

$K[x]$ 中, 若 $c(x) \mid f(x)$, 且 $c(x) \mid g(x)$, 则称 $c(x)$ 为 $f(x)$ 与 $g(x)$ 的一个公因式
定义1, 设 $f(x), g(x) \in K[x]$, 若 $\exists d(x) \in K[x]$ 满足:

1° $d(x) \mid g(x), d(x) \mid f(x)$

2° $f(x)$ 与 $g(x)$ 任一公因式 $c(x) \mid d(x)$

则称 $d(x)$ 为 $f(x)$ 与 $g(x)$ 的一个最大公因式

$\forall f(x) \in K[x] \because f(x) \mid f(x)$, 且 $f(x) \mid 0$, $f(x)$ 的任一因式 $c(x) \mid f(x)$

$\therefore f(x)$ 为 $f(x)$ 与 0 的最大公因式,

特别地: 0 与 0 的最大公因式为 0

引理1. 设 $f(x), g(x) \in K[x]$, 且 $g(x) \neq 0$, 若 $f(x) = g(x)h(x) + r(x)$

则 $c(x) \mid f(x), c(x) \mid g(x) \iff c(x) \mid g(x), c(x) \mid r(x)$

$d(x)$ 为 $f(x), g(x)$ 最大公因式 $\iff d(x)$ 为 $r(x), g(x)$ 最大公因式

设 $f(x), g(x) \in K[x]$, 且 $g(x) \neq 0$, 作带余除法,

$f(x) = h_1 g(x) + r_1(x), \deg r_1(x) < \deg g(x)$

若 $r_1(x) \neq 0$, 则 $g(x) = h_2(x) r_1(x) + r_2(x), \deg r_2 < \deg r_1$

若 $r_2(x) \neq 0$, 则 $r_1(x) = h_3(x) r_2(x) + r_3(x), \deg r_3 < \deg r_2$

\vdots

\vdots

\vdots

若 $r_{s-1}(x) \neq 0$, 则 $r_{s-2}(x) = h_s(x) r_{s-1}(x) + r_s(x), \deg r_s < \deg r_{s-1}$

若 $r_s(x) \neq 0$, 则 $r_{s-1}(x) = h_{s+1}(x) r_s(x) + r_{s+1}(x), \deg r_{s+1} < \deg r_s$

$\therefore \deg g(x)$ 有限, \therefore 至多 $n = \deg g(x)$ 次后, 可使 $r_{s+1}(x) = 0$

即 $r_{s-1}(x) = h_{s+1}(x) r_s(x) + 0$

$\therefore r_s(x)$ 为 $r_s(x)$ 与 0 的一个最大公因式.

辗转相除法

$r_s(x)$ 为 $r_{s-1}(x)$ 与 $r_s(x)$ 的一个最大公因式

\vdots

$r_s(x)$ 为 $f(x)$ 与 $g(x)$ 的一个最大公因式

又 $r_1(x)$ 可由 $f(x), g(x)$ 表示, $r_2(x)$ 可由 $g(x), r_1(x)$ 表示, \dots , $r_s(x)$ 可由 $r_{s-1}(x), r_{s-2}(x)$ 表示

$\therefore r_s(x)$ 可由 $f(x), g(x)$ 表示, 即 $r_s(x) = u_1 f(x) + u_2 g(x)$

定理 1. $K[x]$ 中任一对多项式 $f(x), g(x)$ 有最大公因式 $d(x)$, 且

$$\exists u_1(x), u_2(x) \in K[x], \text{ s.t. } d(x) = u_1(x)f(x) + u_2(x)g(x)$$

易知任 $f(x), g(x)$ 最大公因式 $d_1(x) \sim d_2(x)$

当 $f(x), g(x)$ 不全为零多项式时, 其最大公因式 $d(x)$ 为非零多项式且有多解. 记 $(f(x), g(x))$ 为其首项系数为 1 的最大公因式.

命题 1. 设 $f(x), g(x) \in K[x]$, 且 $g(x) \neq 0$. 数域 $E \supset K$, 则

$f(x)$ 与 $g(x)$ 在 $K[x]$ 中首-最大公因式, 与 $f(x)$ 与 $g(x)$ 在 $E[x]$ 中首-最大公因式相同. 即首-最大公因式不随数域扩大改变

定义 2. 若 $(f(x), g(x)) = 1$, 称 $f(x)$ 与 $g(x)$ 互素

推论. $(f(x), g(x)) = 1 \iff \forall c(x) \in K[x], c(x) | f(x), c(x) | g(x), c(x)$ 为零次多项式

定理 2. 在 $K[x]$ 中, $(f(x), g(x)) = 1 \iff$

$$\exists u_1(x), u_2(x) \in K[x], \text{ s.t. } u_1(x)f(x) + u_2(x)g(x) = 1$$

证: \Leftarrow 设 $c(x) \in K[x], c(x) | f(x), c(x) | g(x)$.

则 $c(x) | 1$, 即 $c(x)$ 为零次多项式

命题 2. 设 $f(x), g(x) \in K[x]$, 且 $g(x) \neq 0$, 数域 $E \supseteq K$,

则 $f(x)$ 在 $g(x)$ 互素 $\iff f(x)$ 与 $g(x)$ 在 $E[x]$ 互素

即数域的扩大不改变互素性

性质 1. 在 $K[x]$ 中, 若 $f(x) | g(x)h(x)$, 且 $(f(x), g(x)) = 1$, 则 $f(x) | h(x)$

证: $u(x)f(x) + v(x)g(x) = 1$

若 $h(x) \neq 0$, 则 $u(x)f(x)h(x) + v(x)g(x)h(x) = h(x)$

即 $f(x) | h(x)$

若 $h(x) = 0$, 则 $f(x) | 0$.

性质 2. 在 $K[x]$ 中, 若 $f(x) | h(x)$, $g(x) | h(x)$, $(f(x), g(x)) = 1$, 则 $f(x)g(x) | h(x)$

证: $u(x)f(x) + v(x)g(x) = 1$,

若 $h(x) \neq 0$, $h(x) = k_1(x)f(x) = k_2(x)g(x)$. ($k_1(x), k_2(x) \neq 0$)

$u(x)f(x)g(x)k_2(x) + v(x)g(x)f(x)k_1(x) = h(x)$

$\therefore f(x)g(x) | h(x)$

性质 3. 在 $K[x]$ 中, 若 $(f(x), h(x)) = 1$, 且 $(g(x), h(x)) = 1$, 则 $(f(x)g(x), h(x)) = 1$

证: $u_1(x)f(x) + v_1(x)h(x) = 1$

$u_2(x)g(x) + v_2(x)h(x) = 1$

$u_1(x)f(x)u_2(x)g(x) + (v_2(x)u_1(x)f(x) + v_1(x)u_2(x)g(x) + v_1(x)v_2(x)h(x))h(x) = 1$

\downarrow 推广为, 在 $K[x]$ 中, 若 $(f_i(x), h(x)) = 1, i = 1, \dots, n$, 则 $(f_1(x) \cdots f_n(x), h(x)) = 1$