Invariants of Weil representations

Stephan Ehlen (joint work with Nils P. Skoruppa)

Winter seminar
March 12-18, 2017
Chalet Fleurs des Neiges, La Plagne, France

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Finite quadratic modules

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Finite quadratic modules

- (A, Q) a *finite quadratic module*,

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Finite quadratic modules

- (A, Q) a *finite quadratic module*,
- A is a finite abelian group

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Finite quadratic modules

- (A, Q) a *finite quadratic module*,
- A is a finite abelian group
- and $Q : A \to \mathbb{Q}/\mathbb{Z}$ a non-degenerate quadratic form

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Finite quadratic modules

- (A, Q) a *finite quadratic module*,
- A is a finite abelian group
- and $Q : A \to \mathbb{Q}/\mathbb{Z}$ a non-degenerate quadratic form
- with bilinear form $(x, y) := Q(x + y) - Q(x) - Q(y)$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Finite quadratic modules

- (A, Q) a *finite quadratic module*,
- A is a finite abelian group
- and $Q : A \to \mathbb{Q}/\mathbb{Z}$ a non-degenerate quadratic form
- with bilinear form $(x, y) := Q(x + y) - Q(x) - Q(y)$.
- The level N of A is the smallest $n \in \mathbb{N}$, such that $nQ(x) \in \mathbb{Z}$ for all $x \in A$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Finite quadratic modules

- (A, Q) a *finite quadratic module*,
- A is a finite abelian group
- and $Q : A \to \mathbb{Q}/\mathbb{Z}$ a non-degenerate quadratic form
- with bilinear form $(x, y) := Q(x + y) - Q(x) - Q(y)$.
- The level N of A is the smallest $n \in \mathbb{N}$, such that $nQ(x) \in \mathbb{Z}$ for all $x \in A$.
- Assume that N is odd (for this talk).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

The Weil representation

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

The Weil representation

- Let $G := \mathrm{SL}_2(\mathbb{Z})$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

The Weil representation

- Let $G := \mathrm{SL}_2(\mathbb{Z})$.
- G is generated by $S = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

The Weil representation

- Let $G := \mathrm{SL}_2(\mathbb{Z})$.
- G is generated by $S = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$.
- Define a representation $\rho = \rho_A$ of G on $\mathbb{C}[A] = \bigoplus_{x \in A} \mathbb{C}\mathfrak{e}_x$ via

$$\rho(T)\mathfrak{e}_x = e(Q(x))\mathfrak{e}_x,$$

$$\rho(S)\mathfrak{e}_x = \frac{e(-\operatorname{sig}(A)/8)}{\sqrt{|A|}} \sum_{y \in A} e\left(-(x,y)\right)\mathfrak{e}_y.$$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

The Weil representation

- Let $G := \mathrm{SL}_2(\mathbb{Z})$.
- G is generated by $S = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$.
- Define a representation $\rho = \rho_A$ of G on $\mathbb{C}[A] = \bigoplus_{x \in A} \mathbb{C}\mathfrak{e}_x$ via

$$\rho(T)\mathfrak{e}_x = e(Q(x))\mathfrak{e}_x,$$

$$\rho(S)\mathfrak{e}_x = \frac{e(-\operatorname{sig}(A)/8)}{\sqrt{|A|}} \sum_{y \in A} e\left(-(x,y)\right)\mathfrak{e}_y.$$

- $\operatorname{sig}(A) \in \mathbb{Z}/8\mathbb{Z}$ can be defined via Milgram's formula

$$\sum_{x \in A} e(Q(x)) = \sqrt{|A|}\, e(\operatorname{sig}(A)/8).$$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

The Weil representation

- Let $G := \mathrm{SL}_2(\mathbb{Z})$.
- G is generated by $S = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$.
- Define a representation $\rho = \rho_A$ of G on $\mathbb{C}[A] = \bigoplus_{x \in A} \mathbb{C}\mathfrak{e}_x$ via

$$\rho(T)\mathfrak{e}_x = e(Q(x))\mathfrak{e}_x,$$

$$\rho(S)\mathfrak{e}_x = \frac{e(-\operatorname{sig}(A)/8)}{\sqrt{|A|}} \sum_{y \in A} e\left(-(x,y)\right)\mathfrak{e}_y.$$

- $\operatorname{sig}(A) \in \mathbb{Z}/8\mathbb{Z}$ can be defined via Milgram's formula

$$\sum_{x \in A} e(Q(x)) = \sqrt{|A|}\, e(\operatorname{sig}(A)/8).$$

- This representation is called the *Weil representation* of G associated with A.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Theta functions

