The Characteristic Sets Method

- Let K be a field of characteristic 0 and let $x_1, \ldots, x_n$ be a set of indeterminates. Let $K[x_1, \ldots, x_n]$ be the ring of polynomials in these indeterminates.

- Fix an ordering on the variables: $x_1 \prec \ldots \prec x_n$

- Let f and g be any two non-zero and non-constant polynomials in $K[x_1, \ldots, x_n]$.

- We define the *degree of f with respect to the variable x_i*, denoted as $deg_{x_i}(f)$, to be the maximum degree of the variable x_i in f.

- Let c be the greatest subscript such that x_c actually occurs in f. We define:

  1. *cls(f)* = the *class* of $f = c$.
  2. *lvar(f)* = the *leading variable* of $f = x_c$.
  3. *cdeg(f)* = the *class degree* of $f = deg_{x_c}(f)$.
  4. *ini(f)* = the *initial* of f with respect to *lvar(f)* = coefficient of x_c. Note that *ini(f)* is a polynomial in $K[x_1, \ldots, x_{c-1}]$.

- We say that polynomial f has a *lower rank* than polynomial g if either $cls(f) < cls(g)$ or $cls(f) = cls(g) \Rightarrow cdeg(f) < cdeg(g)$

- A polynomial g is said to be *reduced* with respect to f if $deg_{x_c}(g) < cdeg(f)$.

- If g is not reduced with respect to f, we can pseudo-divide g by f as polynomials in x_c and obtain the *pseudo-remainder* of f with respect to g such that
$$(ini(f))^s g = qf + r$$
where q and $r = prem(g, f)$ are both polynomials, $s = deg_{x_c} g - cdeg f + 1$, and either $r = 0$ or $deg_{x_c}(r) < cdeg(f)$.
The following algorithm computes q and $r = prem(g, f)$ as defined above:

Input: Two polynomials f and g
Output: $r = prem(g, f)$
Method:
    $r = g$
    $q = 0$
    $m = deg_{x_c}(r) - deg_{x_c}(f)$
    while($r \neq 0$ and $m \geq 0$)
        $q = ini(f) \cdot q + ini(r) \cdot x_c^m$
        $r = ini(f) \cdot r - ini(r) \cdot f \cdot x_c^m$

Algorithm: prem(g , f)

- Let $F = \{f_1, f_2, \ldots, f_s\}$ be a finite set of polynomials over the polynomial ring $K[x_1, \ldots, x_n]$.

- F is called a *triangular form* if either $s = 1$ and $f_1 \neq 0$, or $s > 1$ and $lvar(f_1) < lvar(f_2) < \cdots < lvar(f_s)$.

- A triangular form, F, with $s > 1$ is said to be a *non-contradictory ascending set* if f_j is reduced with respect to f_i for each pair $j > i$.

- Let g be any non-zero polynomial and F be a non-contradictory ascending set. We can generalize the pseudo-division mentioned above and pseudo-divide g successively by $f_s, \ldots, f_1$, considered as polynomials in their leading variables. The final remainder R is called the *pseudo-remainder* of g with respect to F.
  So, if $I_i = ini(f_i)$, we obtain the following expression:

  $$I_1^{t_1} \cdots I_s^{t_s} \cdot g = q_1 \cdot f_1 + \cdots + q_s \cdot f_s + R$$

  where q_i are all polynomials. The following algorithm computes $R = PseudoRemainder(g, A)$ as defined above:

Input: A polynomial g and an ascending set A
Output: $R = PseudoRemainder(g, A)$
Method:
```
    R = g
    n = number of polynomials in A
    for( i = n ; i ≥ 1 ; i − −)
        f = the ith polynomial in A
        R = prem(R, f)
```

Algorithm: PseudoRemainder(g , A)

- Let F be a non-contradictory ascending set. Let P be any other given set of polynomials over $K[x_1, \ldots, x_n]$.

  1. The set of all non-zero pseudo-remainders of polynomials in P with respect to F is called the *remainder set of P with respect to F*.
  2. The set of all common zeros of polynomials in P is denoted by $Zero(P)$.
  3. If h is any other non-zero polynomial, we write $Zero(P/h)$ for $Zero(P) - Zero(h)$.

- The minimal ascending set of all ascending sets contained in a polynomial set F with respect to their ranks is called a *basic set* of F. Basic set is computed via the following algorithm:

Input: A set of polynomials F
Output: The basic set B of F as defined above *Method:*
$Q = F$
$B = \phi$
Repeat
$f =$ a polynomial of Q with lowest rank
$B = B \cup \{f\}$
If $cls(f) = 0$ then
$Q = \phi$
else
$Q = \{g \in Q | g \neq f$ and g is reduced wrt $f\}$
Until $Q = \phi$

Algorithm: BasicSet(F)

- An ascending set *CS* is said to be a *Characteristic Set* of a set of polynomials F if *CS* is a subset of the ideal generated by F and the remainder set of F with respect to *CS* is empty.

- **Well Ordering Principle**: Given a finite, non-empty set F of non-zero polynomials, there is an algorithm that computes the characteristic set *CS* of F which is of the form

$$\text{CS} \quad \begin{array}{l} C_1(x_1, \ldots, x_{p_1}), \\ C_2(x_1, \ldots, x_{p_1}, \ldots, x_{p_2}), \\ \vdots \qquad\qquad\qquad \vdots \\ C_r(x_1, \ldots, x_{p_1}, \ldots, x_{p_2}, \ldots, x_{p_r}); \end{array}$$

with $I_i = ini(C_i)$ such that

$$Zero(CS/J) \subset Zero(F) \subset Zero(CS)$$
$$Zero(F) = Zero(CS/J) \bigcup (\bigcup_{i=1}^{r} Zero(F_i)),$$

where $J = I_1 \ldots I_r$ and $F_i = F \bigcup \{I_i\}$.

Input: A set of polynomials F
Output: The characteristic set B of F as defined above *Method:*
    $Q = F$
    $R = F$
    While $R \neq \phi$ do
      $C = BasicSet(Q)$
      If C is contradictory then
      If $cls(f) = 0$ then
        $R = \phi$
      else
        $R = PseudoRemainder(Q \backslash C, C) \backslash \{0\}$
        $Q = Q \cup R$

Algorithm: CharSet(F)

- Given a finite, non-empty set F of non-zero polynomials, and a sequence of ascending sets $CS_1, \ldots, CS_r$ such that

$$Zero(F) = \bigcup_{i=1}^{r} Zero(CS_i/J_i),$$

where each J_i is the product of initials of the polynomials in CS_i, then $\{CS_1, \ldots, CS_r\}$ is called a *characteristic series* of F.

- **Zero Decomposition Theorem**: Given a finite, non-empty set F of non-zero polynomials, there is an algorithm that computes a characteristic series of F.

Input: A set of polynomials F
Output: A characteristic series Ψ of F as defined above *Method:*

```
Φ = {F}
Ψ = φ
While Φ ≠ φ do
  Q = an element of Φ
  Φ = Φ\{Q}
  C = CharSet(Q)
  If C is non-contradictory then
    Φ = Φ ∪ {Q ∪ {I}|I = ini(P), P ∈ C, cls(I) > 0}
```

Algorithm: CharSer(F)

- If all polynomials in the ascending sets $CS_1, \ldots, CS_r$ are irreducible, then the characteristic series of F is called *quasi-irreducible.*