

# Computing with Multiplicative Invariants

*Euler Symposium at Temple U 04-16-2007*

Martin Lorenz

Temple University  
Philadelphia



Leonhard Euler

1707 - 1783



- **Classical invariant theory:** a brief introduction



- **Classical invariant theory**: a brief introduction
- **Multiplicative invariants**: definition and some computational issues



# Overview

- **Classical invariant theory**: a brief introduction
- **Multiplicative invariants**: definition and some computational issues
- **Regularity**: the significance of reflections



# Overview

- **Classical invariant theory**: a brief introduction
- **Multiplicative invariants**: definition and some computational issues
- **Regularity**: the significance of reflections
- The **Cohen-Macaulay property**: exploring the unknown



# Part I: Classical invariant theory



# Algebraic formulation

- **Given:** a **linear group**

$$G \subseteq GL_n(\mathbb{k})$$

over some field  $\mathbb{k}$  (usually  $\mathbb{C}$ )



# Algebraic formulation

- **Given:** a **linear group**

$$G \subseteq \mathrm{GL}_n(\mathbb{k})$$

over some field  $\mathbb{k}$  (usually  $\mathbb{C}$ )

- $G$  acts on the **polynomial algebra**

$$\mathbb{k}[x_1, \dots, x_n]$$

by "linear substitutions of the variables"



# Algebraic formulation

- **Given:** a **linear group**

$$G \subseteq \mathrm{GL}_n(\mathbb{k})$$

over some field  $\mathbb{k}$  (usually  $\mathbb{C}$ )

- $G$  acts on the **polynomial algebra**

$$\mathbb{k}[x_1, \dots, x_n]$$

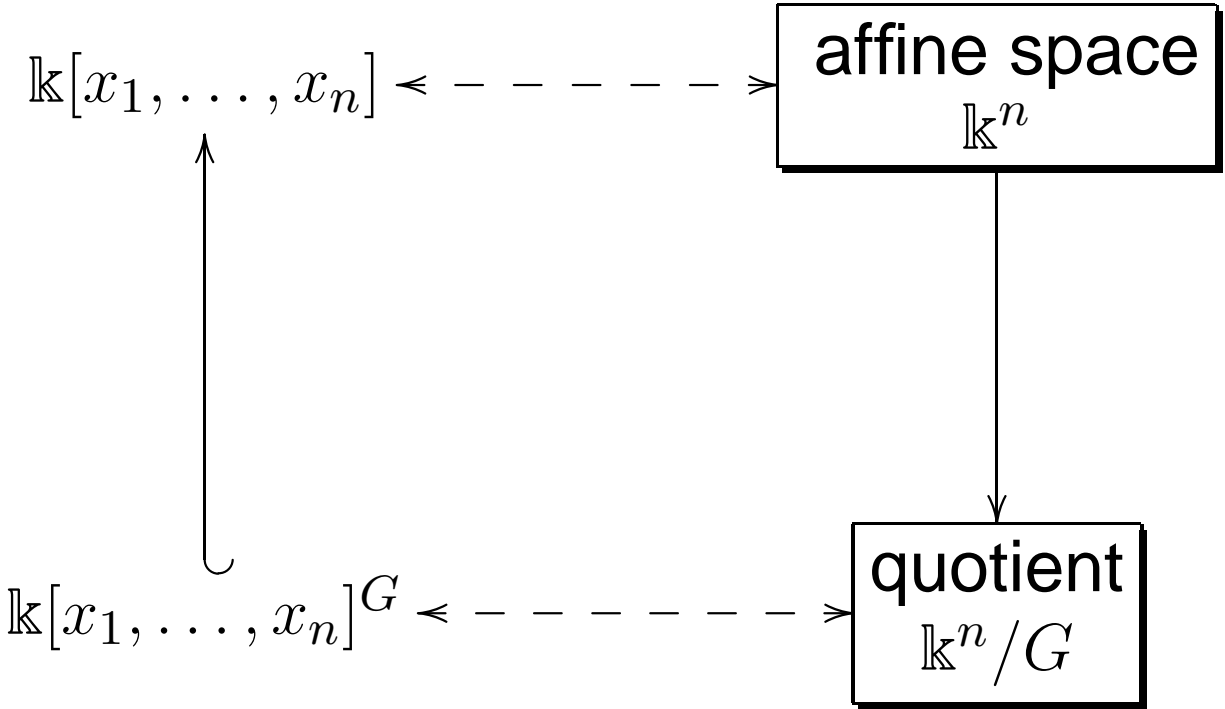
by "linear substitutions of the variables"