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Theta functions

- Significance: Theta functions transform with the Weil representation

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Theta functions

- Significance: Theta functions transform with the Weil representation
- If (L, Q) is an even positive definite lattice and L' its dual, then $A = L'/L$ with $Q \mod \mathbb{Z}$ is a finite quadratic module.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Theta functions

- Significance: Theta functions transform with the Weil representation
- If (L, Q) is an even positive definite lattice and L' its dual, then $A = L'/L$ with $Q \mod \mathbb{Z}$ is a finite quadratic module.
- The theta function

$$\Theta_L(\tau) := \sum_{\lambda \in L} \exp(2\pi i Q(\lambda)\tau)\mathfrak{e}_{\bar{\lambda}}$$

is a vector valued modular form of weight $\frac{n}{2}$ for ρ_A ($\bar{\lambda} = \lambda \mod L$).

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Theta functions

- Significance: Theta functions transform with the Weil representation
- If (L, Q) is an even positive definite lattice and L' its dual, then $A = L'/L$ with $Q \mod \mathbb{Z}$ is a finite quadratic module.
- The theta function

$$\Theta_L(\tau) := \sum_{\lambda \in L} \exp(2\pi i Q(\lambda)\tau)\mathfrak{e}_{\bar{\lambda}}$$

  is a vector valued modular form of weight $\frac{n}{2}$ for ρ_A ($\bar{\lambda} = \lambda \mod L$).
- Modular forms for the Weil representation occur in many places, for instance as input to regularized theta lifts.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Invariants

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Invariants

- We are interested in the space of G-invariants $\mathbb{C}[A]^G$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Invariants

- We are interested in the space of G-invariants $\mathbb{C}[A]^G$.
- For various reasons:

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Invariants

- We are interested in the space of G-invariants $\mathbb{C}[A]^G$.
- For various reasons:
- $\dim_{\mathbb{C}} \mathbb{C}[A]^G$ is one of the terms in the dimension formula for holomorphic cusp forms of weight 2.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Invariants

- We are interested in the space of G-invariants $\mathbb{C}[A]^G$.
- For various reasons:
- $\dim_{\mathbb{C}} \mathbb{C}[A]^G$ is one of the terms in the dimension formula for holomorphic cusp forms of weight 2.
- Also (the dimension formulas for) modular forms of weight $\frac{1}{2}$ and $\frac{3}{2}$ involve (the dimension of) $\mathbb{C}[A]^G$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Invariants

- We are interested in the space of G-invariants $\mathbb{C}[A]^G$.
- For various reasons:
- $\dim_{\mathbb{C}} \mathbb{C}[A]^G$ is one of the terms in the dimension formula for holomorphic cusp forms of weight 2.
- Also (the dimension formulas for) modular forms of weight $\frac{1}{2}$ and $\frac{3}{2}$ involve (the dimension of) $\mathbb{C}[A]^G$.
- No general, explicit formula known.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Observations

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Observations

- The representation ρ is in fact defined over $\mathbb{Q}(\zeta_N)$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Observations

- The representation ρ is in fact defined over $\mathbb{Q}(\zeta_N)$.
- This is clear for $\rho(T)$ and for $\rho(S)$ use Milgram's formula:

$$\sum_{x \in A} e(Q(x)) = \sqrt{|A|}\, e(\mathrm{sig}(A)/8).$$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Observations

- The representation ρ is in fact defined over $\mathbb{Q}(\zeta_N)$.
- This is clear for $\rho(T)$ and for $\rho(S)$ use Milgram's formula:

$$\sum_{x \in A} e(Q(x)) = \sqrt{|A|}\, e(\mathrm{sig}(A)/8).$$

- The representation ρ factors through a representation of the finite group $G_N := \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Explicit formula

Lemma

Let $g = \left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right] \in G_N$ *and* x *in* A. *Then*

$$\rho(g)\mathfrak{e}_x = \chi(d)\, e\left(bdQ(x)\right) \mathfrak{e}_{dx},$$

where $\chi(d) = \sigma_d(w)/w$ *with*

$$w = \sum_{x \in A} e\left(Q(x)\right)$$

and $\sigma_d \in \mathrm{Gal}(K_N/\mathbb{Q})$ *with* $\sigma_d(\zeta_N) = \zeta_N^d$.

