Definition 0.1 — Gröbner Basis.
A Gröbner basis G of an ideal I in a polynomial ring over a field is a generating set of I characterized by any one of the following properties

- the ideal generated by the leading terms of polynomials in I equals the ideal generated by the leading terms of G;

  Example 0.2 — . Consider $p_1 = y - x^2$ and $p_2 = z - x^3$. Set $I := (p_1, p_2)$.

  1. Under the lexicographic ordering $y > z > x$, $G := \{p_1, p_2\}$ forms a Gröbner basis. The ideal generated by the leading terms of G is

     $$(\mathrm{LT}(p_1), \mathrm{LT}(p_2)) = (y, z). \tag{1}$$

     On the other hand,
  2. However, if we choose the lexicographic ordering $x > y > z$, then $\{p_1, p_2\}$ is not a Gröbner basis. The ideal generated by the leading terms of G is

     $$(\mathrm{LT}(p_1), \mathrm{LT}(p_2)) = (-x^2, -x^3) = (x^2). \tag{2}$$

     But $x \cdot p_1 - p_2 \in I$ and it is

     $$x \cdot p_1 - p_2 = -x^3 + xy + x^3 - z = xy - z \tag{3}$$

     which is clearly not included in (x^2).

- the leading term of any polynomial in I is divisible by the leading term of some polynomial in G;

  Example 0.3 — . Again, consider $p_1 = y - x^2$ and $p_2 = z - x^3$. Set $I := (p_1, p_2)$.

  1. Again, under the lexicographic ordering $y > z > x$, the leading terms of the polynomials in $G = \{p_1, p_2\}$ are $\{y, z\}$. With similar reasoning as above, G forms a Gröbner basis.
  2. But if the lexicographic ordering is $x > y > z$, then the leading polynomials in $\{p_1, p_2\}$ are ... the same as above.

- the multivariate division of any polynomial in the polynomial ring R by G gives unique remainder;