- The **algebra of (polynomial) invariants** is

$$\mathbb{k}[x_1, \dots, x_n]^G = \{f \in \mathbb{k}[x_1, \dots, x_n] \mid g(f) = f \ \forall g \in G\}$$



# Geometric view



# Example #1

**Linear group:**

$\rightsquigarrow$  action on  $\mathbb{k}[x, y]$ :

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, g = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

$$g(x) = -x, g(y) = -y$$



**invariants:**

only **even** degrees:

$$\mathbb{k}[x, y]^G = \mathbb{k}[x^2, y^2, xy]$$





## Masters of computation:

- Aronhold (1819 - 1884)
- Clebsch (1833 - 1872)
- Gordan (1837 - 1912)
- Cayley (1821 - 1895)
- Sylvester (1814 - 1897)
- Cremona (1830 - 1903)
- ...



# Pioneers of invariant theory

**Abstract approach:**

**David Hilbert**

1862 - 1943



# Part II: Multiplicative Invariants



# The setting

- **Given:** a group  $G$  and a  **$G$ -lattice**  $L \cong \mathbb{Z}^n$ ; so

$$G \rightarrow \mathrm{GL}(L) \cong \mathrm{GL}_n(\mathbb{Z})$$

an integral representation of  $G$



# The setting

- **Given:** a group  $G$  and a  **$G$ -lattice**  $L \cong \mathbb{Z}^n$ ; so

$$G \rightarrow \mathrm{GL}(L) \cong \mathrm{GL}_n(\mathbb{Z})$$

- Choose a base ring  $\mathbb{k}$  and form the **group algebra**

$$\mathbb{k}[L] = \bigoplus_{m \in L} \mathbb{k}\mathbf{x}^m \cong \mathbb{k}[x_1^{\pm 1}, \dots, x_n^{\pm 1}], \quad \mathbf{x}^m \mathbf{x}^{m'} = \mathbf{x}^{m+m'}$$

The  $G$ -action on  $L$  extends uniquely to a “**multiplicative**” action by  $\mathbb{k}$ -algebra automorphisms on  $\mathbb{k}[L]$ :

$$g(\mathbf{x}^m) = \mathbf{x}^{g(m)} \quad (g \in G, m \in L)$$



# The setting

- **Given:** a group  $G$  and a  **$G$ -lattice**  $L \cong \mathbb{Z}^n$ ; so

$$G \rightarrow \mathrm{GL}(L) \cong \mathrm{GL}_n(\mathbb{Z})$$

- Choose a base ring  $\mathbb{k}$  and form the **group algebra**

$$\mathbb{k}[L] = \bigoplus_{m \in L} \mathbb{k}\mathbf{x}^m \cong \mathbb{k}[x_1^{\pm 1}, \dots, x_n^{\pm 1}], \quad \mathbf{x}^m \mathbf{x}^{m'} = \mathbf{x}^{m+m'}$$

The  $G$ -action on  $L$  extends uniquely to a “**multiplicative**” action by  $\mathbb{k}$ -algebra automorphisms on  $\mathbb{k}[L]$ .

- The **multiplicative invariant algebra** is

$$\mathbb{k}[L]^G = \{f \in \mathbb{k}[L] \mid g(f) = f \ \forall g \in G\}$$



# Example #2

**Multiplicative inversion in rank 2:**

$$G = \langle g \mid g^2 = 1 \rangle$$

$$L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$$

**action:**  $g(e_i) = -e_i$



# Example #2

**Multiplicative inversion in rank 2:**

$$G = \langle g \mid g^2 = 1 \rangle$$

$$L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$$

$$\text{action: } g(e_i) = -e_i$$

Putting  $x_i = x^{e_i}$  we have:

$$\mathbb{k}[L] = \mathbb{k}[x_1^{\pm 1}, x_2^{\pm 1}] \quad \text{with } g(x_i) = x_i^{-1}$$



# Example #2

**Multiplicative inversion in rank 2:**

$$G = \langle g \mid g^2 = 1 \rangle$$
$$L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$$

