

§1.2 带余除法与整除

高等代数 <https://gdfzu.club>

Outline

1 带余除法

2 整除

例子

- 整数带余除法（欧几里得除法）： $a = bq + r, 0 \leq r < |b|$ 。

例子

- 整数带余除法（欧几里得除法）： $a = bq + r, 0 \leq r < |b|$ 。

例 1.1

$f(x) = 3x^4 - 4x^3 + 5x - 1$, $g(x) = x^2 - x + 1$ 。求多项式 $q(x), r(x)$, 使得

$$f(x) = q(x)g(x) + r(x)$$

且 $\deg r(x) < \deg g(x)$ 。

例子

- 整数带余除法（欧几里得除法）： $a = bq + r, 0 \leq r < |b|$ 。

例 1.1

$f(x) = 3x^4 - 4x^3 + 5x - 1, g(x) = x^2 - x + 1$ 。求多项式 $q(x), r(x)$ ，使得

$$f(x) = q(x)g(x) + r(x)$$

且 $\deg r(x) < \deg g(x)$ 。

- **思考：**多项式“带余除法”与整数带余除法的相似性。

带余除法

定理 1.1 (多项式的带余除法)

设 $f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$, 则存在**唯一** $q(x), r(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)q(x) + r(x),$$

其中 $\deg r(x) < \deg g(x)$ 。

带余除法

定理 1.1 (多项式的带余除法)

设 $f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$, 则存在**唯一** $q(x), r(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)q(x) + r(x),$$

其中 $\deg r(x) < \deg g(x)$ 。

- 此时 $q(x)$ 、 $r(x)$ 分别称为 $g(x)$ 除 $f(x)$ 或 $f(x)$ 除以 $g(x)$ 的**商式**和**余式**。

带余除法

定理 1.1 (多项式的带余除法)

设 $f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$, 则存在**唯一** $q(x), r(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)q(x) + r(x),$$

其中 $\deg r(x) < \deg g(x)$ 。

- 此时 $q(x)$ 、 $r(x)$ 分别称为 $g(x)$ 除 $f(x)$ 或 $f(x)$ 除以 $g(x)$ 的**商式**和**余式**。
- 带余除法的结果与数域扩大无关。

带余除法

定理 1.1 (多项式的带余除法)

设 $f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$, 则存在**唯一** $q(x), r(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)q(x) + r(x),$$

其中 $\deg r(x) < \deg g(x)$ 。

- 此时 $q(x)$ 、 $r(x)$ 分别称为 $g(x)$ 除 $f(x)$ 或 $f(x)$ 除以 $g(x)$ 的**商式**和**余式**。
- 带余除法的结果与数域扩大无关。
- 条件 $\deg r(x) < \deg g(x)$ 保证了唯一性。

余数定理

定理 1.2 (余数定理)

设 $f(x) \in \mathbb{F}[x]$, $b \in \mathbb{F}$, 则存在**唯一**的 $g(x) \in \mathbb{F}[x]$, 使得

$$f(x) = (x - b)g(x) + f(b).$$

余数定理

定理 1.2 (余数定理)

设 $f(x) \in \mathbb{F}[x]$, $b \in \mathbb{F}$, 则存在**唯一**的 $g(x) \in \mathbb{F}[x]$, 使得

$$f(x) = (x - b)g(x) + f(b)。$$

例 1.2

设 $f(x) = x^5 - 12x^3 + 36x + 12$, 求 $f(x)$ 除以 $x - 2$ 的余式?

Outline

1 带余除法

2 整除

整除

定义 2.1

设 $f(x), g(x) \in \mathbb{F}[x]$ 。若存在 $h(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)h(x),$$

则称 $g(x)$ 是 $f(x)$ 的因式,

整除

定义 2.1

设 $f(x), g(x) \in \mathbb{F}[x]$ 。若存在 $h(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)h(x),$$

则称 $g(x)$ 是 $f(x)$ 的因式, 或 $f(x)$ 被 $g(x)$ 整除,

整除

定义 2.1

设 $f(x), g(x) \in \mathbb{F}[x]$ 。若存在 $h(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)h(x),$$

