# Lecture 13: Primary and Secondary Invariants

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

February 28, 2021

# Overview

- Graded Algebras, Modules & Cohen-Macaulay Property
- Cohen-Macaulayness of Ring of Invariants of Finite Groups & Primary and Secondary Invariants
- Conclusion
- Acknowledgements

# Graded Rings and Algebras

- A *graded ring* is a ring $R$ together with a direct sum decomposition into abelian groups:

$$R = \underline{R_0} \oplus \underline{R_1} \oplus \underline{R_2} \oplus \cdots$$

such that

$$\overset{f_i}{R_i} \cdot \overset{f_j}{R_j} \subseteq \overset{f_i f_j}{R_{i+j}}$$

R commutative with unit

+ R is abelian group

×

$1 \cdot r = r \cdot 1 = r$

# Graded Rings and Algebras

- A *graded ring* is a ring $R$ together with a direct sum decomposition into abelian groups:

$$R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots$$

  such that

$$R_i \cdot R_j \subseteq R_{i+j}$$

- Example: $R = \mathbb{C}[x_1, \ldots, x_n]$, grading by degree

$$R = \mathbb{C} \oplus \underbrace{R_1}_{\text{linear forms}} \oplus \underbrace{R_2}_{\text{quadratic forms}} \oplus \cdots$$

# Graded Rings and Algebras

- A *graded ring* is a ring $R$ together with a direct sum decomposition into abelian groups:

$$R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots$$

  such that

$$R_i \cdot R_j \subseteq R_{i+j}$$

- Example: $R = \mathbb{C}[x_1, \ldots, x_n]$, grading by degree
- A *homogeneous element* of $R$ is an element of some $R_d$
- A *homogeneous ideal* of $R$ is an ideal generated by homogeneous elements

# Graded Rings and Algebras

- A *graded ring* is a ring $R$ together with a direct sum decomposition into abelian groups:

$$R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots$$

  such that

$$R_i \cdot R_j \subseteq R_{i+j}$$

- Example: $R = \mathbb{C}[x_1, \ldots, x_n]$, grading by degree
- A *homogeneous element* of $R$ is an element of some $R_d$
- A *homogeneous ideal* of $R$ is an ideal generated by homogeneous elements
- For any $f \in R$ there is a unique expression of $f$ into homogeneous parts:

$$f = f_0 + f_1 + \cdots \qquad f_d \in R_d$$

  and $f_k = 0$ for all but finitely many $k \in \mathbb{N}$
- A graded $\mathbb{C}$-algebra is a graded ring $R$ with $\boxed{R_0 = \mathbb{C}.}$

# Algebraic Independence

- Given a $\mathbb{C}$-algebra $R$, we say that elements $f_1, \ldots f_k$ are *algebraically dependent* if there is a non-zero polynomial $P \in \mathbb{C}[z_1, \ldots, z_k]$ such that
$$P(f_1, \ldots, f_k) = 0$$

$f$ is integral over $f_1, \ldots, f_n$ if there is $\underline{\text{monic}}$ in $t$ $P \in \mathbb{C}[z_1, \ldots, z_n][t]$

s.t. $P(f_1, \ldots, f_n, f) = 0$

# Algebraic Independence

- Given a $\mathbb{C}$-algebra $R$, we say that elements $f_1, \ldots f_k$ are *algebraically dependent* if there is a non-zero polynomial $P \in \mathbb{C}[z_1, \ldots, z_k]$ such that
$$P(f_1, \ldots, f_k) = 0$$
- If there are no non-zero polynomials $P$ which vanish on $f_1, \ldots, f_k$, we say they are *algebraically independent*

$x_1^{a_1}, x_2^{a_2}, \ldots, x_n^{a_n}$

# Algebraic Independence

- Given a $\mathbb{C}$-algebra $R$, we say that elements $f_1, \dots f_k$ are *algebraically dependent* if there is a non-zero polynomial $P \in \mathbb{C}[z_1, \dots, z_k]$ such that
$$P(f_1, \dots, f_k) = 0$$
- If there are no non-zero polynomials $P$ which vanish on $f_1, \dots, f_k$, we say they are *algebraically independent*
- The maximal number $n \in \mathbb{N}$ of algebraically independent elements in $R$ is called its *Krull dimension*

