

$$G \cdot I = I \implies I = \langle g_1, \dots, g_m \rangle_{R[G]}$$

# Groebner Bases of Symmetric Ideals in Infinite Dimensional Rings

Christopher Hillar  
(Texas A&M University)

Joint with Matthias Aschenbrenner  
(U. Illinois, Chicago)

# Outline of talk

- Motivational **Problem**
- Introduction: What is **Finiteness**?
  - Group rings, invariant ideals, etc.
- **Theorem**: Finiteness of Symmetric Ideals for Infinite Dimensional Polynomial Rings
- Symmetric Cancellation **Partial Order**
- **Reduction Theory** for Groups Actions on Polynomial Rings
- **Groebner Basis** and ideal membership
- **Algorithms**

# Motivational Problem

Let  $R = K[x_1, x_2, x_3, \dots]$  over a field  $K$ ,  
 $G = S_\infty = \text{Perm}(\{1, 2, 3, \dots\})$ .

Let  $I = G \cdot \langle f_1, f_2 \rangle_R$  be the ideal generated by  
all permutations of the two polynomials

$$f_1 = x_1^3 x_3 + x_1^2 x_2^3$$

$$f_2 = x_2^2 x_3^2 - x_2^2 x_1 + x_1 x_3^2$$

**Problem:** Let  $g$  be a polynomial in  $R$ . Can you  
tell me if  $g$  is in  $I$ ?

# Motivational Problem

Concretely, for instance, what if

$$\begin{aligned} g = & -x_{10}^2 x_9^2 x_5^6 - 2x_{10}^2 x_9 x_8^3 x_5^5 - x_{10}^2 x_8^6 x_5^4 + 3x_{10}^2 x_8^2 + 3x_{10}^2 x_7 + \\ & 3x_{10} x_9 x_7 x_4^3 x_3^2 x_2^2 x_1 + 3x_{10} x_9 x_7 x_4^3 x_3^2 x_1^2 - 3x_{10} x_9 x_7 x_4^3 x_2^2 x_1^2 - x_9^2 x_8^7 x_7 x_6 x_5^6 - \\ & 2x_9 x_8^{10} x_7 x_6 x_5^5 + x_9 x_5^3 x_3 x_2 x_1^3 + x_9 x_5^3 x_2^4 x_1^2 + x_9 x_3 x_2^3 x_1^4 + x_9 x_2^6 x_1^3 - \\ & x_8^{13} x_7 x_6 x_5^4 - 3x_8^2 x_7 + x_7^2 x_6 x_3^3 x_2^7 + x_7^2 x_6 x_3^3 x_2^5 x_1 - x_7^2 x_6 x_3 x_2^7 x_1 + x_5 x_4^2 - \\ & 3x_5 x_3^2 + 2x_5 x_1^2 + x_4^2 x_3^2 - 2x_3^2 x_1^2 + 5x_3 x_1^5 + 5x_2^3 x_1^4 \end{aligned}$$

How would you try to answer the **question**:

Can you express  $g$  as a **finite linear combination** over  $R$  of polynomials  $\sigma f_i$  ( $\sigma$  a permutation,  $i = 1, 2$ )?

# What is Finiteness?

Let  $K$  be a field and let  $R = K[x_1, \dots, x_n]$  be the polynomial ring over  $K$ . **Computational algebraic geometry** starts with:

**Hilbert's Basis Theorem (1890):** Every ideal  $I$  in  $K[x_1, \dots, x_n]$  is finitely generated. That is, there exist polynomials  $f_1, \dots, f_m$  such that

$$I = \langle f_1, \dots, f_m \rangle_R = \{r_1 f_1 + \dots + r_m f_m : r_i \text{ in } R\}.$$

# Finiteness in Infinite Dimensional Polynomial Rings?

Let  $R = K[x_1, x_2, x_3, \dots]$  be the (infinite dimensional) polynomial ring over  $K$ . We will discuss methods for *computing* (!) with ideals in  $R$ .

However, Classical Finiteness Fails:

$I = \langle x_1, x_2, x_3, \dots \rangle_R$  is **not** finitely generated!

*Proof:* A finite set of  $n$  generators have no constant terms and involve only a **finite number** of the indeterminates  $x_1, \dots, x_m$ . Now, set  $x_1 = \dots = x_m = 0$  in

$$x_{m+1} = r_1 f_1 + \dots + r_n f_n.$$



# Need Extra Structure: Group Actions and Invariant Ideals

**Group Rings:** Let  $G$  be a group and  $R$  a commutative ring.

The (left) group ring  $R[G]$  over  $R$  is formally all linear combinations:

$$r_1g_1 + \cdots + r_mg_m, \quad r_i \text{ in } R, g_i \text{ in } G.$$

Multiplication is given by  $(r_1g_1) \cdot (r_2g_2) = (r_1r_2)g_1g_2$  and extended by linearity.