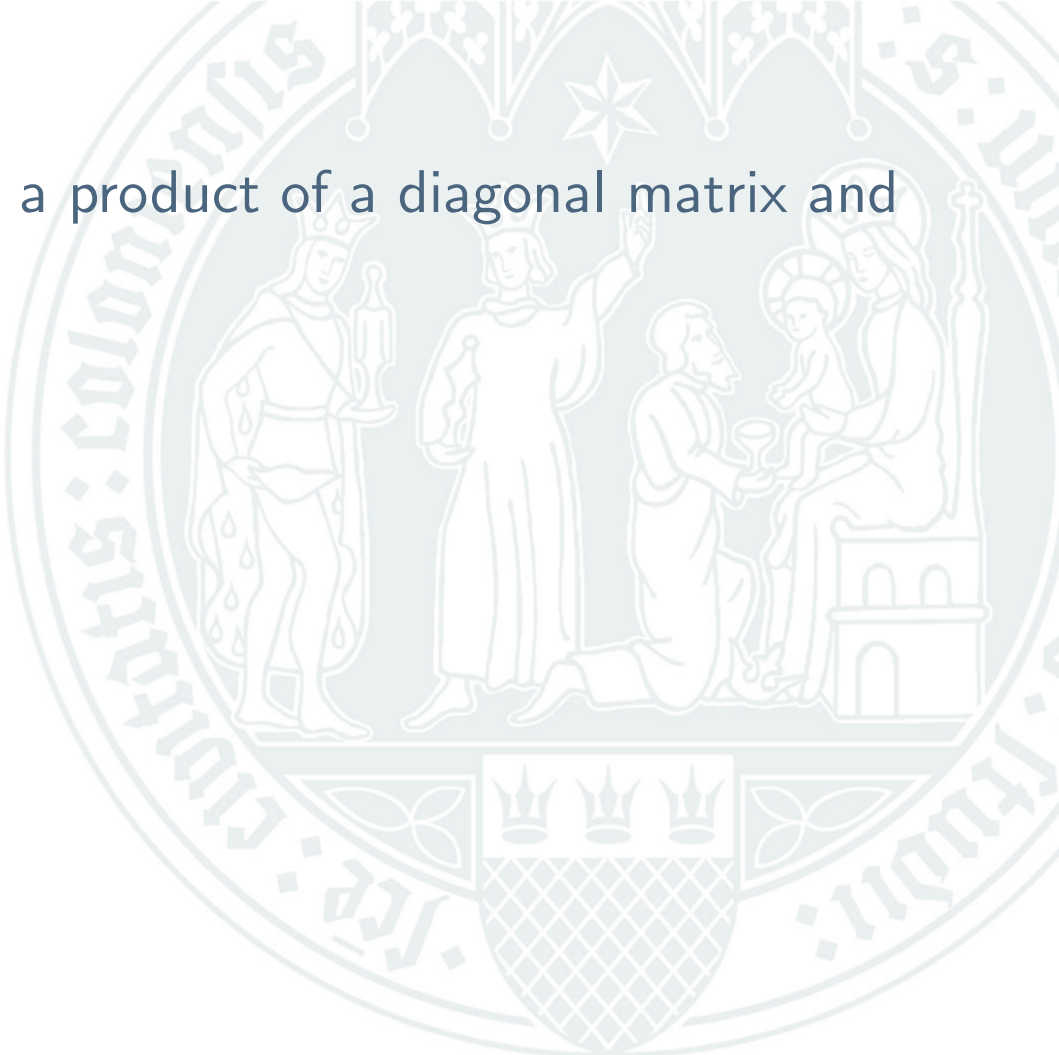
Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

1. Exercise 1: Write $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]$ as a product of a diagonal matrix and a power of T.



Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

1. Exercise 1: Write $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]$ as a product of a diagonal matrix and a power of T.
2. Answer: $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right] = \left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & bd \\ 0 & 1 \end{smallmatrix}\right]$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

1. Exercise 1: Write $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]$ as a product of a diagonal matrix and a power of T.
2. Answer: $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right] = \left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & bd \\ 0 & 1 \end{smallmatrix}\right]$
3. This is good because $\left[\begin{smallmatrix} 1 & bd \\ 0 & 1 \end{smallmatrix}\right] \mathfrak{e}_x = e(bdQ(x))\mathfrak{e}_x$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

1. Exercise 1: Write $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]$ as a product of a diagonal matrix and a power of T.
2. Answer: $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right] = \left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & bd \\ 0 & 1 \end{smallmatrix}\right]$
3. This is good because $\left[\begin{smallmatrix} 1 & bd \\ 0 & 1 \end{smallmatrix}\right] \mathfrak{e}_x = e(bdQ(x))\mathfrak{e}_x$.
4. Only need to consider the action of $\left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right]$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