## Graded Modules

- Given a graded ring $R$, a *graded R-module* $M$ is an $R$-module with a direct sum decomposition into abelian groups

$$M = M_0 \oplus M_1 \oplus M_2 \oplus \cdots$$

such that $\underline{R_i} \cdot \underline{M_j} \subseteq \underline{M_{i+j}}$

$I_0 = 0 \quad I_1 = 0$

$I_2 = \langle x^2, yz \rangle$

$I_3 = \langle x^3, x^2y, x^2z, xyz, y^2z, yz^2 \rangle$

M is R-module if

M + abelian group

$R \times M \longrightarrow M$

$(r, m) \mapsto rm$

$(rs)m = r(sm)$

generalization of vector space

$R = \mathbb{C}[x, y, z]$ $\quad I \subset R$ homogeneous ideal

$(x^2, yz) = I$

# Graded Modules

- Given a graded ring $R$, a *graded $R$-module* $M$ is an $R$-module with a direct sum decomposition into abelian groups

$$M = M_0 \oplus M_1 \oplus M_2 \oplus \cdots$$

  such that $R_i \cdot M_j \subseteq M_{i+j}$
- Examples:
  1. homogeneous ideal $I \subset R$
  2. Free $R$-modules $R^n$

# Graded Modules

- Given a graded ring $R$, a *graded R-module* $M$ is an $R$-module with a direct sum decomposition into abelian groups

$$M = M_0 \oplus M_1 \oplus M_2 \oplus \cdots$$

  such that $R_i \cdot M_j \subseteq M_{i+j}$
- Examples:
  1. homogeneous ideal $I \subset R$
  2. Free $R$-modules $R^n$
- An $R$-module $M$ is finitely generated iff there are elements $m_1, \ldots, m_k$ such that

$$M = \underbrace{Rm_1 + Rm_2 + \cdots + Rm_k}$$

R-module generated by $m_1, \ldots, m_n$

$\{ r_1 m_1 + r_2 m_2 + \cdots + r_n m_n \}$

# Graded Modules

- Given a graded ring $R$, a *graded $R$-module* $M$ is an $R$-module with a direct sum decomposition into abelian groups
$$M = M_0 \oplus M_1 \oplus M_2 \oplus \cdots$$
such that $R_i \cdot M_j \subseteq M_{i+j}$
- Examples:
  1. homogeneous ideal $I \subset R$
  2. Free $R$-modules $R^n$
- An $R$-module $M$ is finitely generated iff there are elements $m_1, \ldots, m_k$ such that
$$M = Rm_1 + Rm_2 + \cdots + Rm_k$$
- Note that finitely generated modules need not be free.

$Rp \cong R$

$$R = \mathbb{C}[x, y] \quad M = Rx^2y + Rxy^2 = (x^2y, xy^2)$$

$(x^2y) \cdot y - x \cdot (xy^2) = 0$

# Regular Sequences

$\nexists\, r \in R$ s.t. $r \cdot m_1 = 0$

- A sequence of elements $m_1, m_2, \ldots, m_k$ in an $R$-module $M$ is a *regular sequence* if
  1. $m_1$ is a **non-zero divisor** over $M$ and
  2. $m_i$ is a **non-zero divisor** over $M/(Rm_1 + \cdots + Rm_{i-1})$

# Regular Sequences

- A sequence of elements $m_1, m_2, \ldots, m_k$ in an $R$-module $M$ is a *regular sequence* if
  1. $m_1$ is a **non-zero divisor** over $M$ and
  2. $m_i$ is a **non-zero divisor** over $M/(Rm_1 + \cdots + Rm_{i-1})$
- Example: $R = \mathbb{C}[x, y, z]$, $M = R$ and $m_1 = y - x^2$, $m_2 = z - x^3$

$(y - x^2, z - x^3)$

# Regular Sequences

- A sequence of elements $m_1, m_2, \ldots, m_k$ in an $R$-module $M$ is a *regular sequence* if
  1. $m_1$ is a **non-zero divisor** over $M$ and
  2. $m_i$ is a **non-zero divisor** over $M/(Rm_1 + \cdots + Rm_{i-1})$
- Example: $R = \mathbb{C}[x, y, z]$, $M = R$ and $m_1 = y - x^2$, $m_2 = z - x^3$
- A good intuition for regular sequences: they give “new equations”