**action:**  $g(e_i) = -e_i$

Straightforward calculation gives

$$\mathbb{k}[L]^G = \mathbb{k}[\xi_1, \xi_2] \oplus \eta \mathbb{k}[\xi_1, \xi_2]$$

with  $\xi_i = x_i + x_i^{-1}$  and  $\eta = x_1x_2 + x_1^{-1}x_2^{-1}$ ; they satisfy

$$\eta\xi_1\xi_2 = \eta^2 + \xi_1^2 + \xi_2^2 - 4$$



# Example #2

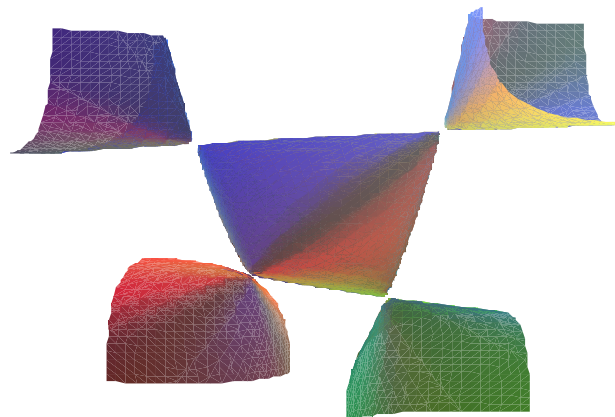
**Multiplicative inversion in rank 2:**

$$G = \langle g \mid g^2 = 1 \rangle$$

$$L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$$

$$\text{action: } g(e_i) = -e_i$$

Hence:  $\mathbb{k}[L]^G \cong \mathbb{k}[x, y, z]/(x^2 + y^2 + z^2 - xyz - 4)$



# Some computational issues

Back to general multiplicative actions:

|                 |                          |
|-----------------|--------------------------|
| $\mathcal{G}$   | a <b>finite</b> group    |
| $L$             | a $\mathcal{G}$ -lattice |
| $\mathbb{k}$    | a commutative base ring  |
| $\mathbb{k}[L]$ | the group algebra        |



# Some computational issues

In general,  $\mathbb{k}[L]$  has **no grading** ( with only  $\mathbb{k}$  in degree 0) that is preserved by the action of  $\mathcal{G}$

↪ computational theory not yet highly developed

∃ some GAP & MAGMA-programs (L., Marc Renault)

But ...



# Some computational issues

**Jordan (1880):**  $GL_n(\mathbb{Z})$  has only finitely many finite subgroups up to conjugacy

⇒ there are only **finitely many** multiplicative invariant algebras  $\mathbb{k}[L]^{\mathcal{G}}$  (up to  $\cong$ ) with  $\text{rank } L$  bounded



# Some computational issues

**Jordan (1880):**  $GL_n(\mathbb{Z})$  has only finitely many finite subgroups up to conjugacy

**Minkowski (1887):** The least common multiple of their orders is given by

$$M_n = \prod_p p^{\lfloor \frac{n}{p-1} \rfloor + \lfloor \frac{n}{p(p-1)} \rfloor + \lfloor \frac{n}{p^2(p-1)} \rfloor + \dots}$$



# Some computational issues

| $n$ | # fin. $\mathcal{G} \leq \text{GL}_n(\mathbb{Z})$<br>(up to conj.) | # max'l $\mathcal{G}$<br>(up to conj.) | $M_n$   |
|-----|--|--|---------|
| 1   | 2  | 1                                      | 2       |
| 2   | 13   | 2                                      | 24      |
| 3   | 73   | 4                                      | 48      |
| 4   | 710  | 9                                      | 5760    |
| 5   | 6079   | 17                                     | 11520   |
| 6   | 85311  | 39                                     | 2903040 |



# Some computational issues

## Accessing these groups via computer:

- **All** finite subgroups  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  with  $n \leq 4$  are available through GAP
- GAP and MAGMA both have data bases of all **maximal** finite subgroups of  $\mathrm{GL}_n(\mathbb{Z})$  for  $n \leq 31$
- The specialized computer algebra system CARAT provides **all** finite  $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$  (and more) up to  $n = 6$



# Part III: Regularity



# Regularity and reflections

## Notations:

$\mathcal{G}$  a finite group

$L \cong \mathbb{Z}^n$  a faithful  $\mathcal{G}$ -lattice

$\mathbb{k} = \bar{\mathbb{k}}$  a field with  $\text{char } \mathbb{k} \nmid |\mathcal{G}|$

Will explain the following result . . .