1. Exercise 1: Write $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]$ as a product of a diagonal matrix and a power of T.
2. Answer: $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right] = \left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & bd \\ 0 & 1 \end{smallmatrix}\right]$
3. This is good because $\left[\begin{smallmatrix} 1 & bd \\ 0 & 1 \end{smallmatrix}\right] \mathfrak{e}_x = e(bdQ(x))\mathfrak{e}_x$.
4. Only need to consider the action of $\left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right]$.
5. Exercise 2: Write $\left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right]$ as a word in S and T (in G_N)!

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

1. Exercise 1: Write $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]$ as a product of a diagonal matrix and a power of T.
2. Answer: $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right] = \left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & bd \\ 0 & 1 \end{smallmatrix}\right]$
3. This is good because $\left[\begin{smallmatrix} 1 & bd \\ 0 & 1 \end{smallmatrix}\right] \mathfrak{e}_x = e(bdQ(x))\mathfrak{e}_x$.
4. Only need to consider the action of $\left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right]$.
5. Exercise 2: Write $\left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right]$ as a word in S and T (in G_N)!
6. Answer:

$$\left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right] = S^{-1} \left[\begin{smallmatrix} 1 & d \\ 0 & 1 \end{smallmatrix}\right] S \left[\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right] S \left[\begin{smallmatrix} 1 & d \\ 0 & 1 \end{smallmatrix}\right]$$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

1. Exercise 1: Write $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]$ as a product of a diagonal matrix and a power of T.
2. Answer: $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right] = \left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & bd \\ 0 & 1 \end{smallmatrix}\right]$
3. This is good because $\left[\begin{smallmatrix} 1 & bd \\ 0 & 1 \end{smallmatrix}\right] \mathfrak{e}_x = e(bdQ(x))\mathfrak{e}_x$.
4. Only need to consider the action of $\left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right]$.
5. Exercise 2: Write $\left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right]$ as a word in S and T (in G_N)!
6. Answer:
$$\left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right] = S^{-1} \left[\begin{smallmatrix} 1 & d \\ 0 & 1 \end{smallmatrix}\right] S \left[\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right] S \left[\begin{smallmatrix} 1 & d \\ 0 & 1 \end{smallmatrix}\right]$$
7. Exercise 3 (due tomorrow): Show that:
$$\left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right] \mathfrak{e}_x = \gamma\, \mathfrak{e}_{dx},$$

   where
$$\gamma = \sigma_d(w)/w, \qquad w = \sum_{x \in A} e\left(Q(x)\right).$$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Integrality

Theorem

The space $\mathbb{C}[A]^G$ is defined over $\mathbb{Z}$, i.e. it has a basis in $\mathbb{Z}[A]$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Integrality

Theorem

The space $\mathbb{C}[A]^G$ is defined over $\mathbb{Z}$, i.e. it has a basis in $\mathbb{Z}[A]$.

Proof.

Use the projection to the invariants and show that it has coefficients in $\mathbb{Z}$ (wrt to the standard basis), which follows from: For any $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ in G and $s \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have

$$\sigma_s(\rho\left(\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]\right)) = \rho\left(\left[\begin{smallmatrix} a & sb \\ s^{-1}c & d \end{smallmatrix}\right]\right)$$

□

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Computing the invariants

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Computing the invariants

- Our goal is just to compute the dimension of $\mathbb{C}[A]^G$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Computing the invariants

- Our goal is just to compute the dimension of $\mathbb{C}[A]^G$
- and optionally also a basis (contained in $\mathbb{Z}[A]$ if possible)

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Computing the invariants

- Our goal is just to compute the dimension of $\mathbb{C}[A]^G$
- and optionally also a basis (contained in $\mathbb{Z}[A]$ if possible)
- which works in all cases.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Identifying invariants

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Identifying invariants

- $v \in \mathbb{C}[A]^G$ is of course equivalent to:

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Identifying invariants

- $v \in \mathbb{C}[A]^G$ is of course equivalent to:
- $\rho(T)v = v$ and $\rho(S)v = v$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Identifying invariants

- $v \in \mathbb{C}[A]^G$ is of course equivalent to:
- $\rho(T)v = v$ and $\rho(S)v = v$.
- $\rho(T)v = v$ means that $\mathrm{supp}(v) \subset \mathrm{Iso}(A)$,