- Think of this as a **vector space** with **basis elements** from  $G$  and a multiplication coming from the **multiplication in  $G$** .

# Group Ring Example

**Example:** Let  $G = S_2 = \{(1), (12)\}$ , the group of permutations of the integers  $\{1,2\}$ . And let  $R = \mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ . Then,

$$R[G] = \{a(1) + b(12) : a, b \text{ in } \mathbf{Z}\}$$

In this ring, for example, we have

$$\begin{aligned} [3(12) - 2(1)]^2 &= 9(12)^2 - 6(12)(1) - 6(1)(12) + 4(1)^2 \\ &= 9(1) - 6(12) - 6(12) + 4(1) \\ &= -12(12) + 13(1) \end{aligned}$$

- One can check that  $R[G] \cong \mathbf{Z}[x]/\langle x^2-1 \rangle$ .

# Invariant Ideals

Assume further that  $R$  is a  $G$ -module; that is,  $G$  gives an action on  $R$  (i.e.  $G \rightarrow \text{Perm}(R)$ ) that is linear:

$$g(r+s) = gr + gs, \quad g \text{ in } G, \quad r, s \text{ in } R$$

This gives  $R$  the structure of a (left) module over the group ring  $R[G]$ .

**Definition:** An ideal  $I$  of  $R$  is invariant under  $G$  if

$$G \cdot I = \{g \cdot f : f \text{ in } I, g \text{ in } G\} = I$$

Said another way, invariant ideals are simply the  $R[G]$ -submodules of  $R$ .

# Examples

1. Let  $R = K[x_1, \dots, x_n]$  and  $G = \{1\}$ . Then,  
 $R[G] = R$   
 invariant ideals = the ideals of  $R$ .

2. Let  $R = K[x_1, x_2]$  and  $G = S_2 = \{(1), (12)\}$

$$\underbrace{(x_1(1) + x_2(12))}_{R[G]} \cdot \underbrace{(x_1 + x_2 x_1^2)}_R = \underbrace{x_1^2 + x_2^2 + x_2 x_1^3 + x_2^3 x_1}_R$$

$I = \langle x_1 + x_2^2, x_2 + x_1^2 \rangle_R = \langle x_1 + x_2^2 \rangle_{R[G]}$  is an invariant ideal  
 (i.e. an  $R[G]$ -submodule of  $R$ ).

# Finiteness Finally

We now state a simplified version of our result, which says *computation is at least possible*

**Setup:**  $R = K[x_1, x_2, x_3, \dots]$ ,  $K$  a field,  
 $G = S_\infty = \text{Perm}(\{1, 2, 3, \dots\})$

**Theorem [A,H]:** Invariant ideals of  $R$  are finitely generated over  $R[G]$ . ( $R$  is a **Noetherian**  $R[G]$ -module)

Remark: Finiteness problems before because we couldn't "generate" enough of  $I$  using a finite number of polynomials. Here, extra structure of  $I$  allows us to find a **finite presentation** by allowing action of  $G$ .

# Basic Example

**Example:** Recall that we couldn't have

$$I = \langle x_1, x_2, x_3, \dots \rangle_R = \langle f_1, \dots, f_m \rangle_R$$

However,  $I$  has extra structure: it is invariant under  $G = S_\infty$ . The previous theorem should apply:

$$I = \langle x_1, x_2, \dots \rangle_R = \langle x_1 \rangle_{R[G]} = \{h \cdot x_1 : h \text{ in } R[G]\}$$

The point is that by allowing action of **bigger ring**  $R[G]$  instead of  $R$ , we get **finite presentations** of  $I$

- Note:  $I$  might need **arbitrarily large numbers** of generators

# Symmetric Cancellation Partial Order on Monomials

Let  $<_{\text{lex}}$  be the **lexicographic ordering** of monomials with  $x_1 <_{\text{lex}} x_2 <_{\text{lex}} x_3 <_{\text{lex}} \dots$ . E.g.,  $x_2 x_3^3 <_{\text{lex}} x_1 x_4$

**Definition/Lemma:** Symmetric cancellation partial order

$$u \leq v \quad :\Leftrightarrow \quad \left\{ \begin{array}{l} u \leq_{\text{lex}} v, \text{ there exists } \sigma \text{ in } G \\ \text{with } \sigma u \mid v, \text{ and for all} \\ w \leq_{\text{lex}} u, \text{ we have } \sigma w \leq_{\text{lex}} \sigma u \end{array} \right.$$

