Constructing a Groebner Basis

\[ R = \mathbb{F}[x_1, \ldots, x_n] \], \text{ } \mathbb{F} \text{ a field} \\
we have a monomial order

\text{Let } f_1, f_2 \in \mathbb{F}[x_1, \ldots, x_n] \text{ be mon- } \text{one.} \\
\text{Let } \text{LT}(f_1) = a_1 x_1^{\alpha_1} \ldots x_n^{\alpha_n}, \text{ LT}(f_2) = b_2 x_1^{\beta_1} \ldots x_n^{\beta_n}. \\
\text{Let } M = x_1^{\max(\alpha_1, \beta_1)} \ldots x_n^{\max(\alpha_n, \beta_n)} \text{, } a_{i_1} b_{i_2} \neq 0. \text{ } \in \mathbb{F} \\
The construction designed to cancel the leading terms:
\[ S(f_1, f_2) = \frac{1}{\text{LT}(f_1)} f_1 - \frac{1}{\text{LT}(f_2)} f_2. \]

**Lemma:** Suppose \( f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_m] \) be non-zero polynomials with the same multi-degree. Suppose \( a_1, \ldots, a_k \in \mathbb{F} \) are such that

\[ h = a_1 f_1 + \cdots + a_k f_k \]

has lower multi-degree. Then there exist \( b_i \in \mathbb{F} \) such that

\[ h = b_1 S(f_1, f_2) + \cdots + b_{k-1} S(f_{k-1}, f_k). \]
Proof: WLOG, $f_1, \ldots, f_k$ are monic. (The $S$'s stay the same when we divide by the coefficients of the leading terms.) But then

$$S(f_{i-1}, f_i) = f_{i-1} - f_i.$$ 

Write

$$h = a_1 f_1 + \ldots + a_k f_k = a_1 (f_1 - f_k) + (a_1 + a_2) (f_2 - f_3) + \ldots + (a_1 + \ldots + a_{k-1}) (f_{k-1} - f_k) + (a_1 + \ldots + a_k) f_k .$$

All the summand except the last one have lower multi-degree. So since $h$ has a lower multi-degree as well, we must have $a_1 + \ldots + a_k = 0$. $\square$
Theorem (the Buchberger criterion): Nonzero polynomials $g_1, \ldots, g_k \in \mathbb{K}[x_1, \ldots, x_n]$ are a Gröbner basis of $(g_1, \ldots, g_k)$ if and only if each $S(g_i, g_j)$ produces remainder $0$ upon long division by $g_1, \ldots, g_k$ (at least one implementation).

The Buchberger algorithm for finding a Gröbner basis of $(g_1, \ldots, g_k)$. From all the $S(g_i, g_j)$'s $i < j$, perform long division by $g_1, \ldots, g_k$, append the remainders to $g_1, \ldots, g_k$. Repeat until all remainders
are 0. Simplifications: if \( g_j \mid g_i \), you can throw out \( g_j \). More generally, if
\[ g_j \in (g_1, \ldots, g_{j-1}, g_{j+1}, \ldots, g_k) \]
then throw \( g_j \) out.

Proof of the Theorem: Necessity (any implementation of division) is obvious — anything in the ideal will produce 0 remainder (< unique).

Sufficiency: let \( I = (g_1, \ldots, g_k) \). It suffices to prove that \( \text{LT}(I) = (\text{LT}(g_1), \ldots, \text{LT}(g_k)) \).
So let \( f \in I, \, f \neq 0 \).

\[
f = h_1 q_1 + \ldots + h_m q_m \quad h_i \in \mathbb{R}[x_1, \ldots, x_m]
\]

Choose \( h_i \) such that \( \max \{ \partial (h_1 q_1), \ldots, \partial (h_m q_m) \} = \alpha_m \)
is the smallest possible. We know \( \alpha_m \geq \Theta(f) \).

If \( m = \Theta(f) \), we are done: Just take the leading term. So suppose \( m > \Theta(f) \). WLOG, \( h_1, \ldots, h_k \) are monomials

\[
h_i = a_i x_{i_1}^{\alpha_{i_1}} \ldots x_{i_m}^{\alpha_{i_m}}.
\]

On the right hand side, let \( S = \{ i_1, \ldots, i_j \} \) be the set of all \( i \) such that \( \partial (h_i q_i) = \alpha_m \).
Then $0 \left( \sum_{i \in S} h \cdot g_i \right) < m$

\[
f - \sum_{i \in S} h \cdot g_i
\]

So we can apply the Lemma: lower multi-degree

\[
\sum_{i \in S} h \cdot g_i = \sum_{i,j \in S} a_{ij} \cdot s(h \cdot g_i, h \cdot g_j)
\]

The division algorithm does not raise multi-degrees! a monomial multiple

Moreover, they are linear combinations of terms with lower or equal degrees!

of $s(g_i, g_j) \in I$

Contradiction with the minimality of $m$. $\square$
HW 1) Compute a Groebner basis of
\((x^3 + x^2y, xy + 1)\)
lexicographic order, \(x > y\), \(F = \mathbb{Q}\).