# Regularity and reflections

- Theorem 1** *TFAE*
- (1)  $\mathbb{k}[L]^{\mathcal{G}}$  is **regular**
  - (2)  $\mathcal{G}$  acts as a **reflection group** on  $L$   
and  $H^1(\mathcal{G}/\mathcal{D}, L^{\mathcal{D}}) = 0$
  - (3)  $\mathbb{k}[L]^{\mathcal{G}} \cong \mathbb{k}[\mathbb{Z}_+^r \oplus \mathbb{Z}^s]$
  - (4)  $\exists$  **root system**  $\Phi$  s.t.  $L/L^{\mathcal{G}} \cong \Lambda(\Phi)$   
and  $\mathcal{G} = \mathcal{W}(\Phi)$

Here,  $\mathcal{D}$  is the subgroup of  $\mathcal{G}$  that is generated by the “diagonalizable” reflections, conjugate in  $GL(L)$  to

$$d = \begin{pmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$



# Regularity and reflections

A search of the crystallographic groups library  
in GAP yields

| $n$ | # finite $\mathcal{G} \leq \mathrm{GL}_n(\mathbb{Z})$<br>(up to conjugacy) | # reflection groups $\mathcal{G}$<br>(up to conjugacy) | # cases with<br>$\mathbb{k}[L]^{\mathcal{G}}$ regular |
|-----|--|--|---|
| 2   | 13   | 9  | 7   |
| 3   | 73   | 29   | 18  |
| 4   | 710  | 102  | 51  |



# Example #3: the root lattice $A_{n-1}$

**Notation:**

$$U_n = \bigoplus_1^n \mathbb{Z}e_i \cong \mathbb{Z}^n$$

$$A_{n-1} = \{ \sum_i z_i e_i \in U_n \mid \sum_i z_i = 0 \} \cong \mathbb{Z}^{n-1}$$

$$\mathcal{S}_n\text{-action: } \sigma(e_i) = e_{\sigma(i)} \quad (\sigma \in \mathcal{S}_n)$$

**Note:**  $\mathcal{S}_n$  acts as a reflection group;  
transpositions are reflections



# Example #3: the root lattice $A_{n-1}$

**Notation:**

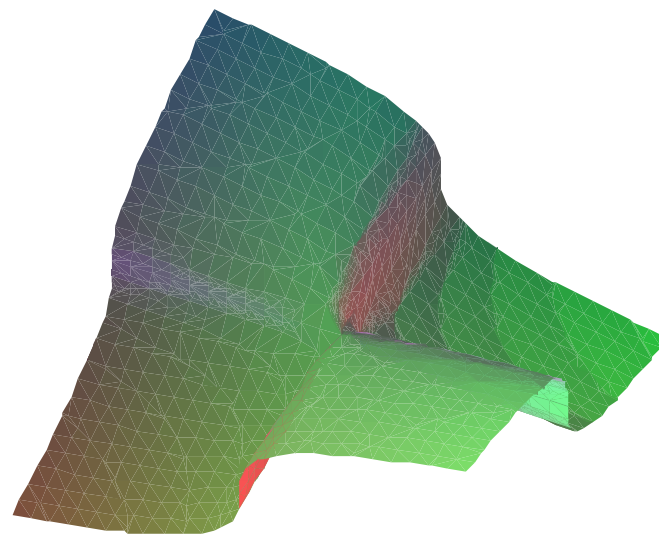
$$U_n = \bigoplus_1^n \mathbb{Z}e_i \cong \mathbb{Z}^n$$

$$A_{n-1} = \{ \sum_i z_i e_i \in U_n \mid \sum_i z_i = 0 \} \cong \mathbb{Z}^{n-1}$$

$$\mathcal{S}_n\text{-action: } \sigma(e_i) = e_{\sigma(i)} \quad (\sigma \in \mathcal{S}_n)$$

$\mathbb{C}[A_{n-1}]^{\mathcal{S}_n}$  is **not** regular:

( $n > 2$ ; picture for  $n = 3$ )



# Part IV: The Cohen-Macaulay Property



- **Hypotheses:**
  - $R$  a comm. noetherian ring
  - $\mathfrak{a}$  an ideal of  $R$



