Gröbner Basis

1. Polynomial Division:
   1. Leading monomial: Monomial of the polynomial with the highest degree.
   2. Leading coefficient: Coefficient of the leading monomial.
   3. Leading term: Product of *a* and *b*.
   4. Degree of polynomial: Degree of the leading term.

* *Degree of remainder always lesser than that of the divisor.*

1. Monomial Orderings:
   1. Lexicographic ordering or Lex ordering:



* 1. Graded lex order:



1. Multi-variable Polynomial Division:
   1. Dividing 2 polynomials:



* 1. Dividing by a system of polynomials:



1. Rings and Fields:
   1. Rings: A ring is a non-empty set equipped with 2 operations that satisfy the following axioms:
      1. It is closed under addition:
      2. Associative
      3. Commutative
      4. Should have an additive identity:
      5. Should have additive inverse.
      6. Closed under multiplication:
      7. Distributive, associative.

*A set of* ***Z****,* ***Q*** *and* ***C*** *are rings. Set of even numbers form a ring but set of odd nos don’t.*

* 1. Field: A field is a commutative ring with identity in which every nonzero element has an inverse. *Fields are closed under division also while rings are not.*

*A set of* ***Q*** *and* ***C*** *can be called fields. A subset of a ring need not be a ring but one which is, is known as a subring.*

1. Ideals:

A subring I of a ring R is an **ideal** *iff* when *r ∈ R* and *a ∈ I,* then *r.a ∈ I* and *a.r ∈ I*. For eg. a set of even integers is an ideal of the ring ***Z*** and {***0R***} and ***R*** are ideals for every ring ***R***.



* The zero ideal is generated by a single element set; *I=<0R>={0R} ∀* ring ***R***.
* Ideals can have different set of generators.

Noetherian Rings: A ring ***R*** is a Noetherian ring if every ideal *I*of ***R*** is finitely generated. And, according to Hilbert’s Basis Theorem if *R* is a Noetherian ring then so is the polynomial ring *R[x]*.

1. Gröbner Basis: (LM(*f*) denotes fixed monomial ordering and LT(*f*) denotes the leading term.)
   1. A Gröbner basis of an ideal *I* is a set of generators of *I*.



For a fixed monomial ordering a finite subset *G={g1,...,gt}* of an ideal *I* is said to be a Gröbner basis if:



* 1. Reduced Gröbner basis: A RGb for a set of polynomials *F* is a Gröbner basis *G* of *F* such that:
     1. LC is *1 ∀ p ∈ G*.
     2. For all *p ∈ G,* none of the terms of *p* is divisible by the *LT(q) ∀ q ∈ G-{p}*.
  2. S-polynomials:



* 1. Example:



1. Buchberger’s Algorithm:
   1. Steps:
      1. Chose the monomial ordering.
      2. Start with *G := F*.
      3. Repeat G’ := G until G = G’
   2. Example:



1. Unique Remainders:
   1. Example:



A zero remainder implies that the solutions of *F* are the roots of *f*. In conclusion, to divide a polynomial *f* by a set of polynomials *F* to get a unique remainder the following steps are to be followed.

* + 1. Compute Gröbner basis *G={g1,...,gt}* of the ideal *I=<F>.*
    2. Divide *f* by *G* to get a unique remainder *r*.
    3. Trace the quotients *qi*, *i=1 to n* from the S-polynomials to write *f=q1f1+...+qnfn+r.*