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Identifying invariants

- $v \in \mathbb{C}[A]^G$ is of course equivalent to:
- $\rho(T)v = v$ and $\rho(S)v = v$.
- $\rho(T)v = v$ means that $\mathrm{supp}(v) \subset \mathrm{Iso}(A)$,
- where $\mathrm{Iso}(A) = \{x \in A \mid Q(x) = 0\}$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Identifying invariants

Proposition

Let M be a G-submodule of $\mathbb{C}[A]$. Then

$$M^G = \left(1 + \rho(S) + \rho(S)^2 + \rho(S)^3\right)\left(\mathbb{C}[\mathrm{Iso}(A)]\right) \cap \mathbb{C}[\mathrm{Iso}(A)]$$

Proof.

Exercise. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

The algorithm

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

The algorithm

1. Find the isotropic elements $a_1, \ldots, a_m$ and the non-isotropic elements $b_1, \ldots, b_n$ in A.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

The algorithm

1. Find the isotropic elements $a_1, \ldots, a_m$ and the non-isotropic elements $b_1, \ldots, b_n$ in A.
2. Compute the $(m+n) \times m$ matrix H such that

$$(L\mathfrak{e}_{a_1}, \ldots, L\mathfrak{e}_{a_m}) = (\mathfrak{e}_{a_1}, \ldots, \mathfrak{e}_{a_m}, \mathfrak{e}_{b_1}, \ldots, \mathfrak{e}_{b_n})H,$$

where $L = 1 + \rho(S) + \rho(S)^2 + \rho(S)^3$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

The algorithm

1. Find the isotropic elements $a_1, \ldots, a_m$ and the non-isotropic elements $b_1, \ldots, b_n$ in A.
2. Compute the $(m+n) \times m$ matrix H such that

$$(L\mathfrak{e}_{a_1}, \ldots, L\mathfrak{e}_{a_m}) = (\mathfrak{e}_{a_1}, \ldots, \mathfrak{e}_{a_m}, \mathfrak{e}_{b_1}, \ldots, \mathfrak{e}_{b_n})H,$$

   where $L = 1 + \rho(S) + \rho(S)^2 + \rho(S)^3$.
3. Let U and V be the matrices obtained by extraction the first m and the last n rows of H, respectively.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

The algorithm

1. Find the isotropic elements $a_1, \ldots, a_m$ and the non-isotropic elements $b_1, \ldots, b_n$ in A.
2. Compute the $(m+n) \times m$ matrix H such that

$$(L\mathfrak{e}_{a_1}, \ldots, L\mathfrak{e}_{a_m}) = (\mathfrak{e}_{a_1}, \ldots, \mathfrak{e}_{a_m}, \mathfrak{e}_{b_1}, \ldots, \mathfrak{e}_{b_n})H,$$

   where $L = 1 + \rho(S) + \rho(S)^2 + \rho(S)^3$.
3. Let U and V be the matrices obtained by extraction the first m and the last n rows of H, respectively.
4. Compute a basis $\mathfrak{V}$ for $\ker V$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

The algorithm

1. Find the isotropic elements $a_1, \ldots, a_m$ and the non-isotropic elements $b_1, \ldots, b_n$ in A.
2. Compute the $(m+n) \times m$ matrix H such that

$$(L\mathfrak{e}_{a_1}, \ldots, L\mathfrak{e}_{a_m}) = (\mathfrak{e}_{a_1}, \ldots, \mathfrak{e}_{a_m}, \mathfrak{e}_{b_1}, \ldots, \mathfrak{e}_{b_n})H,$$

   where $L = 1 + \rho(S) + \rho(S)^2 + \rho(S)^3$.
3. Let U and V be the matrices obtained by extraction the first m and the last n rows of H, respectively.
4. Compute a basis $\mathfrak{V}$ for $\ker V$.
5. Return a basis of $U(\ker V) = \{Ux \mid x \in \mathfrak{V}\}$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

The algorithm

1. Find the isotropic elements $a_1, \ldots, a_m$ and the non-isotropic elements $b_1, \ldots, b_n$ in A.
2. Compute the $(m+n) \times m$ matrix H such that

$$(L\mathfrak{e}_{a_1}, \ldots, L\mathfrak{e}_{a_m}) = (\mathfrak{e}_{a_1}, \ldots, \mathfrak{e}_{a_m}, \mathfrak{e}_{b_1}, \ldots, \mathfrak{e}_{b_n})H,$$

   where $L = 1 + \rho(S) + \rho(S)^2 + \rho(S)^3$.
3. Let U and V be the matrices obtained by extraction the first m and the last n rows of H, respectively.
4. Compute a basis $\mathfrak{V}$ for $\ker V$.
5. Return a basis of $U(\ker V) = \{Ux \mid x \in \mathfrak{V}\}$.
6. Exercise: U seems to be invertible in practice. Tell me why.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Reduction mod ℓ