# Regular Sequences

- A sequence of elements $m_1, m_2, \ldots, m_k$ in an $R$-module $M$ is a *regular sequence* if
  1. $m_1$ is a **non-zero divisor** over $M$ and
  2. $m_i$ is a **non-zero divisor** over $M/(Rm_1 + \cdots + Rm_{i-1})$
- Example: $R = \mathbb{C}[x, y, z]$, $M = R$ and $m_1 = y - x^2$, $m_2 = z - \cancel{y}x^3$
- A good intuition for regular sequences: they give "new equations"
- **Non-Example:** $m_1 = y - x^2$, $m_2 = z - \cancel{y}x^3$ and $m_3 = xz - y^2$

$$Z(\underbrace{y - x^2, z - x^3}, \underline{xz - y^2})$$

$$= \{\underline{(t, t^2, t^3)} \mid t \in \mathbb{C}\} = Z(y - x^2, z - x^3)$$

algebraic independence $\not\Rightarrow$ regular sequence

$xy$, $x$ algebraically independent

but not regular sequence

$x \cdot y \equiv 0 \quad \mathbb{C}[x,y]/(yx)$

$\Rightarrow x$ zero divisor

# Homogeneous System of Parameters

- Given a graded $\mathbb{C}$-algebra $R$ of Krull dimension $n$, a set of homogeneous elements $\theta_1, \ldots, \theta_n$ is a

  *homogeneous system of parameters* (h.s.o.p.)

  if

  $R$ is *finitely generated* as a $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module.

$R = \mathbb{C}[x, y, z]$ $\qquad x, y^2, z^2$ h.s.o.p.

$S = \mathbb{C}[x, y^2, z^2]$

$R = 1 \cdot S + y \cdot S + z \cdot S + yz \cdot S$

# Homogeneous System of Parameters

- Given a graded $\mathbb{C}$-algebra $R$ of Krull dimension $n$, a set of homogeneous elements $\theta_1, \ldots, \theta_n$ is a

  *homogeneous system of parameters* (h.s.o.p.)

  if

  $R$ is *finitely generated* as a $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module.

- In particular, $\theta_1, \ldots, \theta_n$ are *algebraically independent*

# Homogeneous System of Parameters

- Given a graded $\mathbb{C}$-algebra $R$ of Krull dimension $n$, a set of homogeneous elements $\theta_1, \ldots, \theta_n$ is a

  *homogeneous system of parameters* (h.s.o.p.)

  if

  $R$ is *finitely generated* as a $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module.

- In particular, $\theta_1, \ldots, \theta_n$ are *algebraically independent*
- **Noether Normalization Lemma:**

  An h.s.o.p always exists for finitely generated $\mathbb{C}$-algebras.

# Properties of Homogeneous System of Parameters

- If $R$ is a finitely generated graded $\mathbb{C}$-algebra of dimension $n$, and $a_1, \ldots, a_n \in \mathbb{Z}_{>0}$
  1. $\theta_1, \ldots, \theta_n$ is an h.s.o.p. iff $\theta_1^{a_1}, \ldots, \theta_n^{a_n}$ is an h.s.o.p.
  2. a sequence $f_1, \ldots, f_n$ of homogeneous and algebraically independent elements is regular iff $f_1^{a_1}, \ldots, f_n^{a_n}$ is regular

# Properties of Homogeneous System of Parameters

- If $R$ is a finitely generated graded $\mathbb{C}$-algebra of dimension $n$, and $a_1, \ldots, a_n \in \mathbb{Z}_{>0}$
  1. $\theta_1, \ldots, \theta_n$ is an h.s.o.p. iff $\theta_1^{a_1}, \ldots, \theta_n^{a_n}$ is an h.s.o.p.
  2. a sequence $f_1, \ldots, f_n$ of homogeneous and algebraically independent elements is regular iff $f_1^{a_1}, \ldots, f_n^{a_n}$ is regular
- First property is usually used to make h.s.o.p. of elements of same degree

# Properties of Homogeneous System of Parameters

- If $R$ is a finitely generated graded $\mathbb{C}$-algebra of dimension $n$, and $a_1, \ldots, a_n \in \mathbb{Z}_{>0}$
  1. $\theta_1, \ldots, \theta_n$ is an h.s.o.p. iff $\theta_1^{a_1}, \ldots, \theta_n^{a_n}$ is an h.s.o.p.
  2. a sequence $f_1, \ldots, f_n$ of homogeneous and algebraically independent elements is regular iff $f_1^{a_1}, \ldots, f_n^{a_n}$ is regular
- First property is usually used to make h.s.o.p. of elements of <u>same degree</u>
- **Weak exchange property:** if $f_1, \ldots, f_n$ and $\theta_1, \ldots, \theta_n$ are h.s.o.p.'s of $R$, with $\deg(\theta_i) = \deg(\theta_j)$.
  Then, there is linear combination $\theta = \lambda_1\theta_1 + \cdots + \lambda_n\theta_n$ such that

