# Algebraic Geometry, Lecture 4

Frank-Olaf Schreyer

Saarland University, Perugia 2021

# Overview

1. Monomial orders on free modules
2. Division with remainder in free modules
3. Proof of Buchberger's criterion
4. Schreyer's corollary
5. Module membership problem

# Monomial orders in free modules

**Notation.** We denote the polynomial ring by $S = K[x_1, \ldots, x_n]$ and the free $S$-module $S^k$ with basis $e_j = (0, \ldots 1, \ldots 0)^t$ by

$$F = S^k.$$

**Definition.** A **monomial** in $F$ is an element of the form $x^\alpha e_j$, a **term** in $F$ is an element of the form $ax^\alpha e_j$ with $a \in K$.
A **monomial order** on $F$ is a complete order $>$ of all the monomials in F satisfying

$$x^\alpha e_j > x^\beta e_i \implies x^\gamma x^\alpha e_j > x^\gamma x^\beta e_i$$

for any two monomials in $F$ and any monomial $x^\gamma$ in $S$.
Every element $f \in F$ is a finite sum of terms, and we can define the **lead term** of $f$ as before:
If $f = \sum_{\alpha,j} f_{\alpha,j} x^\alpha e_j$, then $\mathrm{Lt}(f) = f_{\beta,i} x^\beta e_i$ where

$$x^\beta e_i = \max\{x^\alpha e_j \mid f_{\alpha,j} \neq 0\}.$$

# Examples of monomial orders

**Definition.** A monomial order $>$ on $F$ is **global** if

$$x_i e_j > e_j \text{ holds for } i = 1, \ldots, n \text{ and } j = 1, \ldots, k.$$

**Examples.** Let $>$ be a global monomial order on $S$. We can define a monomial order on $F$ in two ways:

1.) $x^\alpha e_j >_1 x^\beta e_i$ iff $x^\alpha > x^\beta$ or $(x^\alpha = x^\beta$ and $j > i)$,

2.) $x^\alpha e_j >_2 x^\beta e_i$ iff $j > i$ or $(j = i$ and $x^\alpha > x^\beta)$

which we call the **monomial before component order** and **component before monomial order**, respectively.

There are many more ways to define global monomial orders on $F$, for example, weight orders, where also the $e_j$ get some weights.

A monomial order on $F = S^r$ gives $r$ monomial orders on $S$ using the isomomophism

$$S \cong Se_j.$$

These might not coincide, but in all examples we are considering they do.

# Division with remainder

**Theorem.** *Let $>$ be a global monomial order on $F = S^k$ and let $f_1, \ldots, f_r \in F$ be non-zero polynomial vectors. For every $f \in F$ there exist uniquely determined $g_1, \ldots, g_r \in S$ and a unique remainder $h \in F$ satisfying*

1) $f = g_1 f_1 + \ldots + g_r f_r + h$
2a) *No term of $g_j \operatorname{Lt}(f_j)$ is divisible by a lead term $\operatorname{Lt}(f_i)$ for some $i < j$.*
2b) *No term of $h$ is divisible by a lead term $\operatorname{Lt}(f_j)$.*

**Proof.** As before we write

$$f = g_1^{(0)} \operatorname{Lt}(f_1) + \ldots + g_r^{(0)} \operatorname{Lt}(f_r) + h^{(0)}$$

satisfying 2a) and 2b). Consider

$$f^{(1)} = f - (g_1^{(0)} f_1 + \ldots + g_r^{(0)} f_r + h^{(0)}).$$

Then $\operatorname{Lt}(f^{(1)}) < \operatorname{Lt}(f)$ and we can iterate until $f^{(k)} = 0$. □

# Remarks

1. Notice that to perform the division algorithm we do not need to know the monomial order precisely. We only need to know the lead terms $\mathrm{Lt}(f_j)$.
2. The role of the global monomial order is to guarantee that the algorithm terminates.
3. This in turn is based on the fact that monomial submodules of $F$ are finitely generated.
4. We deduce the descending chain condition:
   *Every strictly decreasing chain $m_1 > m_2 > \ldots$ of monomials in $F$ with respect to a global monomial order is finite.*

# Proof of the descending chain condition

Let $m_1 > m_2 > \ldots$ a (possibly infinite) strict chain of monomials in $F$. Let $I = (\{m_k \mid k \geq 1\}) \subset F$ be the monomial submodule generated by the $m_k$'s. By Dixon's Lemma $I$ is generated by a finite set $J$ of monomials. Set

$$m = \min\{J\}.$$

$m$ exists because $J$ is finite, and $>$ is a total order. Since a global monomial order refines divisibility in $F$ we have

$$\min(J) = \min\{\tilde{m} \mid \tilde{m} \text{ is a monomial in } I\} = \min\{m_k\}$$

The last minimum exists if and only if the chain is finite. □

# Gröbner basis in $F$

Let $I \subset F$ be a submodule. Then $\mathrm{Lt}(I) = (\{\mathrm{Lt}(f) \mid f \in I\})$ is the lead term module of $I$.
$f_1, \ldots, f_r \in I$ is a Gröbner basis iff $\mathrm{Lt}(I) = (\mathrm{Lt}(f_1, \ldots, \mathrm{Lt}(f_r))$.

