1-5 One variable polynomial

Division algorithm, GCD

Division algorithm for polynomial of $k[x]$.

Definition 0.1. For non-zero $f \in k[x]$, set

$$f = a_0x^m + a_1x^{m-1} + \cdots + a_m, \tag{1}$$

here, $a_i \in k$ and $a_0 \neq 0$ ($m = \deg(f)$). a_0x^m is the leading term of f and write as $\mathrm{LT}(f) = a_0x^m$.

$$\deg(f) \leq deg(g) \equiv \mathrm{LT}(g) \,\text{can be divided by}\, \mathrm{LT}(f). \tag{2}$$

Proposition 0.1. *k is field, $g \in k[x]$ is non-zero polynomial. Then, any $f \in k[x]$ is described as*

$$f = qg + r, \tag{3}$$

here, $q, r \in k[x]$ and $r = 0$ or $\deg(r) < \deg(g)$. q, r is uniquely determined. There exists the algolithm to obtain q and r.

Algorithm

Input: g, f

Output: q, r

$q := 0, r := f$

WHILE $r \neq 0$ AND $\mathrm{LT}(g)$ divides $\mathrm{LT}(r)$ DO

  $q := q + \mathrm{LT}(r)/\mathrm{LT}(g)$

  $r := r - (\mathrm{LT}(r)/\mathrm{LT}(g))g$

Corollary. *If k is field and $f \in k[x]$ is non-zero polynomial, f has at most* $\deg(f)$ *roots in k.*

Proof, see textbook.

Corollary. *For the field k, any ideal of $k[x]$ is represented as the form of $< f >$ by $f \in k[x]$ and f is determined uniquely up to non-zero multiplicative.*

Proof, see textbook.

Principal ideal, Principal ideal domain.

Definition 0.2. The greatest common divisor of polynomial $f, g \in k[x]$ is the polynomial h which satisfies the following conditions.
(i) h divides f, g.
(ii) If p is another polynomial which divides f, g, p divides h.
For h with these properties, we write $h = \mathrm{GCD}(f, g)$.

Corollary. *For $f, g \in k[x]$, followings hold*
(i) $\mathrm{GCD}(f, g)$ *exists and is unique up to multiplicative non-zero k.*
(ii) $\mathrm{GCD}(f, g)$ *is the generator of the ideal $< f, g >$.*
(iii) There exists the algorithm to obtain $\mathrm{GCD}(f, g)$*.*

Proof, see textbook.

Euclidean algorithm

Input: f, g

Output: h

$h := f$

$s := g$

WHILE $s \neq 0$ DO

  $rem :=$ remainder(h, s)

  $h := s$

  $s := rem$

Definition 0.3. multi-polynomials

Corollary. *multi-polynomials*

Ideal membership problem, see textbook.