**Example:**

$$x_1^2 < x_1 x_2^2 < x_1^3 x_2 x_3^2$$

- This ordering **refines** monomial division

# A Closer Inspection

- (1)  $u \leq_{\text{lex}} v$     A variable in  $u$  is not bigger than one in  $v$
- (2)  $\sigma u \mid v$     Symmetric division
- (3)  $w \leq_{\text{lex}} u \implies \sigma w \leq_{\text{lex}} \sigma u$     for the *witness*  $\sigma$  in (2)

3rd Condition allows for “nice” leading term cancellation.

Let  $g$  in  $R$ . If  $\text{lm}_{\langle \text{lex} \rangle}(g) \leq v$  for some  $v$  and witness  $\sigma$  then:

$$\sigma \text{lm}_{\langle \text{lex} \rangle}(g) = \text{lm}_{\langle \text{lex} \rangle}(\sigma g)$$

I.e.  $\sigma$  commutes with taking leading (lex) monomials

# Symmetric SG-Polynomial

This looks quite **technical**, but is remembered by the

**Cancellation Property:** If  $m_1 < m_2$  and if  $f_1$  and  $f_2$  have leading (lexicographic) terms  $m_1$  and  $m_2$ , then the **SG-polynomial**

$$\text{SG}_\sigma(f_1, f_2) = f_2 - \frac{m_2}{\sigma m_1} \sigma f_1$$

has a smaller (lex) leading monomial than  $f_2$ .

*Proof:*  $f_1 = (m_1 + w + \dots)$ ,  $f_2 = (m_2 + \dots)$ .  $\text{SG}_\sigma(f_1, f_2)$  kills off  $m_2$ . Terms bigger (lex) than  $m_2$  come from  $w$  in  $f_1$ :

$$w <_{\text{lex}} m_1 \Rightarrow \sigma w <_{\text{lex}} \sigma m_1 \Rightarrow \frac{m_2}{\sigma m_1} \sigma w <_{\text{lex}} \frac{m_2}{\sigma m_1} \sigma m_1 = m_2 \quad \square$$

# Basic Theory of Reduction

We now explain **reduction** in the  $R[G]$ -module  $R$ ,  $G = S_\infty$

**Definition:**  $\text{lm}(f)$  = largest lexicographic monomial in  $f$ .

**Definition:**  $f$  in  $R$  is **reducible** by a set of polynomials  $B$  means that for some  $g$  in  $B$ , we have

$$\text{lm}(g) \leq \text{lm}(f) \qquad \text{so } \sigma \text{lm}(g) \mid \text{lm}(f)$$

In this case, we write  $f \dashrightarrow h$  where

$$h = f - cm(\sigma g)$$

$m$  is a monomial and  $c$  is the coefficient of  $\text{lm}(f)$  in  $f$

# Reduction Intuition

The point: if  $I$  is invariant,  $f$  and  $g$  in  $I$ , and  $f \rightarrow h$ , then  $h$  is in  $I$  with smaller (lex) leading monomial

In analog to classical GB, we would like to find a (finite) subset  $B$  of  $I$  such that being in  $I$  is same as there being a sequence of reductions

$$f \rightarrow h_1 \rightarrow h_2 \rightarrow \dots \rightarrow 0$$

Example:  $B = \{x_1x_2^2 + x_2, x_1 - 1\}$ ,  $f = x_1^3x_2x_3^2 + x_1^4x_3$

$$f \rightarrow x_1^4x_3 - x_1^3x_3 \rightarrow 0$$

So  $f = x_1^3(123)(x_1x_2^2 + x_2) + x_1^3x_3(x_1 - 1)$  is in  $\langle B \rangle_{R[G]}$

# Groebner Bases

**Definition/Proposition:** Let  $I$  be an invariant ideal and  $B$  a set of nonzero polynomials. The following are equivalent

- (1)  $B$  is a **Groebner Basis** for  $I$
- (2) Every  $f$  in  $I$  has **unique normal form** 0

Notice that (2) implies that  $I = \langle B \rangle_{R[G]}$

So our previous theorem may be deduced from the

**Theorem [A,H]:** An invariant ideal of  $R$  has a **finite Groebner basis**  $B$

# Example Groebner Basis

**Achtung!** Classical intuition sometimes fails here.

**Example:** Let  $I = \langle x_1 x_2^2 \rangle_{R[G]}$ , which is a monomial ideal.

The set  $B = \{x_1 x_2^2\}$  is **not** a Groebner Basis for  $I$ .