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Reduction mod ℓ

- Let ℓ be a prime with $\ell \equiv 1 \bmod N$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Reduction mod ℓ

- Let ℓ be a prime with $\ell \equiv 1 \bmod N$.
- Then $\mathbb{Q}_\ell$ contains the Nth roots of unity, hence the Nth cyclotomic field.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Reduction mod ℓ

- Let ℓ be a prime with $\ell \equiv 1 \bmod N$.
- Then $\mathbb{Q}_\ell$ contains the Nth roots of unity, hence the Nth cyclotomic field.
- We can consider ρ as a representation of G_N on $\mathbb{Q}_\ell[A]$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Reduction mod ℓ

- Let ℓ be a prime with $\ell \equiv 1 \bmod N$.
- Then $\mathbb{Q}_\ell$ contains the Nth roots of unity, hence the Nth cyclotomic field.
- We can consider ρ as a representation of G_N on $\mathbb{Q}_\ell[A]$.
- In fact, G acts on $\mathbb{Z}_\ell[A]$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Reduction mod ℓ

- Let ℓ be a prime with $\ell \equiv 1 \bmod N$.
- Then $\mathbb{Q}_\ell$ contains the Nth roots of unity, hence the Nth cyclotomic field.
- We can consider ρ as a representation of G_N on $\mathbb{Q}_\ell[A]$.
- In fact, G acts on $\mathbb{Z}_\ell[A]$.
- $\dim_{\mathbb{C}} \mathbb{C}[A]^{G_N}$ equals the $\mathbb{Z}_\ell$-rank of $\mathbb{Z}_\ell[A]^{G_N}$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Reduction mod ℓ

- Let ℓ be a prime with $\ell \equiv 1 \bmod N$.
- Then $\mathbb{Q}_\ell$ contains the Nth roots of unity, hence the Nth cyclotomic field.
- We can consider ρ as a representation of G_N on $\mathbb{Q}_\ell[A]$.
- In fact, G acts on $\mathbb{Z}_\ell[A]$.
- $\dim_{\mathbb{C}} \mathbb{C}[A]^{G_N}$ equals the $\mathbb{Z}_\ell$-rank of $\mathbb{Z}_\ell[A]^{G_N}$.
- Reduction mod ℓ: have a short exact sequence of G-modules:

$$0 \longrightarrow \ell\mathbb{Z}_\ell[A] \longrightarrow \mathbb{Z}_\ell[A] \xrightarrow{r} \mathbb{F}_\ell[A] \longrightarrow 0,$$

where r denotes the reduction map $r(f) : a \mapsto f(a) + \ell\mathbb{Z}_\ell$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Reduction mod ℓ

Theorem

Suppose that $(N, \ell) \neq (2, 3)$. *Then*

$$\dim_{\mathbb{Q}_\ell} \mathbb{Q}_\ell[A]^{G_N} = \dim_{\mathbb{F}_\ell} \mathbb{F}_\ell[A]^{G_N}.$$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

- Obtain the long exact sequence in cohomology

$$0 \longrightarrow \ell\mathbb{Z}_\ell[A]^{G_N} \longrightarrow \mathbb{Z}_\ell[A]^{G_N} \xrightarrow{r} \mathbb{F}_\ell[A]^{G_N} \longrightarrow \mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) \cdots .$$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

- Obtain the long exact sequence in cohomology

$$0 \longrightarrow \ell\mathbb{Z}_\ell[A]^{G_N} \longrightarrow \mathbb{Z}_\ell[A]^{G_N} \xrightarrow{r} \mathbb{F}_\ell[A]^{G_N} \longrightarrow \mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) \cdots .$$

- If $|G_N|$ is a unit in $\mathbb{Z}_\ell$, then $\mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) = \{0\}$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

- Obtain the long exact sequence in cohomology

$$0 \longrightarrow \ell\mathbb{Z}_\ell[A]^{G_N} \longrightarrow \mathbb{Z}_\ell[A]^{G_N} \xrightarrow{r} \mathbb{F}_\ell[A]^{G_N} \longrightarrow \mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) \cdots .$$