则称 $g(x)$ 是 $f(x)$ 的因式, 或 $f(x)$ 被 $g(x)$ **整除**, 或 $g(x)$ 整除 $f(x)$,

整除

定义 2.1

设 $f(x), g(x) \in \mathbb{F}[x]$ 。若存在 $h(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)h(x),$$

则称 $g(x)$ 是 $f(x)$ 的因式, 或 $f(x)$ 被 $g(x)$ **整除**, 或 $g(x)$ 整除 $f(x)$, 记为 $g(x) | f(x)$ 。

整除

定义 2.1

设 $f(x), g(x) \in \mathbb{F}[x]$ 。若存在 $h(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)h(x),$$

则称 $g(x)$ 是 $f(x)$ 的因式, 或 $f(x)$ 被 $g(x)$ **整除**, 或 $g(x)$ 整除 $f(x)$, 记为 $g(x)|f(x)$ 。否则称 $g(x)$ 不整除 $f(x)$, 记为 $g(x) \nmid f(x)$ 。

整除

定义 2.1

设 $f(x), g(x) \in \mathbb{F}[x]$ 。若存在 $h(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)h(x),$$

则称 $g(x)$ 是 $f(x)$ 的因式, 或 $f(x)$ 被 $g(x)$ **整除**, 或 $g(x)$ 整除 $f(x)$, 记为 $g(x)|f(x)$ 。否则称 $g(x)$ 不整除 $f(x)$, 记为 $g(x) \nmid f(x)$ 。

例 1

整除

定义 2.1

设 $f(x), g(x) \in \mathbb{F}[x]$ 。若存在 $h(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)h(x),$$

则称 $g(x)$ 是 $f(x)$ 的因式, 或 $f(x)$ 被 $g(x)$ **整除**, 或 $g(x)$ 整除 $f(x)$, 记为 $g(x)|f(x)$ 。否则称 $g(x)$ 不整除 $f(x)$, 记为 $g(x) \nmid f(x)$ 。

例 1

- $2|3$?

整除

定义 2.1

设 $f(x), g(x) \in \mathbb{F}[x]$ 。若存在 $h(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)h(x),$$

则称 $g(x)$ 是 $f(x)$ 的因式, 或 $f(x)$ 被 $g(x)$ **整除**, 或 $g(x)$ 整除 $f(x)$, 记为 $g(x)|f(x)$ 。否则称 $g(x)$ 不整除 $f(x)$, 记为 $g(x) \nmid f(x)$ 。

例 1

- $2|3$?
- $f(x)|0$?

整除

定义 2.1

设 $f(x), g(x) \in \mathbb{F}[x]$ 。若存在 $h(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)h(x),$$

则称 $g(x)$ 是 $f(x)$ 的因式, 或 $f(x)$ 被 $g(x)$ **整除**, 或 $g(x)$ 整除 $f(x)$, 记为 $g(x)|f(x)$ 。否则称 $g(x)$ 不整除 $f(x)$, 记为 $g(x) \nmid f(x)$ 。

例 1

- $2|3$?
- $f(x)|0$?
- $0|f(x)$?

整除的性质

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

整除的性质

- $f(x), g(x), h(x) \in \mathbb{F}[x]$, 则
 - ① 反身性: $f(x) | f(x)$;

整除的性质

- $f(x), g(x), h(x) \in \mathbb{F}[x]$, 则
 - ① 反身性: $f(x)|f(x)$;
 - ② 传递性: $f(x)|g(x), g(x)|h(x)$, 则 $f(x)|h(x)$;

整除的性质

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

- ① 反身性: $f(x)|f(x)$;
- ② 传递性: $f(x)|g(x), g(x)|h(x)$, 则 $f(x)|h(x)$;
- ③ 互伴性: $f(x)|g(x), g(x)|f(x)$, 则存在 $0 \neq c \in \mathbb{F}$, 使得

$$f(x) = cg(x),$$

此时称 $f(x)$ 和 $g(x)$ 为**相伴多项式**, 记作 $f(x) \sim g(x)$ 。

整除的性质

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

- ① 反身性: $f(x)|f(x)$;
- ② 传递性: $f(x)|g(x), g(x)|h(x)$, 则 $f(x)|h(x)$;
- ③ 互伴性: $f(x)|g(x), g(x)|f(x)$, 则存在 $0 \neq c \in \mathbb{F}$, 使得