$$f_1, \ldots, f_{n-1}, \theta \quad \text{is an h.s.o.p.}$$

# Cohen-Macaulay Property

- If $R$ is a graded $\mathbb{C}$-algebra with $\dim(R) = n$, and $\theta_1, \dots, \theta_n$ are an h.s.o.p. for $R$, the following are equivalent
  1. $R$ is a *finitely generated* *free* $\mathbb{C}[\theta_1, \dots, \theta_n]$-module. That is, there is $\eta_1, \dots, \eta_t$ such that

$$R = \bigoplus_{i=1}^{t} \underbrace{\mathbb{C}[\theta_1, \dots, \theta_n]}_{\cong \mathbb{C}[\theta_1, \dots, \theta_n]} \cdot \eta_i \cong \mathbb{C}[\theta_1, \dots, \theta_n]^t \tag{1}$$

  2. $R$ is finitely generated as a free $\mathbb{C}[f_1, \dots, f_n]$-module for *every* h.s.o.p. $f_1, \dots, f_n$

Moreover, the elements $\eta_i$ satisfy equation (1) iff their images form a $\mathbb{C}$-vector space basis over $\underbrace{R/(\theta_1, \dots, \theta_n)}_{\mathbb{C}\text{-vector space}}$

# Cohen-Macaulay Property

- If $R$ is a graded $\mathbb{C}$-algebra with $\dim(R) = n$, and $\theta_1, \ldots, \theta_n$ are an h.s.o.p. for $R$, the following are equivalent
  1. $R$ is a *finitely generated* *free* $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module. That is, there is $\eta_1, \ldots, \eta_t$ such that

     (1)
     $$R = \bigoplus_{i=1}^{t} \mathbb{C}[\theta_1, \ldots, \theta_n] \cdot \eta_i$$

  2. $R$ is finitely generated as a free $\mathbb{C}[f_1, \ldots, f_n]$-module for *every* h.s.o.p. $f_1, \ldots, f_n$

  Moreover, the elements $\eta_i$ satisfy equation (1) iff their images form a $\mathbb{C}$-vector space basis over $R/(\theta_1, \ldots, \theta_n)$
- A graded $\mathbb{C}$-algebra $R$ satisfying the above is *Cohen-Macaulay*
- The decomposition above is called *Hironaka decomposition*

# Cohen-Macaulay Property

- If $R$ is a graded $\mathbb{C}$-algebra with $\dim(R) = n$, and $\theta_1, \ldots, \theta_n$ are an h.s.o.p. for $R$, the following are equivalent
  1. $R$ is a *finitely generated* *free* $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module. That is, there is $\eta_1, \ldots, \eta_t$ such that
  $$R = \bigoplus_{i=1}^{t} \mathbb{C}[\theta_1, \ldots, \theta_n] \cdot \eta_i$$
  2. $R$ is finitely generated as a free $\mathbb{C}[f_1, \ldots, f_n]$-module for *every* h.s.o.p. $f_1, \ldots, f_n$

  Moreover, the elements $\eta_i$ satisfy equation (1) iff their images form a $\mathbb{C}$-vector space basis over $R/(\theta_1, \ldots, \theta_n)$
- A graded $\mathbb{C}$-algebra $R$ satisfying the above is *Cohen-Macaulay*
- The decomposition above is called *Hironaka decomposition*
- "Life is really worth living in an Noetherian Cohen-Macaulay ring"

Hochster 1978

- Graded Algebras, Modules & Cohen-Macaulay Property
- Cohen-Macaulayness of Ring of Invariants of Finite Groups & Primary and Secondary Invariants
- Conclusion
- Acknowledgements

# Invariant Rings of Finite Groups are Cohen-Macaulay

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.

# Invariant Rings of Finite Groups are Cohen-Macaulay

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.
- Every $x_i$ satisfies a *monic* polynomial equation with coefficients in $\mathbb{C}[\mathbf{x}]^G$ integral over $\mathbb{C}[\mathbf{x}]^G$

# Invariant Rings of Finite Groups are Cohen-Macaulay

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.
- Every $x_i$ satisfies a *monic* polynomial equation with coefficients in $\mathbb{C}[\mathbf{x}]^G$ integral over $\mathbb{C}[\mathbf{x}]^G$
- Let $P_i(t) = \prod_{h \in G}(h \circ x_i - t)$