Reason:  $x_1^2 x_2$  is in  $I$ , however,

$$x_1^2 x_2 \not\rightarrow 0$$

so that  $x_1^2 x_2$  does not have normal form 0 wrt  $B$

---

But  $B = \{x_1 x_2^2, x_1^2 x_2\}$  is a minimal Groebner basis.

**Example:**  $x_3 x_4 x_6^3 = x_4 x_6 (13)(26) x_1 x_2^2$  is in  $I$ , and indeed

$$x_3 x_4 x_6^3 \rightarrow 0$$

# Algorithms

*Can we compute a Groebner basis for an invariant ideal  $I$  given a finite list of generators?* If so, then we really could do computations in the infinite dimensional (module)  $R$ .

**Theorem [H]:** Let  $I = \langle f_1, f_2, \dots, f_n \rangle_{R[G]}$  be an invariant ideal of  $R$ . There exists an **effective** algorithm to compute a minimal Groebner Basis  $B$  for  $I$

**Corollary:** There is an algorithm to solve the **ideal membership problem**.

- This algorithm has been implemented and is currently being optimized for use in **SINGULAR**

# Example Groebner Basis

**Example:** Consider the set  $F = \{x_1 + x_2, x_1x_2\}$ .  
Let  $S = K[x_1, x_2]$ ,  $G = \{(1), (12)\}$ . Then

$$\langle F \rangle_{S[G]} \neq \langle F \rangle_{R[G]} = \langle x_1 \rangle_{R[G]}$$

Therefore, we cannot simply **restrict** the number of variables in computing  $G$ .

A **Groebner basis** for  $I$  is given by  $G = \{x_1\}$ .

# Motivational Problem Again

**Example:** Let  $I$  be generated by

$$F = \{x_1^3x_3 + x_1^2x_2^3, x_2^2x_3^2 - x_2^2x_1 + x_1x_3^2\}.$$

A symmetric **Groebner basis** is given by 5 polynomials:

$$G = \{x_3x_2x_1^2, x_3^2x_1 + x_2^4x_1 - x_2^2x_1, x_3x_1^3, x_2x_1^4, x_2^2x_1^2\}$$

To see if any polynomial  $g$  is in  $I$ , we simply **reduce  $g$  by  $G$**  and see if the result is **0**.

Traditionally, we would have to (at the very least) compute a (normal) Groebner basis of the  $S_n$  orbit of the generators of  $I$ , where  $n$  is the number of indeterminates in  $f$ .

# Motivational Problem Again

So, is

$$\begin{aligned} & -x_{10}^2 x_9^2 x_5^6 - 2x_{10}^2 x_9 x_8^3 x_5^5 - x_{10}^2 x_8^6 x_5^4 + 3x_{10}^2 x_8^2 + 3x_{10}^2 x_7 + 3x_{10} x_9 x_7 x_4^3 x_3^2 x_2^2 x_1 + \\ & 3x_{10} x_9 x_7 x_4^3 x_3^2 x_1^2 - 3x_{10} x_9 x_7 x_4^3 x_2^2 x_1^2 - x_9^2 x_8^7 x_7 x_6 x_5^6 - 2x_9 x_8^{10} x_7 x_6 x_5^5 + \\ & x_9 x_5^3 x_3 x_2 x_1^3 + x_9 x_5^3 x_2^4 x_1^2 + x_9 x_3 x_2^3 x_1^4 + x_9 x_2^6 x_1^3 - x_8^{13} x_7 x_6 x_5^4 - 3x_8^2 x_7 + \\ & x_7^2 x_6 x_3^3 x_2^7 + x_7^2 x_6 x_3^3 x_2^5 x_1 - x_7^2 x_6 x_3 x_2^7 x_1 + x_5 x_4^2 - 3x_5 x_3^2 + 2x_5 x_1^2 + x_4^2 x_3^2 - \\ & 2x_3^2 x_1^2 + 5x_3 x_1^5 + 5x_2^3 x_1^4 \end{aligned}$$

in the ideal  $I$  ?

**One way to check:** Compute a traditional GB with a priori  $2 \cdot 10!$  polynomials in 10 variables! (and it still might not work!)

**Better way:** Reduce it modulo the symmetric Groebner bases and check if you get 0 (you do).

# Open Problems

1. Extensions to other group actions  $G$ .
2. Applications to finite dimensional situation.
3. Can we read off properties of the ideals  $I$  from their Groebner bases as in the traditional case?

# The End

(of talk)