$$f(x) = cg(x),$$

此时称 $f(x)$ 和 $g(x)$ 为**相伴多项式**, 记作 $f(x) \sim g(x)$ 。

例 2.1

整除的性质

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

- ① 反身性: $f(x)|f(x)$;
- ② 传递性: $f(x)|g(x), g(x)|h(x)$, 则 $f(x)|h(x)$;
- ③ 互伴性: $f(x)|g(x), g(x)|f(x)$, 则存在 $0 \neq c \in \mathbb{F}$, 使得

$$f(x) = cg(x),$$

此时称 $f(x)$ 和 $g(x)$ 为**相伴多项式**, 记作 $f(x) \sim g(x)$ 。

例 2.1

- $[0]$;

整除的性质

- $f(x), g(x), h(x) \in \mathbb{F}[x]$, 则
 - ① 反身性: $f(x)|f(x)$;
 - ② 传递性: $f(x)|g(x), g(x)|h(x)$, 则 $f(x)|h(x)$;
 - ③ 互伴性: $f(x)|g(x), g(x)|f(x)$, 则存在 $0 \neq c \in \mathbb{F}$, 使得

$$f(x) = cg(x),$$

此时称 $f(x)$ 和 $g(x)$ 为**相伴多项式**, 记作 $f(x) \sim g(x)$ 。

例 2.1

- $[0]$;
- $[1]$;

整除的性质

- $f(x), g(x), h(x) \in \mathbb{F}[x]$, 则
 - ① 反身性: $f(x)|f(x)$;
 - ② 传递性: $f(x)|g(x), g(x)|h(x)$, 则 $f(x)|h(x)$;
 - ③ 互伴性: $f(x)|g(x), g(x)|f(x)$, 则存在 $0 \neq c \in \mathbb{F}$, 使得

$$f(x) = cg(x),$$

此时称 $f(x)$ 和 $g(x)$ 为**相伴多项式**, 记作 $f(x) \sim g(x)$ 。

例 2.1

- $[0]$;
- $[1]$;
- $[x^n]$;

整除的性质

- $f(x), g(x), h(x) \in \mathbb{F}[x]$, 则
 - ① 反身性: $f(x)|f(x)$;
 - ② 传递性: $f(x)|g(x), g(x)|h(x)$, 则 $f(x)|h(x)$;
 - ③ 互伴性: $f(x)|g(x), g(x)|f(x)$, 则存在 $0 \neq c \in \mathbb{F}$, 使得

$$f(x) = cg(x),$$

此时称 $f(x)$ 和 $g(x)$ 为**相伴多项式**, 记作 $f(x) \sim g(x)$ 。

例 2.1

- $[0]$;
- $[1]$;
- $[x^n]$;
- $[1 + x + \cdots + x^n]$ 。

整除的性质

命题 2.1

设 $f(x)|g(x)$, $f(x)|h(x)$, 则对任意 $u(x), v(x) \in \mathbb{F}[x]$, 有

$$f(x)|g(x)u(x) + h(x)v(x).$$

整除的性质

命题 2.1

设 $f(x)|g(x)$, $f(x)|h(x)$, 则对任意 $u(x), v(x) \in \mathbb{F}[x]$, 有

$$f(x)|g(x)u(x) + h(x)v(x).$$

特别地, 若 $f(x)|g(x)$, $f(x)|g(x)q(x) + r(x)$, 则 $f(x)|r(x)$ 。

整除的性质

命题 2.1

设 $f(x)|g(x)$, $f(x)|h(x)$, 则对任意 $u(x), v(x) \in \mathbb{F}[x]$, 有

$$f(x)|g(x)u(x) + h(x)v(x).$$

特别地, 若 $f(x)|g(x)$, $f(x)|g(x)q(x) + r(x)$, 则 $f(x)|r(x)$ 。

- 整除关系关于多项式组合封闭。

例子

例 2.2

设 $f(x)|g_1(x) - g_2(x)$, $f(x)|h_1(x) - h_2(x)$, 证明:

$$f(x)|g_1(x)h_1(x) - g_2(x)h_2(x)。$$

例子

例 2.2

设 $f(x)|g_1(x) - g_2(x)$, $f(x)|h_1(x) - h_2(x)$, 证明:

$$f(x)|g_1(x)h_1(x) - g_2(x)h_2(x)。$$

例 2.3

若 $g(x)|f(x)$, 则 $\deg g(x) \leq \deg f(x)$?