$id \in G$ $\qquad P_i(x_i) = 0$

$P_i(t)$ monic in $t$

# Invariant Rings of Finite Groups are Cohen-Macaulay

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.
- Every $x_i$ satisfies a *monic* polynomial equation with coefficients in $\mathbb{C}[\mathbf{x}]^G$ integral over $\mathbb{C}[\mathbf{x}]^G$
- Let $P_i(t) = \prod_{h \in G}(h \circ x_i - t)$
- Coefficients of $P_i$ are invariants, and $x_i$ is a root

$$g \circ P_i(t) = \prod_{h \in G} \left( h \circ (g \circ x_i) - t \right)$$

$$= \prod_{\bar{h} \in G} \left( \bar{h} \circ x_i - t \right) = P_i(t)$$

$x_i$ is integral (algebraically dependent over invariants)

# Invariant Rings of Finite Groups are Cohen-Macaulay

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.
- Every $x_i$ satisfies a *monic* polynomial equation with coefficients in $\mathbb{C}[\mathbf{x}]^G$ integral over $\underbrace{\mathbb{C}[\mathbf{x}]^G}_{S}$

$$P_i(t) = \underbrace{t^{d_i} + \cdots \in \mathbb{C}[\bar{x}]^G[t]}$$

- This implies $\underline{\mathbb{C}[\mathbf{x}]}$ finitely generated as $\underline{\mathbb{C}[\mathbf{x}]^G\text{-module}}$

$$1, x_i, x_i^2, \ldots, x_i^{d_i-1}$$

$$x_i^{d_i} \in 1 \cdot S + x_i \cdot S + \cdots + x_i^{d_i-1} \cdot S$$

# Invariant Rings of Finite Groups are Cohen-Macaulay

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.
- Every $x_i$ satisfies a *monic* polynomial equation with coefficients in $\mathbb{C}[\mathbf{x}]^G$ integral over $\mathbb{C}[\mathbf{x}]^G$
- This implies $\mathbb{C}[\mathbf{x}]$ finitely generated as $\mathbb{C}[\mathbf{x}]^G$-module
- Let $K = \ker(R_G)$, where $R_G$ is the $\underbrace{\text{Reynolds operator}}_{\text{averaging}}$. Also a $\mathbb{C}[\mathbf{x}]^G$-module

$$R_G : \mathbb{C}[x] \longrightarrow \mathbb{C}[x]^G \quad \text{linear}$$

$$f \in \mathbb{C}[x], \quad p \in \mathbb{C}[x]^G$$

$$R_G(p \cdot f) = p \cdot R_G(f)$$

# Invariant Rings of Finite Groups are Cohen-Macaulay

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.
- Every $x_i$ satisfies a *monic* polynomial equation with coefficients in $\mathbb{C}[\mathbf{x}]^G$ integral over $\mathbb{C}[\mathbf{x}]^G$
- This implies $\mathbb{C}[\mathbf{x}]$ finitely generated as $\mathbb{C}[\mathbf{x}]^G$-module
- Let $K = \ker(R_G)$, where $R_G$ is the Reynolds operator. Also a $\mathbb{C}[\mathbf{x}]^G$-module
- We can write $\mathbb{C}[\mathbf{x}] = \mathbb{C}[\mathbf{x}]^G \oplus K$ direct sum of $\underbrace{\mathbb{C}[\mathbf{x}]^G}_{S}$-modules

# Invariant Rings of Finite Groups are Cohen-Macaulay

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.
- Every $x_i$ satisfies a *monic* polynomial equation with coefficients in $\mathbb{C}[\mathbf{x}]^G$ integral over $\mathbb{C}[\mathbf{x}]^G$
- This implies $\mathbb{C}[\mathbf{x}]$ finitely generated as $\mathbb{C}[\mathbf{x}]^G$-module
- Let $K = \ker(R_G)$, where $R_G$ is the Reynolds operator. Also a $\mathbb{C}[\mathbf{x}]^G$-module
- We can write $\mathbb{C}[\mathbf{x}] = \mathbb{C}[\mathbf{x}]^G \oplus K$ direct sum of $\mathbb{C}[\mathbf{x}]^G$-modules
- Noether Normalization Lemma $\Rightarrow$ h.s.o.p. $\theta_1, \ldots, \theta_n$ for $\mathbb{C}[\mathbf{x}]^G$