- If $|G_N|$ is a unit in $\mathbb{Z}_\ell$, then $\mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) = \{0\}$.
- Of course $\ell \equiv 1 \bmod N$ implies that $\ell > N$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

- Obtain the long exact sequence in cohomology

$$0 \longrightarrow \ell\mathbb{Z}_\ell[A]^{G_N} \longrightarrow \mathbb{Z}_\ell[A]^{G_N} \xrightarrow{r} \mathbb{F}_\ell[A]^{G_N} \longrightarrow \mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) \cdots .$$

- If $|G_N|$ is a unit in $\mathbb{Z}_\ell$, then $\mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) = \{0\}$.
- Of course $\ell \equiv 1 \bmod N$ implies that $\ell > N$
- $|G_N| = N^3 \prod_{p|N} \frac{p^2-1}{p^2}$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

- Obtain the long exact sequence in cohomology

$$0 \longrightarrow \ell\mathbb{Z}_\ell[A]^{G_N} \longrightarrow \mathbb{Z}_\ell[A]^{G_N} \xrightarrow{r} \mathbb{F}_\ell[A]^{G_N} \longrightarrow \mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) \cdots .$$

- If $|G_N|$ is a unit in $\mathbb{Z}_\ell$, then $\mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) = \{0\}$.
- Of course $\ell \equiv 1 \bmod N$ implies that $\ell > N$
- $|G_N| = N^3 \prod_{p|N} \frac{p^2-1}{p^2}$
- Thus, if $\ell \mid |G_N|$, there is a prime $p \mid N$, such that $\ell \mid p+1$ or $\ell \mid p-1$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

- Obtain the long exact sequence in cohomology

$$0 \longrightarrow \ell\mathbb{Z}_\ell[A]^{G_N} \longrightarrow \mathbb{Z}_\ell[A]^{G_N} \xrightarrow{r} \mathbb{F}_\ell[A]^{G_N} \longrightarrow \mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) \cdots .$$

- If $|G_N|$ is a unit in $\mathbb{Z}_\ell$, then $\mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) = \{0\}$.
- Of course $\ell \equiv 1 \bmod N$ implies that $\ell > N$
- $|G_N| = N^3 \prod_{p|N} \frac{p^2-1}{p^2}$
- Thus, if $\ell \mid |G_N|$, there is a prime $p \mid N$, such that $\ell \mid p+1$ or $\ell \mid p-1$.
- However, $p - 1 < N < \ell$ and thus the only possibility is $\ell = p + 1$ and $N = p$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

- Obtain the long exact sequence in cohomology

$$0 \longrightarrow \ell\mathbb{Z}_\ell[A]^{G_N} \longrightarrow \mathbb{Z}_\ell[A]^{G_N} \xrightarrow{r} \mathbb{F}_\ell[A]^{G_N} \longrightarrow \mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) \cdots .$$

- If $|G_N|$ is a unit in $\mathbb{Z}_\ell$, then $\mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) = \{0\}$.
- Of course $\ell \equiv 1 \bmod N$ implies that $\ell > N$
- $|G_N| = N^3 \prod_{p|N} \frac{p^2-1}{p^2}$
- Thus, if $\ell \mid |G_N|$, there is a prime $p \mid N$, such that $\ell \mid p+1$ or $\ell \mid p-1$.
- However, $p - 1 < N < \ell$ and thus the only possibility is $\ell = p + 1$ and $N = p$.
- This only leaves the case $N = 2$ and $\ell = 3$, which we excluded.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Proof

- Obtain the long exact sequence in cohomology

$$0 \longrightarrow \ell\mathbb{Z}_\ell[A]^{G_N} \longrightarrow \mathbb{Z}_\ell[A]^{G_N} \xrightarrow{r} \mathbb{F}_\ell[A]^{G_N} \longrightarrow \mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) \cdots .$$

- If $|G_N|$ is a unit in $\mathbb{Z}_\ell$, then $\mathrm{H}^1(G_N, \ell\mathbb{Z}_\ell[A]) = \{0\}$.
- Of course $\ell \equiv 1 \bmod N$ implies that $\ell > N$
- $|G_N| = N^3 \prod_{p|N} \frac{p^2-1}{p^2}$
- Thus, if $\ell \mid |G_N|$, there is a prime $p \mid N$, such that $\ell \mid p+1$ or $\ell \mid p-1$.
- However, $p - 1 < N < \ell$ and thus the only possibility is $\ell = p + 1$ and $N = p$.
- This only leaves the case $N = 2$ and $\ell = 3$, which we excluded.
- Exercise: Does the theorem hold for $(2, 3)$? We didn't find any counterexamples.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Some dimensions

