchloo, L. Saumell, *Cohomology of classifying spaces of central quotients of rank two Kac-Moody groups.* Preprint.

[2] J. Aguadé, A. Ruíz, *Maps between classifying spaces of Kac-Moody groups.* To appear in Adv. Math.

[3] C. Broto, N. Kitchloo, *Classifying spaces of Kac-Moody groups.* Math. Z. 240 (2002), 621–649.

[4] D.Ž. Đokovič, *Pairs of Involutions in the General Linear Group.* J. Algebra 100 (1986), 214–223.

[5] V. G. Kac (ed.) *Infinite-dimensional groups with Applications.* Papers from the conference held at the Mathematical Sciences Research Institute, Berkeley, Calif., May 10–15, 1984. Math. Sci. Res. Inst. Publ., 4. Springer-Verlag, New York-Berlin, 1985.

[6] N. Kitchloo, *Topology of Kac-Moody groups.* Thesis, MIT, 1998.

Dep. de Matemàtiques, Universitat Autònoma de Barcelona, E-08193 Bellaterra, Spain

E-mail address: aguade@mat.uab.es broto@mat.uab.es laia@mat.uab.es