# Invariant Rings of Finite Groups are Cohen-Macaulay

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.
- Every $x_i$ satisfies a *monic* polynomial equation with coefficients in $\mathbb{C}[\mathbf{x}]^G$ integral over $\mathbb{C}[\mathbf{x}]^G$

$$\mathbb{C}[\bar{x}] = \bigoplus_{i=1}^{s} p_i \cdot \underline{\mathbb{C}[\bar{x}]^G} \qquad \mathbb{C}[\bar{x}]^G = \bigoplus_{j=1}^{t} f_j \mathbb{C}[\bar{\theta}]$$

- This implies $\mathbb{C}[\mathbf{x}]$ finitely generated as $\mathbb{C}[\mathbf{x}]^G$-module
- Let $K = \ker(R_G)$, where $R_G$ is the Reynolds operator. Also a $\mathbb{C}[\mathbf{x}]^G$-module
- We can write $\mathbb{C}[\mathbf{x}] = \mathbb{C}[\mathbf{x}]^G \oplus K$ direct sum of $\mathbb{C}[\mathbf{x}]^G$-modules
- Noether Normalization Lemma $\Rightarrow$ h.s.o.p. $\theta_1, \ldots, \theta_n$ for $\mathbb{C}[\mathbf{x}]^G$
- $\mathbb{C}[\mathbf{x}]$ is a finite $\mathbb{C}[\mathbf{x}]^G$-module, and $\underline{\mathbb{C}[\mathbf{x}]^G}$ is a finite $\underline{\mathbb{C}[\theta_1, \ldots, \theta_n]}$-module $\Rightarrow$ $\underline{\mathbb{C}[\mathbf{x}]}$ is a finite $\underline{\mathbb{C}[\theta_1, \ldots, \theta_n]}$-module

$p_i f_j$

# Proof of Cohen-Macaulayness

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.
- $\mathbb{C}[\mathbf{x}]$ is a finite $\mathbb{C}[\mathbf{x}]^G$-module, and $\mathbb{C}[\mathbf{x}]^G$ is a finite $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module $\Rightarrow$ $\mathbb{C}[\mathbf{x}]$ is a finite $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module

# Proof of Cohen-Macaulayness

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.
- $\mathbb{C}[\mathbf{x}]$ is a finite $\mathbb{C}[\mathbf{x}]^G$-module, and $\mathbb{C}[\mathbf{x}]^G$ is a finite $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module $\Rightarrow \mathbb{C}[\mathbf{x}]$ is a finite $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module
- Thus $\theta_1, \ldots, \theta_n$ is an h.s.o.p. for $\mathbb{C}[\mathbf{x}]$

# Proof of Cohen-Macaulayness

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.
- $\mathbb{C}[\mathbf{x}]$ is a finite $\mathbb{C}[\mathbf{x}]^G$-module, and $\mathbb{C}[\mathbf{x}]^G$ is a finite $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module $\Rightarrow \mathbb{C}[\mathbf{x}]$ is a finite $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module
- Thus $\theta_1, \ldots, \theta_n$ is an h.s.o.p. for $\mathbb{C}[\mathbf{x}]$
- $\mathbb{C}[\mathbf{x}]$ is Cohen-Macaulay      take $x_1, \ldots, x_n$ as h.s.o.p.

# Proof of Cohen-Macaulayness

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.
- $\mathbb{C}[\mathbf{x}]$ is a finite $\mathbb{C}[\mathbf{x}]^G$-module, and $\mathbb{C}[\mathbf{x}]^G$ is a finite $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module $\Rightarrow$ $\mathbb{C}[\mathbf{x}]$ is a finite $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module
- Thus $\theta_1, \ldots, \theta_n$ is an h.s.o.p. for $\mathbb{C}[\mathbf{x}]$
- $\mathbb{C}[\mathbf{x}]$ is Cohen-Macaulay take $x_1, \ldots, x_n$ as h.s.o.p.
- Our Cohen-Macaulay Theorem says that $\mathbb{C}[\mathbf{x}]$ is a finitely generated free $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module!

# Proof of Cohen-Macaulayness

- Let $G$ be a finite group acting linearly on $\mathbb{C}^n$. The invariant ring $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.
- $\mathbb{C}[\mathbf{x}]$ is a finite $\mathbb{C}[\mathbf{x}]^G$-module, and $\mathbb{C}[\mathbf{x}]^G$ is a finite $\mathbb{C}[\theta_1, \dots, \theta_n]$-module $\Rightarrow$ $\mathbb{C}[\mathbf{x}]$ is a finite $\mathbb{C}[\theta_1, \dots, \theta_n]$-module
- Thus $\theta_1, \dots, \theta_n$ is an h.s.o.p. for $\mathbb{C}[\mathbf{x}]$
- $\mathbb{C}[\mathbf{x}]$ is Cohen-Macaulay take $x_1, \dots, x_n$ as h.s.o.p.
- Our Cohen-Macaulay Theorem says that $\mathbb{C}[\mathbf{x}]$ is a finitely generated free $\mathbb{C}[\theta_1, \dots, \theta_n]$-module!
- From module decomposition $\mathbb{C}[\mathbf{x}] = \underline{\mathbb{C}[\mathbf{x}]}^G \oplus \underline{K}$ we get *finite dimensional $\mathbb{C}$-vector space* decomposition