# CM Rings

- **Hypotheses:**  $R$  a comm. noetherian ring  
 $\mathfrak{a}$  an ideal of  $R$
- Always:

$$\text{height } \mathfrak{a} \geq \text{depth } \mathfrak{a} = \inf\{i \mid H_{\mathfrak{a}}^i(R) \neq 0\}$$



# CM Rings

- **Hypotheses:**  $R$  a comm. noetherian ring  
 $\mathfrak{a}$  an ideal of  $R$
- Always:

$$\text{height } \mathfrak{a} \geq \text{depth } \mathfrak{a} = \inf\{i \mid H_{\mathfrak{a}}^i(R) \neq 0\}$$

(Zariski) topology  
dimension theory

(homological) algebra

- **Def:**  $R$  is **Cohen-Macaulay** iff equality holds for all (maximal) ideals  $\mathfrak{a}$



# Some Examples of CM Rings

- **Standard example:**  $R$  an affine domain/PID  $\mathbb{k}$ , finite / some polynomial subalgebra  $P = \mathbb{k}[x_1, \dots, x_n]$ . Then:

$$R \text{ CM} \Leftrightarrow R \text{ is free over } P$$

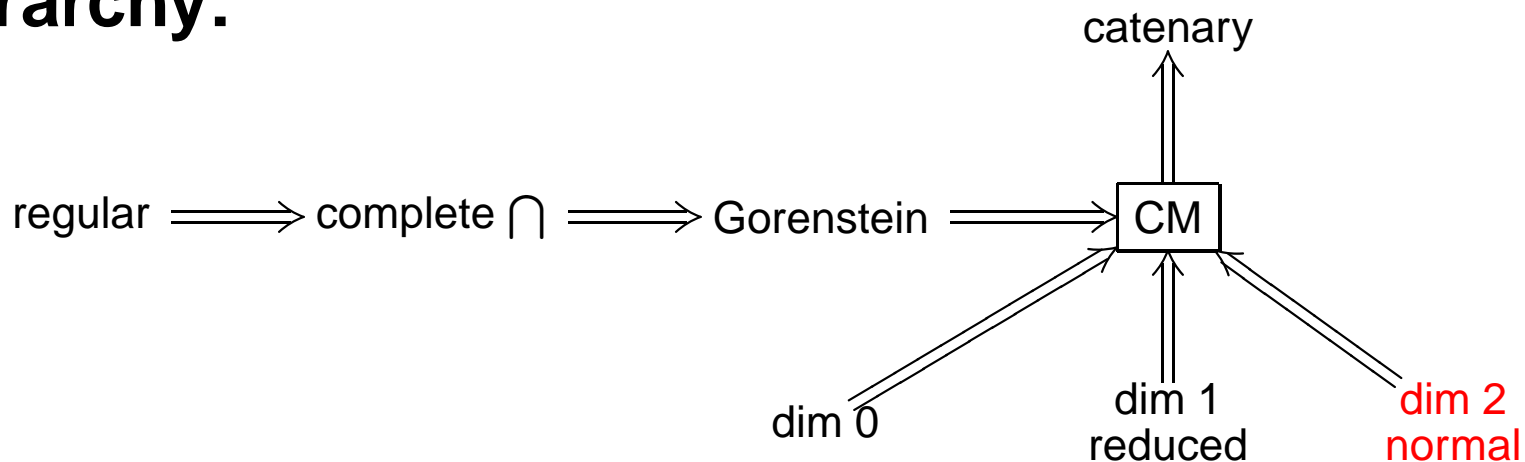


# Some Examples of CM Rings

- **Standard example:**  $R$  an affine domain/PID  $\mathbb{k}$ , finite / some polynomial subalgebra  $P = \mathbb{k}[x_1, \dots, x_n]$ . Then:

$$R \text{ CM} \Leftrightarrow R \text{ is free over } P$$

- **Hierarchy:**



# Multiplicative Invariants: CM-property

**Notations:**  $\mathcal{G}$  is a finite group  $\neq 1$   
 $L$  a  $\mathcal{G}$ -lattice, WLOG faithful



# Multiplicative Invariants: CM-property

**Notations:**  $\mathcal{G}$  is a finite group  $\neq 1$   
 $L$  a  $\mathcal{G}$ -lattice, WLOG faithful

If  $|\mathcal{G}|^{-1} \in \mathbb{k}$  ("non-modular case") then  $\mathbb{k}[L]^{\mathcal{G}}$  is certainly CM;  
otherwise **usually not**

