## §5.3 最大公因式

**思考** 在 $F[x]$ 中, 设 $f(x)$ 是首一多项式. 写出 $(2,4), (1, f(x)), (0, f(x)), (f(x), f(x))$ 和 $(f(x), f(x)g(x))$.

**解** $(2,4)=1, (1, f(x))=1, (0, f(x))=f(x), (f(x), f(x))=f(x), (f(x), f(x)g(x))=f(x)$.

**思考** 设 $f(x), g(x) \in F[x]$, 若存在 $u(x), v(x) \in F[x]$, 使得 $d(x)=u(x)f(x)+v(x)g(x)$. 问 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的最大公因式吗？

**解** $d(x)$ 未必是 $f(x)$ 与 $g(x)$ 的最大公因式. 例如， $d(x)=x+1$, $f(x)=x$, $g(x)=u(x)=v(x)=1$. 这时 $d(x)=u(x)f(x)+v(x)g(x)$, 但 $d(x)$ 不是 $f(x)$ 与 $g(x)$ 的公因式.

**思考** 若 $f(x), g(x), h(x)$ 两两互素，问是否 $(f(x), g(x), h(x))=1$? 反之，若 $(f(x), g(x), h(x))=1$, 问 $f(x), g(x), h(x)$ 是否两两互素？

**解** 若 $f(x), g(x), h(x)$ 两两互素, 则 $(f(x), g(x), h(x))=1$. 事实上, 设 $(f(x), g(x), h(x))=d(x)$, 则 $d(x)|f(x)$ 且 $d(x)|g(x)$, 所以 $d(x)|(f(x), g(x))$, 即 $d(x)=1$.

反之，若 $(f(x), g(x), h(x))=1$, 则 $f(x), g(x), h(x)$ 未必两两互素. 例如, $f(x)=g(x)=x$, $h(x)=1$. 这时 $(f(x), g(x), h(x))=1$, 但 $(f(x), g(x))=x$.

**思考** 最大公因式和互素与数域的扩大相关否？即，设 $F, K$ 是两数域，且 $F \subseteq K$, $f(x), g(x) \in F[x]$. 在 $F[x]$ 上 $(f(x), g(x))=d(x)$, 那么 $K[x]$ 上是否 $(f(x), g(x))=d(x)$? 反之，在 $K[x]$ 上 $(f(x), g(x))=d(x)$, 那么在 $F[x]$ 上是否 $(f(x), g(x))=d(x)$?

**解** 最大公因式和互素与数域的扩大无关. 事实上, 最大公因式只与整除有关, 而整除与数域的扩大无关.

### 习题

1. 对于给定的 $f(x)$, $g(x)$, 求 $(f(x), g(x))$, 并求 $u(x), v(x)$, 使得 $u(x)f(x)+v(x)g(x)=(f(x), g(x))$.

(1) $f(x)=x^4-2x^3+4x^2-x+1$, $g(x)=x^2-x+1$;

(2) $f(x)=x^4-x^3-4x^2+4x+1$, $g(x)=x^2-x-1$.

**解** (1)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | $x^4$ | $-2x^3$ | $+4x^2$ | $-x$ | $+1$ | $x^2$ | $-x$ | $+1$ | |
| $q_1=x^2-x+2$ | $x^4$ | $-x^3$ | $+x^2$ | | | $x^2$ | $-\frac{1}{2}x$ | | $q_2=\frac{1}{2}x-\frac{1}{4}$ |
| | | | $2x^2$ | $-2x$ | $+2$ | | | | |
| $q_3=\frac{8}{3}x-\frac{4}{3}$ | | | | | | | | | |
| | | | | $r_3=$ | $0$ | | | | |

因此 $(f(x),g(x))=\frac{4}{3}r_2=\frac{4}{3}(f(x)(-q_2(x))+g(x)(1+q_1(x)q_2(x)))$, 故 $u(x)=-\frac{2}{3}x+\frac{1}{3}$, $v(x)=\frac{2}{3}x^3-x^2+\frac{5}{3}x+\frac{2}{3}$.

(2) (过程略) $(f(x),g(x))=1$, $u(x)=-x-1$, $v(x)=x^3+x^2-3x-3$.

2. 设 $d(x)=u(x)f(x)+v(x)g(x)$, 其中 $d(x)$ 首一，且 $d(x)|f(x)$, $d(x)|g(x)$, 则 $d(x)=(f(x),g(x))$.

**证明** 设 $h(x)|f(x)$, $h(x)|g(x)$, 根据 §2.2 性质 4, 知 $h(x)|(u(x)f(x)+v(x)g(x))$, 即 $h(x)|d(x)$. 由定义， $d(x)=(f(x),g(x))$.

3. 设 $(f(x),g(x))=1$ ，则 $(f(x^m),g(x^m))=1$.

**证明** 因为 $f(x)$ 与 $g(x)$ 互素，存在多项式 $u(x),v(x)$, 使

$$f(x)u(x)+g(x)v(x)=1.$$

故

$$f(x^m)u(x^m)+g(x^m)v(x^m)=1.$$

即知 $f(x^m)$ 与 $g(x^m)$ 互素.

4. 设 $f(x), g(x)$ 不全为零，且 $(f(x), g(x)) = d(x), f(x) = f_1(x)d(x), g(x) = g_1(x)d(x)$, 则 $(f_1(x), g_1(x)) = 1$.

**证明** 因为 $(f(x), g(x)) = d(x)$, 故存在多项式 $u(x), v(x)$, 使 $f(x)u(x)+g(x)v(x) = d(x)$. 而 $f(x) = f_1(x)d(x)$, $g(x) = g_1(x)d(x)$ 代入上式，得 $d(x)f_1(x)u(x) + d(x)g_1(x)v(x) = d(x)$. 又因为 $f(x), g(x)$ 不全为零，因此 $d(x) \neq 0$, 由消去律即得 $f_1(x)u(x) + g_1(x)v(x) = 1$, 从而 $(f_1(x), g_1(x)) = 1$.

5. 设 $(f(x), g(x)) = d(x)$, $h(x)$ 为首一多项式，则 $(f(x)h(x), g(x)h(x)) = d(x)h(x)$.

**证明** 因为 $(f(x), g(x)) = d(x)$, 存在 $u(x), v(x)$, 使得 $f(x)u(x) + g(x)v(x) = d(x)$, 则 $h(x)f(x)u(x)+h(x)g(x)v(x) = d(x)h(x)$. 因此,若 $t(x)|f(x)h(x), t(x)|g(x)h(x)$, 则必有 $t(x)|d(x)h(x)$. 又 $d(x)h(x)$ 是 $f(x)h(x), g(x)h(x)$ 的公因式，因此 $d(x)h(x)$ 是 $f(x)h(x)$ 与 $g(x)h(x)$ 的最大公因式.

6. 设 $(f(x), g(x)) = 1$. 求证： $(f(x)g(x), f(x) + g(x)) = 1$.

**证明** (法一) 由 $(f(x), g(x)) = 1$ 可知存在 $u(x), v(x)$ 使得 $f(x)u(x)+g(x)v(x) = 1$. 简单计算得 $f(x)(u(x)-v(x))+(f(x)+g(x))v(x) = 1$. 于是 $(f(x), f(x)+g(x)) = 1$. 同理 $(g(x), f(x) + g(x)) = 1$. 再由推论 5.3.3 即得 $(f(x)g(x), f(x) + g(x)) = 1$.

(法二) 由 $(f(x), g(x)) = 1$ 可知存在 $u(x), v(x)$ 使得 $f(x)u(x)+g(x)v(x) = 1$, 从而 $(f(x)u(x)+g(x)v(x))^2 = 1$, 即 $f^2(x)u^2(x)+g^2(x)v^2(x)+2f(x)g(x)u(x)v(x) = 1$, 整理得 $f(x)g(x)(2-u^2(x)-v^2(x)) + (f(x)+g(x))(f(x)u^2(x)+g(x)v^2(x)) = 1$, 故 $(f(x)g(x), f(x) + g(x)) = 1$.

(法三) 因为 $(f(x), g(x)) = 1$, 根据引理 5.3.1 知 $(f(x), f(x) + g(x)) = 1$, $(g(x), f(x) + g(x)) = 1$. 再由推论 5.3.3 知 $(f(x)g(x), f(x) + g(x)) = 1$.

7. 设 $f_1(x), f_2(x), \cdots, f_m(x) \in F[x]$. 求证：存在 $u_1(x), u_2(x), \cdots, u_m(x)$, 使得

$$(f_1(x), f_2(x), \cdots, f_m(x)) = u_1(x)f_1(x) + u_2(x)f_2(x) + \cdots + u_m(x)f_m(x).$$

**证明** 首先，用数学归纳法可以证明如下引理：

$$(f_1(x), f_2(x), \cdots, f_{m-1}(x), f_m(x)) = ((f_1(x), f_2(x), \cdots, f_{m-1}(x)), f_m(x)).$$

事实上,当 $m=3$ 时,就是命题 5.3.1. 假设命题对 $m-1$ 时成立. 为证明引理对 $m$ 也成立,设 $(f_1(x), f_2(x), \cdots, f_{m-1}(x), f_m(x)) = d(x)$. 要证 $((f_1(x), f_2(x), \cdots, f_{m-1}(x)), f_m(x)) = d(x)$. 首先,因为 $d(x)|f_i(x), i=1,2,\cdots,m-1,m$, 所以 $d_(x)|(f_1(x), f_2(x), \cdots, f_{m-1}(x))$ 且 $d_(x)|f_m(x)$. 其次,设 $h(x)|(f_1(x), f_2(x), \cdots, f_{m-1}(x))$ 且 $h_(x)|f_m(x)$, 则 $h(x)|f_i(x)$, $i=1,2,\cdots,m-1,m$. 所以 $h(x)|d(x)$. 由定义,知 $((f_1(x), f_2(x), \cdots, f_{m-1}(x)), f_m(x)) = d(x)$.

下面证明习题的结论. 对 $m$ 做数学归纳法. 当 $m=1$ 时,就是定理 5.3.1. 假设命题对于 $m-1$ 成立, 即对于 $f_1(x), f_2(x), \cdots, f_{m-1}(x)$, 存在 $v_1(x), v_2(x), \cdots, v_{m-1}(x)$, 使得

$$(f_1(x), f_2(x), \cdots, f_{m-1}(x)) = v_1(x)f_1(x) + v_2(x)f_2(x) + \cdots + v_{m-1}(x)f_{m-1}(x).$$

由引理, $(f_1(x), f_2(x), \cdots, f_{m-1}(x), f_m(x)) = ((f_1(x), f_2(x), \cdots, f_{m-1}(x)), f_m(x)) = (v_1(x)f_1(x) + v_2(x)f_2(x) + \cdots + v_{m-1}(x)f_{m-1}(x), f_m(x))$. 根据定理 5.3.1, 存在 $v_m(x), u_m(x)$, 使得

$$\begin{aligned} & v_m(x)(v_1(x)f_1(x) + v_2(x)f_2(x) + \cdots + v_{m-1}(x)f_{m-1}(x)) + u_m(x)f_m(x) \\ & \qquad = ((f_1(x), f_2(x), \cdots, f_{m-1}(x)), f_m(x)). \end{aligned}$$

令 $u_i(x) = v_m(x)v_i(x)$, $i=1,2,\cdots,m-1$, 则有

$$(f_1(x), f_2(x), \cdots, f_m(x)) = u_1(x)f_1(x) + u_2(x)f_2(x) + \cdots + u_m(x)f_m(x).$$