$$\mathbb{C}[\mathbf{x}]/(\theta_1, \dots, \theta_n) = \mathbb{C}[\mathbf{x}]^G/(\theta_1, \dots, \theta_n) \oplus K/(\theta_1, \dots, \theta_n)$$

# Proof of Cohen-Macaulayness

- From module decomposition $\mathbb{C}[\mathbf{x}] = \mathbb{C}[\mathbf{x}]^G \oplus K$ we get *finite dimensional* *$\mathbb{C}$-vector space* decomposition

$$\mathbb{C}[\mathbf{x}]/(\theta_1, \ldots, \theta_n) = \mathbb{C}[\mathbf{x}]^G/(\theta_1, \ldots, \theta_n) \oplus K/(\theta_1, \ldots, \theta_n)$$

# Proof of Cohen-Macaulayness

- From module decomposition $\mathbb{C}[\mathbf{x}] = \mathbb{C}[\mathbf{x}]^G \oplus K$ we get *finite dimensional $\mathbb{C}$-vector space* decomposition

$$\boxed{\mathbb{C}[\mathbf{x}]/(\theta_1, \ldots, \theta_n)} = \boxed{\mathbb{C}[\mathbf{x}]^G/(\theta_1, \ldots, \theta_n)} \oplus K/(\theta_1, \ldots, \theta_n)$$

- Taking vector-space basis
$\alpha_1, \ldots, \alpha_t$ for $\mathbb{C}[\mathbf{x}]^G/(\theta_1, \ldots, \theta_n)$ and
$\beta_1, \ldots, \beta_s$ for $K/(\theta_1, \ldots, \theta_n)$
and taking their pre-images in $\mathbb{C}[\mathbf{x}]^G$ and $K$ we get our Hironaka decomposition.

# Proof of Cohen-Macaulayness

- From module decomposition $\mathbb{C}[\mathbf{x}] = \mathbb{C}[\mathbf{x}]^G \oplus K$ we get *finite dimensional* *$\mathbb{C}$-vector space* decomposition

$$\mathbb{C}[\mathbf{x}]/(\theta_1, \ldots, \theta_n) = \mathbb{C}[\mathbf{x}]^G/(\theta_1, \ldots, \theta_n) \oplus K/(\theta_1, \ldots, \theta_n)$$

- Taking vector-space basis
  $\alpha_1, \ldots, \alpha_t$ for $\mathbb{C}[\mathbf{x}]^G/(\theta_1, \ldots, \theta_n)$ and
  $\beta_1, \ldots, \beta_s$ for $K/(\theta_1, \ldots, \theta_n)$
  and taking their pre-images in $\mathbb{C}[\mathbf{x}]^G$ and $K$ we get our Hironaka decomposition.
- This shows $\mathbb{C}[\mathbf{x}]^G$ is Cohen-Macaulay.

# Primary and Secondary Invariants

- Hironaka decomposition is very useful way of representing invariant ring of finite groups!

## Primary and Secondary Invariants

- Hironaka decomposition is very useful way of representing invariant ring of finite groups!
- Every invariant $f(\mathbf{x})$ can then be written as

$$f(\mathbf{x}) = \sum_{i=1}^{t} \eta_i(\mathbf{x}) \cdot p_i(\theta_1, \ldots, \theta_n)$$

$$\mathbb{C}[\bar{x}]^G = \bigoplus_{i=1}^{t} \eta_i \cdot \mathbb{C}[\theta_1, \ldots, \theta_n]$$

# Primary and Secondary Invariants

- Hironaka decomposition is very useful way of representing invariant ring of finite groups!
- Every invariant $f(\mathbf{x})$ can then be written as

$$f(\mathbf{x}) = \sum_{i=1}^{t} \eta_i(\mathbf{x}) \cdot \underline{p_i(\theta_1, \ldots, \theta_n)}$$