- Since every monomial module is finitely generated, every submodule of $F$ has a Gröbner basis.
- The remainder of $f \in F$ by a Gröbner basis $f_1, \ldots, f_r$ is zero iff $f \in (f_1, \ldots, f_r)$.
- In particular a Gröbner basis of $I$ is a generating set of $I$.
- The monomials $m \in F$ with $m \notin \mathrm{Lt}(I)$ represent a $K$-vector space basis of the quotient module $M = F/I$.

# Buchberger's criterion

For submodules $N_1, N_2 \subset M$ of an $R$-module $M$ the colon ideal is defined as

$$N_1 : N_2 = \{a \in R \mid aN_2 \subset N_1\}.$$

**Notation.** Let $f_1, \ldots, f_r \in F$ be polynomial vectors. We define monomial ideals as follows

$$M_j = (\mathrm{Lt}(f_1, \ldots, \mathrm{Lt}(f_{j-1})) : \mathrm{Lt}(f_j)$$

for $j = 2, \ldots, r$.
For each minimal generator $x^\alpha \in M_j$ the multiple $x^\alpha f_j$ is an expression not allowed in the division theorem by condition 2a).

**Theorem.** *With notation as above, $f_1, \ldots, f_r$ is a Gröbner basis for $(f_1, \ldots, f_r)$ if and only if for each $j = 2, \ldots, r$ and each minimal generator $x^\alpha$ of $M_j$ the remainder of $x^\alpha f_j$ divided by $f_1, \ldots, f_r$ is zero.*

part 2

# Proof of Buchberger's criterion

If $f_1, \ldots, f_r$ is a Gröbner basis, then the remainder of $x^\alpha f_j$ is zero, because $x^\alpha f_j \in (f_1, \ldots, f_r)$. For the converse assume that the condition of the criterion is satisfied. Then for each minimal generator $x^\alpha \in M_j$ we have an division expression with remainder zero:

$$x^\alpha f_j = \sum_{i=1}^{r} g_i^{(j,\alpha)} f_i$$

satisfying condition 2a). Consider $F_1 = S^r$ and the $S$-module homomorphism

$$\varphi \colon F_1 \to F,\ e_i \mapsto f_i$$

Then

$$G^{(j,\alpha)} = x^\alpha e_j - \sum_{i=1}^{r} g_i^{(j,\alpha)} e_i$$

is a syzygy of $f_1, \ldots, f_r$, in other words, it is an element of $\ker(\varphi)$.

# The induced order

We define the **induced monomial order** on $F_1$ by

$$x^\alpha e_j > x^\beta e_i \iff x^\alpha \operatorname{Lt}(f_j) > x^\beta \operatorname{Lt}(f_i) \text{ or}$$
$$x^\alpha \operatorname{Lt}(f_j) = x^\beta \operatorname{Lt}(f_i) \text{ up to a non-zero factor in } K$$
$$\text{and } j > i.$$

**Remark.** We could avoid the phrase up to a non-zero factor in $K$ if we assume that the $f_j$ are monic, i.e., have leading coefficients 1.

**Lemma.** *With respect to the induced monomial orders the syzygies $G^{(j,\alpha)} \in F_1$ have the lead terms*

$$\operatorname{Lt}(G^{(j,\alpha)}) = x^\alpha e_j.$$

# Proof of the Lemma

**Proof.** Since $x^\alpha f_j = \sum_{i=1}^{r} g_i^{(j,\alpha)} f_i$ satisfies condition 2a), we have

$$\mathrm{Lt}(x^\alpha f_j) = \max\{\mathrm{Lt}(g_i^{(j,\alpha)} f_i)\},$$

and equality is achieved for $\tilde{i} = \min\{i \mid x^\alpha \mathrm{Lt}(f_j) \in (\mathrm{Lt}(f_i))\}$:

$$x^\alpha \mathrm{Lt}(f_j) = \mathrm{Lt}(g_{\tilde{i}}^{(j,\alpha)}) \mathrm{Lt}(f_{\tilde{i}}).$$

All other terms of any $g_i^{(j,\alpha)} \mathrm{Lt}(f_i)$ are strictly smaller than $x^\alpha \mathrm{Lt}(f_j)$. Since $\tilde{i} < j$, we obtain

$$\mathrm{Lt}(G^{(j,\alpha)}) = x^\alpha e_j$$

from the definition of the induced order.