Table: $d = \dim_{\mathbb{C}} \mathbb{C}[A]^G$ for some 2-modules of even signature s

A $s=0$	d	A $s=4$	d	A $s=0$	d	A	d	s
2^{+2}	2	2^{-2}	0	4^{+2}	3	4^{-8}	1191	0
2^{+4}	5	2^{-4}	1	4^{+4}	16	2_0^{+2}	1	0
2^{+6}	15	2^{-6}	7	4^{+6}	141	2_2^{+2}	0	2
2^{+8}	51	2^{-8}	35	4^{+8}	1711	2_0^{+4}	2	0
2^{+10}	187	2^{-10}	155	4^{-2}	1	2_4^{+4}	0	4
2^{+12}	715	2^{-12}	651	4^{-4}	6	2_6^{+6}	0	6
2^{+14}	2795	2^{-14}	2667	4^{-6}	73	2_0^{+6}	5	0

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Some dimensions

Table: Dimension $d = \dim_{\mathbb{C}} \mathbb{C}[A]^G$ for some 3-modules of signature s

$\mathfrak{A}$	d	$\mathfrak{A}$	d	$\mathfrak{A}$	d	$\mathfrak{A}$	d	s
$s = 6$		$s = 2$		$s = 0$				
3^{+1}	0	3^{-1}	0	9^{+1}	1	27^{+1}	0	6
3^{-2}	2	3^{+2}	0	9^{+2}	1	27^{+2}	0	4
3^{+3}	1	3^{-3}	1	9^{+3}	5	27^{+3}	5	2
3^{-4}	1	3^{+4}	7	9^{+4}	33	27^{-1}	0	2
3^{+5}	10	3^{-5}	10	9^{+5}	121	27^{-2}	4	0
3^{-6}	40	3^{+6}	22	9^{-1}	1	27^{-3}	5	6
3^{+7}	91	3^{-7}	91	9^{-2}	3	81^{+1}	1	0
3^{-8}	247	3^{+8}	301	9^{-3}	5	81^{+2}	1	0
3^{+9}	820	3^{-9}	820	9^{-4}	11	81^{-1}	1	0
3^{-10}	2542	3^{+10}	2380	9^{-5}	121	81^{-2}	5	0

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Some dimensions

Table: Dimension $d = \dim_{\mathbb{C}} \mathbb{C}[A]^G$ for some 3-modules of signature s

$\mathfrak{A}$ $s=6$	d	$\mathfrak{A}$ $s=2$	d	$\mathfrak{A}$ $s=6$	d	$\mathfrak{A}$ $s=2$	d
$3^{+1}27^{-1}$	2	$3^{+1}27^{+1}$	0	$3^{+1}243^{-1}$	2	$3^{+1}243^{+1}$	0
$3^{-2}27^{-1}$	1	$3^{-2}27^{+1}$	1	$3^{-2}243^{-1}$	1	$3^{-2}243^{+1}$	1
$3^{+3}27^{-1}$	1	$3^{+3}27^{+1}$	7	$3^{+3}243^{-1}$	1	$3^{+3}243^{+1}$	7
$3^{-4}27^{-1}$	10	$3^{-4}27^{+1}$	10	$3^{-4}243^{-1}$	10	$3^{-4}243^{+1}$	10
$3^{+5}27^{-1}$	40	$3^{+5}27^{+1}$	22	$3^{+5}243^{-1}$	40	$3^{+5}243^{+1}$	22
$3^{-1}27^{+1}$	2	$3^{-1}27^{-1}$	0	$3^{-1}243^{+1}$	2	$3^{-1}243^{-1}$	0
$3^{+2}27^{+1}$	1	$3^{+2}27^{-1}$	1	$3^{+2}243^{+1}$	1	$3^{+2}243^{-1}$	1
$3^{-3}27^{+1}$	1	$3^{-3}27^{-1}$	7	$3^{-3}243^{+1}$	1	$3^{-3}243^{-1}$	7
$3^{+4}27^{+1}$	10	$3^{+4}27^{-1}$	10	$3^{+4}243^{+1}$	10	$3^{+4}243^{-1}$	10
$3^{-5}27^{+1}$	40	$3^{-5}27^{-1}$	22	$3^{-5}243^{+1}$	40	$3^{-5}243^{-1}$	22

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln