

## \$1.3 最大公因式和辗转相除法

高等代数 <https://gdfzu.club>

# 提纲

① 最大公因式

② 互素

③ 最小公倍式

④ 孙子定理 \*

# 最大公因式

## 定义 1.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 若  $d(x) \in \mathbb{F}[x]$  使得

则称  $d(x)$  是  $f(x)$  与  $g(x)$  的**最大公因式**。

# 最大公因式

## 定义 1.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 若  $d(x) \in \mathbb{F}[x]$  使得

- ①  $d(x) | f(x)$  且  $d(x) | g(x)$ ;

则称  $d(x)$  是  $f(x)$  与  $g(x)$  的**最大公因式**。

# 最大公因式

## 定义 1.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 若  $d(x) \in \mathbb{F}[x]$  使得

- ①  $d(x)|f(x)$  且  $d(x)|g(x)$ ;
- ② 若  $h(x)|f(x)$  且  $h(x)|g(x)$ , 则  $h(x)|d(x)$ ;

则称  $d(x)$  是  $f(x)$  与  $g(x)$  的**最大公因式**。

# 最大公因式

## 定义 1.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 若  $d(x) \in \mathbb{F}[x]$  使得

- ①  $d(x) | f(x)$  且  $d(x) | g(x)$ ;
- ② 若  $h(x) | f(x)$  且  $h(x) | g(x)$ , 则  $h(x) | d(x)$ ;

则称  $d(x)$  是  $f(x)$  与  $g(x)$  的**最大公因式**。

- $d(x)$  是  $f(x)$ 、 $g(x)$  的**次数最高**的公因式。

# 例子

## 例 1

求  $(x-1)^3(x+2)x$  与  $(x-1)^2(x+2)^5(x+3)$  的最大公因式。

# 例子

## 例 1

求  $(x-1)^3(x+2)x$  与  $(x-1)^2(x+2)^5(x+3)$  的最大公因式。

## 例 2

$\forall 0 \neq c \in \mathbb{F}$ , 求  $f(x)$  与  $c$  的最大公因式。

# 例子

## 例 1

求  $(x-1)^3(x+2)x$  与  $(x-1)^2(x+2)^5(x+3)$  的最大公因式。

## 例 2

$\forall 0 \neq c \in \mathbb{F}$ , 求  $f(x)$  与  $c$  的最大公因式。

## 例 3

求  $f(x)$  与  $0$  的最大公因式。

# 最大公因式

- 最大公因式不是唯一的。

# 最大公因式

- 最大公因式不是唯一的。
- $f(x)$  和  $g(x)$  的最大公因式最多差一个非零常数（在相伴意义下是唯一的）。

# 最大公因式

- 最大公因式不是唯一的。
- $f(x)$  和  $g(x)$  的最大公因式最多差一个非零常数（在相伴意义下是唯一的）。
- $f(x), g(x)$  首项系数为 1 (简称首一) 的最大公因式是唯一确定的, 记为  $d(x) = g.c.f(f(x), g(x))$ ,

# 最大公因式

- 最大公因式不是唯一的。
- $f(x)$  和  $g(x)$  的最大公因式最多差一个非零常数（在相伴意义下是唯一的）。
- $f(x), g(x)$  首项系数为 1 (简称首一) 的最大公因式是唯一确定的，记为  $d(x) = g.c.f(f(x), g(x))$ ，或简记为  $d(x) = (f(x), g(x))$ 。

# 例子

## 例 4

# 例子

## 例 4

①  $(f(x), 2);$

# 例子

## 例 4

- ①  $(f(x), 2)$ ;
- ②  $(f(x), 0)$ , 其中  $f(x) \neq 0$ ;

# 例子

## 例 4

- ①  $(f(x), 2)$ ;
- ②  $(f(x), 0)$ , 其中  $f(x) \neq 0$ ;
- ③  $(2, 6)$ ;

# 例子

## 例 4

- ①  $(f(x), 2)$ ;
- ②  $(f(x), 0)$ , 其中  $f(x) \neq 0$ ;
- ③  $(2, 6)$ ;
- ④  $(x^4 + x^3 - 3x^2 - 4x - 1, x^3 + x^2 - x - 1)$ 。

# 最大公因式的存在性

## 引理 1.1

设  $f(x), g(x) \in \mathbb{F}[x]$ 。

# 最大公因式的存在性

## 引理 1.1

设  $f(x), g(x) \in \mathbb{F}[x]$ 。

- ① 若  $g(x) \mid f(x)$ , 则  $(f(x), g(x)) = cg(x)$ ;

# 最大公因式的存在性

## 引理 1.1

设  $f(x), g(x) \in \mathbb{F}[x]$ 。

- ① 若  $g(x)|f(x)$ , 则  $(f(x), g(x)) = cg(x)$ ;
- ② 对任意  $l(x) \in \mathbb{F}[x]$ , 成立

$$(f(x), g(x)) = (f(x) + l(x)g(x), g(x))$$

# 最大公因式的存在性

## 引理 1.1

设  $f(x), g(x) \in \mathbb{F}[x]$ 。

- ① 若  $g(x)|f(x)$ , 则  $(f(x), g(x)) = cg(x)$ ;
- ② 对任意  $l(x) \in \mathbb{F}[x]$ , 成立

$$(f(x), g(x)) = (f(x) + l(x)g(x), g(x))$$

- 若  $f(x) = g(x)q(x) + r(x)$ , 则  $(f(x), g(x)) = (g(x), r(x))$ 。

# 最大公因式的存在性

## 引理 1.1

设  $f(x), g(x) \in \mathbb{F}[x]$ 。

- ① 若  $g(x)|f(x)$ , 则  $(f(x), g(x)) = cg(x)$ ;
- ② 对任意  $l(x) \in \mathbb{F}[x]$ , 成立

$$(f(x), g(x)) = (f(x) + l(x)g(x), g(x))$$

- 若  $f(x) = g(x)q(x) + r(x)$ , 则  $(f(x), g(x)) = (g(x), r(x))$ 。

## 定理 1.1 (裴蜀定理)

设  $f(x), g(x) \in \mathbb{F}[x]$ , 则存在  $d(x) \in \mathbb{F}[x]$ , 使得  $(f(x), g(x)) = d(x)$ , 且存在  $u(x), v(x) \in \mathbb{F}[x]$ , 使

$$d(x) = f(x)u(x) + g(x)v(x)$$

# 说明

- **注：** 证明方法即是计算方法，最大公因式相伴于 Euclidean 辗转相除中最后一个非零的余式。

# 说明

- **注：** 证明方法即是计算方法，最大公因式相伴于 Euclidean 辗转相除中最后一个非零的余式。
- **思考：** 定理中的  $u(x), v(x)$  唯一么？

# 说明

- **注：** 证明方法即是计算方法，最大公因式相伴于 Euclidean 辗转相除中最后一个非零的余式。
- **思考：** 定理中的  $u(x), v(x)$  唯一么？
- **思考：** 设  $f(x), g(x), d(x) \in \mathbb{F}[x]$ ，且  $d(x)$  的首项系数为 1。如果存在  $u(x), v(x) \in \mathbb{F}[x]$ ，使得

$$d(x) = f(x)u(x) + g(x)v(x)$$

问：  $d(x) = (f(x), g(x))$ ？

# 最大公因子的等价命题

## 定理 1.2

$d(x)$  是  $f(x), g(x)$  的最大公因子等价于

# 最大公因子的等价命题

## 定理 1.2

$d(x)$  是  $f(x), g(x)$  的最大公因子等价于

①  $d(x) \mid f(x), d(x) \mid g(x);$

# 最大公因子的等价命题

## 定理 1.2

$d(x)$  是  $f(x), g(x)$  的最大公因子等价于

- ①  $d(x) \mid f(x), d(x) \mid g(x)$ ;
- ②  $\exists u(x), v(x) \in \mathbb{F}[x]$ , 使得

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

# 最大公因子的等价命题

## 定理 1.2

$d(x)$  是  $f(x), g(x)$  的最大公因子等价于

- ①  $d(x) | f(x), d(x) | g(x)$ ;
- ②  $\exists u(x), v(x) \in \mathbb{F}[x]$ , 使得

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

- **思考：**最大公因式与数域扩大有关吗？

# 多个多项式的最大公因式

## 定义 1.2

对  $m$  个多项式  $f_i(x) \in \mathbb{F}[x] (i = 1, 2, \dots, m)$ , 若存在  $d(x) \in \mathbb{F}[x]$ , 使得

则称  $d(x)$  是  $f_i(x) (i = 1, 2, \dots, m)$  的**最大公因式**, 其中首一的最大公因式记为:

$$(f_1(x), f_2(x), \dots, f_m(x))$$

# 多个多项式的最大公因式

## 定义 1.2

对  $m$  个多项式  $f_i(x) \in \mathbb{F}[x] (i = 1, 2, \dots, m)$ , 若存在  $d(x) \in \mathbb{F}[x]$ , 使得

$$\textcircled{1} \quad d(x) | f_i(x) (i = 1, 2, \dots, m);$$

则称  $d(x)$  是  $f_i(x) (i = 1, 2, \dots, m)$  的**最大公因式**, 其中首一的最大公因式记为:

$$(f_1(x), f_2(x), \dots, f_m(x))$$

# 多个多项式的最大公因式

## 定义 1.2

对  $m$  个多项式  $f_i(x) \in \mathbb{F}[x] (i = 1, 2, \dots, m)$ , 若存在  $d(x) \in \mathbb{F}[x]$ , 使得

- ①  $d(x) | f_i(x) (i = 1, 2, \dots, m)$ ;
- ② 若  $h(x) | f_i(x) (i = 1, 2, \dots, m)$ , 则  $h(x) | d(x)$ ;

则称  $d(x)$  是  $f_i(x) (i = 1, 2, \dots, m)$  的**最大公因式**, 其中首一的最大公因式记为:

$$(f_1(x), f_2(x), \dots, f_m(x))$$

# 逐项求公因式

## 命题 1.1

设  $f(x), g(x), h(x) \in \mathbb{F}[x]$ , 则

$$\begin{aligned}(f(x), g(x), h(x)) &= ((f(x), g(x)), h(x)) \\ &= (f(x), (g(x), h(x)))\end{aligned}$$

# 逐项求公因式

## 命题 1.1

设  $f(x), g(x), h(x) \in \mathbb{F}[x]$ , 则

$$\begin{aligned}(f(x), g(x), h(x)) &= ((f(x), g(x)), h(x)) \\ &= (f(x), (g(x), h(x)))\end{aligned}$$

- 求多个多项式的最大公因式可先求任意两个多项式的最大公因式, 再用同样方法继续, 而不必顾及先后顺序。

# 逐项求公因式

## 命题 1.1

设  $f(x), g(x), h(x) \in \mathbb{F}[x]$ , 则

$$\begin{aligned}(f(x), g(x), h(x)) &= ((f(x), g(x)), h(x)) \\ &= (f(x), (g(x), h(x)))\end{aligned}$$

- 求多个多项式的最大公因式可先求任意两个多项式的最大公因式, 再用同样方法继续, 而不必顾及先后顺序。

## 例 5

求  $((x+1)^3, (x+1)(x+2), x+2)$ 。

# 提纲

1 最大公因式

2 互素

3 最小公倍式

4 孙子定理 \*

# 互素

## 定义 2.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 若  $(f(x), g(x)) = 1$ , 则称  $f(x)$  与  $g(x)$  **互素** 或 **互质**。

# 互素

## 定义 2.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 若  $(f(x), g(x)) = 1$ , 则称  $f(x)$  与  $g(x)$  **互素** 或 **互质**。

## 定理 2.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 则  $f(x), g(x)$  互素的充要条件是存在  $u(x), v(x) \in \mathbb{F}[x]$ , 使得

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

# 互素

## 定义 2.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 若  $(f(x), g(x)) = 1$ , 则称  $f(x)$  与  $g(x)$  **互素** 或 **互质**。

## 定理 2.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 则  $f(x), g(x)$  互素的充要条件是存在  $u(x), v(x) \in \mathbb{F}[x]$ , 使得

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

- **注** 一般的若仅有  $d(x) = f(x)u(x) + g(x)v(x)$ , 并不能保证  $d(x) = (f(x), g(x))$ 。但若  $u(x)f(x) + v(x)g(x) = 1$ , 就确保  $(f(x), g(x)) = 1$ 。

# 互素

## 定义 2.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 若  $(f(x), g(x)) = 1$ , 则称  $f(x)$  与  $g(x)$  **互素** 或 **互质**。

## 定理 2.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 则  $f(x), g(x)$  互素的充要条件是存在  $u(x), v(x) \in \mathbb{F}[x]$ , 使得

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

- **注** 一般的若仅有  $d(x) = f(x)u(x) + g(x)v(x)$ , 并不能保证  $d(x) = (f(x), g(x))$ 。但若  $u(x)f(x) + v(x)g(x) = 1$ , 就确保  $(f(x), g(x)) = 1$ 。
- **思考**: 互素与数域扩大有关吗?

# 互素

## 定义 2.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 若  $(f(x), g(x)) = 1$ , 则称  $f(x)$  与  $g(x)$  **互素** 或 **互质**。

## 定理 2.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 则  $f(x), g(x)$  互素的充要条件是存在  $u(x), v(x) \in \mathbb{F}[x]$ , 使得

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

- **注** 一般的若仅有  $d(x) = f(x)u(x) + g(x)v(x)$ , 并不能保证  $d(x) = (f(x), g(x))$ 。但若  $u(x)f(x) + v(x)g(x) = 1$ , 就确保  $(f(x), g(x)) = 1$ 。
- **思考**: 互素与数域扩大有关吗?
- **思考**: 若  $f(x), g(x), h(x)$  两两互素, 则  $(f(x), g(x), h(x)) = 1$ 。反之是否成立?

# 例子

## 例 6

设  $a, b \in \mathbb{F}$ ,  $a \neq b$ , 则

$$(x - a, x - b) = 1.$$

# 例子

## 例 6

设  $a, b \in \mathbb{F}$ ,  $a \neq b$ , 则

$$(x - a, x - b) = 1.$$

## 例 7

设  $f(x), g(x) \in \mathbb{F}[x]$ , 且  $(f(x), g(x)) = 1$ 。证明对任意自然数  $m$

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

# 推论

## 推论 2.1

设  $f_1(x)|g(x)$ ,  $f_2(x)|g(x)$ , 且  $(f_1(x), f_2(x)) = 1$ , 则  $f_1(x)f_2(x)|g(x)$ 。

# 推论

## 推论 2.1

设  $f_1(x)|g(x)$ ,  $f_2(x)|g(x)$ , 且  $(f_1(x), f_2(x)) = 1$ , 则  $f_1(x)f_2(x)|g(x)$ 。

## 推论 2.2

设  $f(x)|g(x)h(x)$ , 且  $(f(x), g(x)) = 1$ , 则

$$f(x)|h(x).$$

## 推论 2.3

设  $(f_1(x), g(x)) = 1$ ,  $(f_2(x), g(x)) = 1$ , 则

$$(f_1(x)f_2(x), g(x)) = 1.$$

## 推论 2.3

设  $(f_1(x), g(x)) = 1$ ,  $(f_2(x), g(x)) = 1$ , 则

$$(f_1(x)f_2(x), g(x)) = 1.$$

## 推论 2.4

设  $(f(x), g(x)) = d(x) \neq 0$ , 且  $f(x) = f_1(x)d(x)$ ,  $g(x) = g_1(x)d(x)$ , 则  $(f_1(x), g_1(x)) = 1$ 。

### 推论 2.3

设  $(f_1(x), g(x)) = 1$ ,  $(f_2(x), g(x)) = 1$ , 则

$$(f_1(x)f_2(x), g(x)) = 1.$$

### 推论 2.4

设  $(f(x), g(x)) = d(x) \neq 0$ , 且  $f(x) = f_1(x)d(x)$ ,  $g(x) = g_1(x)d(x)$ , 则  $(f_1(x), g_1(x)) = 1$ 。

### 推论 2.5

设  $t(x)$  是首一多项式,  $(f(x), g(x)) = d(x)$ , 则

$$(f(x)t(x), g(x)t(x)) = d(x)t(x).$$

# 提纲

① 最大公因式

② 互素

③ 最小公倍式

④ 孙子定理 \*

# 最小公倍式

## 定义 3.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 若  $m(x) \in \mathbb{F}[x]$ , 使得

则称  $m(x)$  是  $f(x)$  与  $g(x)$  的**最小公倍式**(*l.c.m.*)。首一最小公倍式记作  $[f(x), g(x)]$ 。

# 最小公倍式

## 定义 3.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 若  $m(x) \in \mathbb{F}[x]$ , 使得

①  $f(x) \mid m(x)$  且  $g(x) \mid m(x)$ ;

则称  $m(x)$  是  $f(x)$  与  $g(x)$  的**最小公倍式**(*l.c.m.*)。首一最小公倍式记作  $[f(x), g(x)]$ 。

# 最小公倍式

## 定义 3.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 若  $m(x) \in \mathbb{F}[x]$ , 使得

- ①  $f(x)|m(x)$  且  $g(x)|m(x)$ ;
- ② 若  $f(x)|l(x)$  且  $g(x)|l(x)$ , 则  $m(x)|l(x)$

则称  $m(x)$  是  $f(x)$  与  $g(x)$  的**最小公倍式**(*l.c.m.*)。首一最小公倍式记作  $[f(x), g(x)]$ 。

# 最小公倍式

## 定义 3.1

设  $f(x), g(x) \in \mathbb{F}[x]$ , 若  $m(x) \in \mathbb{F}[x]$ , 使得

- ①  $f(x)|m(x)$  且  $g(x)|m(x)$ ;
- ② 若  $f(x)|l(x)$  且  $g(x)|l(x)$ , 则  $m(x)|l(x)$

则称  $m(x)$  是  $f(x)$  与  $g(x)$  的**最小公倍式**(*l.c.m.*)。首一最小公倍式记作  $[f(x), g(x)]$ 。  $f_1(x), f_2(x), \dots, f_m(x)$  的首一最小公倍式记为

$$[f_1(x), f_2(x), \dots, f_m(x)].$$

# 提纲

- 1 最大公因式
- 2 互素
- 3 最小公倍式
- 4 孙子定理 \*

# 孙子定理/中国剩余定理

## 引理 4.1

设  $p_1(x), p_2(x), \dots, p_m(x) \in \mathbb{F}[x] (m \geq 2)$  两两互素, 则存在  $f_i(x) \in \mathbb{F}[x] (i = 1, 2, \dots, m)$ , 使得对任意  $i, j = 1, 2, \dots, m$  且  $i \neq j$ , 都有

$$f_i(x) = l_i(x)p_i(x) + 1, \quad f_i(x) = h_{ij}(x)p_j(x).$$

# 孙子定理/中国剩余定理

## 引理 4.1

设  $p_1(x), p_2(x), \dots, p_m(x) \in \mathbb{F}[x] (m \geq 2)$  两两互素, 则存在  $f_i(x) \in \mathbb{F}[x] (i = 1, 2, \dots, m)$ , 使得对任意  $i, j = 1, 2, \dots, m$  且  $i \neq j$ , 都有

$$f_i(x) = l_i(x)p_i(x) + 1, \quad f_i(x) = h_{ij}(x)p_j(x).$$

## 定理 4.1 (孙子定理/中国剩余定理)

设  $p_1(x), p_2(x), \dots, p_m(x) \in \mathbb{F}[x] (m \geq 2)$  两两互素,  $g_1(x), g_2(x), \dots, g_m(x) \in \mathbb{F}[x]$  且  $\deg g_i(x) < \deg p_i(x)$ , 则存在唯一多项式  $g(x)$ , 使得对任意  $i = 1, 2, \dots, m$ , 有

$$g(x) = p_i(x)q_i(x) + g_i(x),$$

且  $\deg g(x) < \sum_{i=1}^m \deg p_i(x)$ 。

# 例子

## 例 8

设  $f(x)$  除以  $x^2 + 1, x^2 + 2$  的余式分别为  $4x + 4, 4x + 8$ 。求  $f(x)$  以及  $f(x)$  除以  $(x^2 + 1)(x^2 + 2)$  的余式。