# Proof of Buchberger's criterion, 2

Let $f = a_1 f_1 + \ldots + a_r f_r \in (f_1, \ldots, f_r)$ be an arbitrary element. We consider

$$A = \sum_{i=1}^{r} a_i e_i \in F_1$$

and the remainder $H = \sum_{i=1}^{r} g_i e_i$ of $A$ divided by the $G^{(j,\alpha)}$'s. Since the $G^{(j,\alpha)}$ are syzygies of $f_1, \ldots, f_r$, we have

$$f = a_1 f_1 + \ldots + a_r f_r = g_1 f_1 + \ldots + g_r f_r.$$

Indeed

$$A = \sum_{(j,\alpha)} g_{j,\alpha} G^{(j,\alpha)} + H \in F_1 \implies \varphi(A) = \varphi(H).$$

By the definition of the monomial ideals $M_j$ and the $G^{(j,\alpha)}$ we have removed in the remainder $H = \sum_{i=1}^{r} g_i e_i$ any term $t$ from $g_j$ such that $t\,\mathrm{Lt}(f_j) \in (\mathrm{Lt}(f_1), \ldots, Lt(f_{j-1}))$.

# End of the proof and Schreyer's corollary

In other words the coefficients $g_1, \dots g_r$ satisfy the condition 2a) for division by $f_1, \dots, f_r$ in $F$. Thus

$$\mathrm{Lt}(f) = \max\{\mathrm{Lt}(g_j f_j)\} \in (\mathrm{Lt}(f_1), \dots, \mathrm{Lt}(f_r))$$

and

$$\mathrm{Lt}((f_1, \dots, f_r)) = (\mathrm{Lt}(f_1), \dots, \mathrm{Lt}(f_r)),$$

i.e., $f_1, \dots, f_r$ is a Gröbner basis of $(f_1, \dots, f_r)$. □

**Corollary.** *If $f_1, \dots, f_r \in F$ is a Gröbner basis, then the $G^{(j,\alpha)}$'s in $F_1$ form a Gröbner basis of the syzygy module* $\ker(\varphi)$ *where*

$$\varphi \colon F_1 \to F, e_j \mapsto f_j.$$

part 3

# Proof of the corollary

Let $G$ be an element of $\ker(\varphi)$. Consider the remainder

$$H = (g_1, \ldots, g_r)^t$$

of the division of $G$ by the $G^{(j,\alpha)}$. The coefficients $g_j$ satisfy condition 2a) for the division by $f_1, \ldots, f_r$. Thus

$$\mathrm{Lt}(g_1 f_1 + \ldots + g_r f_r) = \max\{\mathrm{Lt}(g_j f_j)\}$$

On the other hand $g_1 f_1 + \ldots + g_r f_r = \varphi(H) = \varphi(G) = 0$. Thus all $g_j = 0$ and hence $H$ is zero.
Thus every $G \in \ker(\varphi)$ has remainder zero under the division by the $G^{(j,\alpha)}$. Applying the condition 2a) for the division by the $G^{(j,\alpha)}$'s, we see that

$$\mathrm{Lt}(G) \in (\{\mathrm{Lt}(G^{(j,\alpha)})\}).$$

# Example

We compute a Gröbner basis of $I = (y - x^2, z - x^3) \subset K[x, y, z]$ with respect to $>_{lex}$.

# Example

We compute a Gröbner basis of $I = (y - x^2, z - x^3) \subset K[x, y, z]$ with respect to $>_{lex}$.

| | | | | | |
|---|---|---|---|---|---|
| $x^2 - y$ | $-x$ | $-y$ | $-z$ | | |
| $x^3 - z$ | 1 | | | | |
| $xy - z$ | -1 | $x$ | $y$ | $-z$ | $-y^2$ |
| $xz - y^2$ | | 1 | $x$ | $y$ | $z$ |
| $y^3 - z^2$ | | | | 1 | $x$ |
| | | $z$ | $-y$ | $x$ | $-1$ |

Note that $y^3 - z^2 \in (y - x^2, z - x^3) \cap K[y, z]$.

We will later see that computing a Gröbner basis of $I \subset K[x_1, \ldots, x_n]$ with respect to $>_{\text{lex}}$ allows to compute the elimination ideals

$$I_j = I \cap K[x_{j+1}, \ldots, x_n]$$

obtained from $I$ by eliminating the first $j$ variables.

# Module membership problem

**Algorithm.** $f \in (f_1, \ldots, f_r)$ ?

**Input.** $f_1, \ldots, f_r \in F$ and a further polynomial vector $f \in F$.

**Output.** A boolean value $t$
and if $t = \mathit{true}$ coefficients $g_1, \ldots, g_r \in S$ such that $f = g_1 f_1 + \ldots + g_r f_r$.

1. Choose a global monomial order $>$ on $F$.
2. Compute a Gröbner basis $f_1, \ldots, f_s$ of $(f_1, \ldots, f_r)$ with Buchberger's algorithm.
3. Divide $f$ by $f_1, \ldots, f_s$ with remainder:
$$f = \tilde{g}_1 f_1 + \ldots + \tilde{g}_s f_s + h.$$
4. If $h \neq 0$ the return $t = \mathit{false}$ else $t = \mathit{true}$ and recursively substitute $f_k$ by a linear combination of $f_1, \ldots, f_{k-1}$ for $k = s, \ldots, r+1$ to obtain an expression $f = g_1 f_1 + \ldots + g_r f_r$.
5. return $t$ and $g_1, \ldots, g_r$.