Will concentrate on  $\mathbb{k} = \mathbb{Z}$



# Multiplicative Invariants: CM-property

**Notations:**  $\mathcal{G}$  is a finite group  $\neq 1$   
 $L$  a  $\mathcal{G}$ -lattice, WLOG faithful

**Theorem 2** *If  $\mathbb{Z}[L]^{\mathcal{G}}$  is CM then all  $\mathcal{G}_m/\mathcal{R}^2(\mathcal{G}_m)$  for  $m \in L$  are perfect groups, but not all  $\mathcal{G}_m$  are.*  
(L, TAMS '06)

subgroup gen. by  
bi-reflections on  $L$ :  
 $\text{rank}(g_L - \text{Id}_L) \leq 2$



# Multiplicative Invariants: CM-property

**Notations:**  $\mathcal{G}$  is a finite group  $\neq 1$   
 $L$  a  $\mathcal{G}$ -lattice, WLOG faithful

**Theorem 2** *If  $\mathbb{Z}[L]^{\mathcal{G}}$  is CM then all  $\mathcal{G}_m/\mathcal{R}^2(\mathcal{G}_m)$  for  $m \in L$  are perfect groups, but not all  $\mathcal{G}_m$  are.*  
(L, TAMS '06)

**Corollary** (“3-copies conjecture”)  $\mathbb{Z}[L^{\oplus r}]^{\mathcal{G}}$  is never CM for  $r \geq 3$ .



# Test case: the group $\mathcal{S}_n$

**Problem**      What are the  $\mathcal{S}_n$ -lattices  $L$   
such that  $\mathbb{Z}[L]^{\mathcal{S}_n}$  is CM ?



# Test case: the group $\mathcal{S}_n$

**Problem**      What are the  $\mathcal{S}_n$ -lattices  $L$   
such that  $\mathbb{Z}[L]^{\mathcal{S}_n}$  is CM ?

Theorem 2 and classification results for certain finite linear groups (Huffman and Wales, 70s) allow to reduce this problem to the following question about **polynomial** invariants ...



# Test case: the group $\mathcal{S}_n$

## **Problem'**

(open for  $p \leq n/2$ )

Are the "vector invariants"

$\mathbb{F}_p[x_1, \dots, x_n, y_1, \dots, y_n]^{\mathcal{S}_n}$  CM?



# Test case: the group $\mathcal{S}_n$

## Problem'

(open for  $p \leq n/2$ )

Are the "vector invariants"

$\mathbb{F}_p[x_1, \dots, x_n, y_1, \dots, y_n]^{\mathcal{S}_n}$  CM?

- 1<sup>st</sup> open case  $n = 4, p = 2$  is ok! (Thanks to MAGMA)

```
> n:=4; p:=2;
> G:=PermutationGroup< 2*n | (i,i+1)(n+i,n+i+1) : i in [1..n-1] >;
> R:=InvariantRing(G,GF(p));
> IsCohenMacaulay(R);
```

true



# Test case: the group $\mathcal{S}_n$

## **Problem'**

(open for  $p \leq n/2$ )

Are the "vector invariants"

$\mathbb{F}_p[x_1, \dots, x_n, y_1, \dots, y_n]^{\mathcal{S}_n}$  CM?

- 1<sup>st</sup> open case  $n = 4, p = 2$  is ok! (Thanks to MAGMA)
- It follows that **Problem'** is ok for  $n \leq 5$  (easy argument)



# Test case: the group $\mathcal{S}_n$

## **Problem'**

(open for  $p \leq n/2$ )

Are the "vector invariants"

$\mathbb{F}_p[x_1, \dots, x_n, y_1, \dots, y_n]^{\mathcal{S}_n}$  CM?

- 1<sup>st</sup> open case  $n = 4, p = 2$  is ok! (Thanks to MAGMA)
- It follows that **Problem'** is ok for  $n \leq 5$  (easy argument)
- Next open cases  $n = 6, p = 2$  and  $p = 3$ : **out of memory!**



# Summary

Let  $L$  be a  $\mathcal{G}$ -lattice, where  $\mathcal{G}$  is a finite group.