- We call the $\theta_1, \ldots, \theta_n$ *primary invariants* and $\eta_1, \ldots, \eta_{\cancel{n}\,t}$ *secondary invariants*

$$\mathbb{C}[\bar{x}]^G = \bigoplus_{i=1}^{t} \eta_i \cdot \mathbb{C}[\theta_1, \ldots, \theta_n]$$

## Primary and Secondary Invariants

- Hironaka decomposition is very useful way of representing invariant ring of finite groups!
- Every invariant $f(\mathbf{x})$ can then be written as

$$f(\mathbf{x}) = \sum_{i=1}^{t} \eta_i(\mathbf{x}) \cdot p_i(\theta_1, \ldots, \theta_n)$$

- We call the $\theta_1, \ldots, \theta_n$ *primary invariants* and $\eta_1, \ldots, \eta_n$ *secondary invariants*
- Hironaka decompositions are not unique (in fact, one could have many of them)
- Also, degrees of primary and secondary invariants are not unique

# Primary and Secondary Invariants

- Hironaka decomposition is very useful way of representing invariant ring of finite groups!
- Every invariant $f(\mathbf{x})$ can then be written as

$$f(\mathbf{x}) = \sum_{i=1}^{t} \eta_i(\mathbf{x}) \cdot p_i(\theta_1, \ldots, \theta_n)$$

- We call the $\theta_1, \ldots, \theta_n$ *primary invariants* and $\eta_1, \ldots, \eta_n$ *secondary invariants*
- Hironaka decompositions are not unique (in fact, one could have many of them)
- Also, degrees of primary and secondary invariants are not unique
- But if we find primary invariants of certain degrees $d_1, \ldots, d_n$ then the number of secondary invariants is determined, as well as their degrees!

$$t = \frac{d_1 \cdot d_2 \cdots d_n}{|G|}$$

# Primary and Secondary Invariants

- Hironaka decomposition is very useful way of representing invariant ring of finite groups!
- Every invariant $f(\mathbf{x})$ can then be written as

$$f(\mathbf{x}) = \sum_{i=1}^{t} \eta_i(\mathbf{x}) \cdot p_i(\theta_1, \ldots, \theta_n)$$

- We call the $\theta_1, \ldots, \theta_n$ *primary invariants* and $\eta_1, \ldots, \eta_n$ *secondary invariants*
- Hironaka decompositions are not unique (in fact, one could have many of them)
- Also, degrees of primary and secondary invariants are not unique
- But if we find primary invariants of certain degrees $d_1, \ldots, d_t$ then the number of secondary invariants is determined, as well as their degrees!
- Computational aspects of Hironaka's decomposition widely open!

# Basic Thoughts on Computation

$$\underbrace{S_n}_{n!} \curvearrowright \mathbb{C}^n \qquad \boxed{\mathbb{C}[\bar{x}]^{S_n}}$$

the invariants must be pretty hard to compute!

elementary symmetric polynomials

$$R_{S_n}(f) = \frac{1}{n!}\sum_{\sigma \in S_n} \sigma \circ f \qquad \underbrace{\prod (t - x_i)}_{\text{low-degree}}$$

$$P_i(t) = \prod_{h \in S_n} (t - h \circ x_i) \xRightarrow{\text{interpolation}} \text{low complexity}$$

$$\prod_{i=1}^{n} P_i = \prod_{i \in n} \prod_{h \in S_n} (t - h \circ x_i) = \left( \prod_{i=1}^{n} (t - x_i) \right)^{n!}$$

$$\mathbb{C}[\bar{x}]^{S_n} = 1 \cdot \mathbb{C}[e_1, \dots, e_n]$$

<u>G reflection</u> group then same thing happens.

$A_n$ $\qquad \underbrace{e_1, \dots, e_n}_{\text{primary}} \qquad \underbrace{\Delta = \prod_{i<j} (x_i - x_j)}_{\text{secondary}}$

$G \subset S_n$

- Graded Algebras, Modules & Cohen-Macaulay Property
- Cohen-Macaulayness of Ring of Invariants of Finite Groups & Primary and Secondary Invariants
- Conclusion
- Acknowledgements

# Conclusion

- Today we proved that invariant rings of finite groups are Cohen-Macaulay and learned about Hironaka decomposition
- Cohen-Macaulayness gives us great algebro-geometric properties of invariant rings!
- Many different Hironaka decompositions not a bad thing! One of them could be efficiently computable!
- Lots of open questions in this area!

# Acknowledgement

- Lecture based on the book

Sturmfels: Algorithms in Invariant Theory