例子

例 2.2

设 $f(x)|g_1(x) - g_2(x)$, $f(x)|h_1(x) - h_2(x)$, 证明:

$$f(x)|g_1(x)h_1(x) - g_2(x)h_2(x)。$$

例 2.3

若 $g(x)|f(x)$, 则 $\deg g(x) \leq \deg f(x)$?

① $f(x) \neq 0$, $g(x)|f(x)$, 则 $\deg g(x) \leq \deg f(x)$ 。

例子

例 2.2

设 $f(x)|g_1(x) - g_2(x)$, $f(x)|h_1(x) - h_2(x)$, 证明:

$$f(x)|g_1(x)h_1(x) - g_2(x)h_2(x)。$$

例 2.3

若 $g(x)|f(x)$, 则 $\deg g(x) \leq \deg f(x)$?

- ① $f(x) \neq 0$, $g(x)|f(x)$, 则 $\deg g(x) \leq \deg f(x)$ 。
- ② $\deg g(x) > \deg f(x)$ 且 $g(x)|f(x)$, 则 $f(x) = 0$ 。

例子

例 2.2

设 $f(x)|g_1(x) - g_2(x)$, $f(x)|h_1(x) - h_2(x)$, 证明:

$$f(x)|g_1(x)h_1(x) - g_2(x)h_2(x)。$$

例 2.3

若 $g(x)|f(x)$, 则 $\deg g(x) \leq \deg f(x)$?

- ① $f(x) \neq 0$, $g(x)|f(x)$, 则 $\deg g(x) \leq \deg f(x)$ 。
- ② $\deg g(x) > \deg f(x)$ 且 $g(x)|f(x)$, 则 $f(x) = 0$ 。

例 2.4

$f(x)$ 满足什么条件时, $f(x)|1$?

推论

推论 2.1

$f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$, 则 $g(x) | f(x)$ 当且仅当 $g(x)$ 除 $f(x)$ 的余式为 0 。

推论

推论 2.1

$f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$, 则 $g(x) | f(x)$ 当且仅当 $g(x)$ 除 $f(x)$ 的余式为 0 。

推论 2.2

设 $f(x) \in \mathbb{F}[x]$, 则 $x - c | f(x)$ 当且仅当 $f(c) = 0$ 。

推论

推论 2.1

$f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$, 则 $g(x) \mid f(x)$ 当且仅当 $g(x)$ 除 $f(x)$ 的余式为 0 。

推论 2.2

设 $f(x) \in \mathbb{F}[x]$, 则 $x - c \mid f(x)$ 当且仅当 $f(c) = 0$ 。

例 2.5

证明: $x \mid f(x)$ 的充要条件是 $x^2 \mid f^2(x)$ 。

推论

推论 2.1

$f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$, 则 $g(x) | f(x)$ 当且仅当 $g(x)$ 除 $f(x)$ 的余式为 0 。

推论 2.2

设 $f(x) \in \mathbb{F}[x]$, 则 $x - c | f(x)$ 当且仅当 $f(c) = 0$ 。

例 2.5

证明: $x | f(x)$ 的充要条件是 $x^2 | f^2(x)$ 。

- **思考:** 整除关系与数域扩大有关吗?

推论

推论 2.1

$f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$, 则 $g(x)|f(x)$ 当且仅当 $g(x)$ 除 $f(x)$ 的余式为 0 。

推论 2.2

设 $f(x) \in \mathbb{F}[x]$, 则 $x - c|f(x)$ 当且仅当 $f(c) = 0$ 。

例 2.5

证明: $x|f(x)$ 的充要条件是 $x^2|f^2(x)$ 。

- **思考:** 整除关系与数域扩大有关吗? 即设 $\mathbb{F}, \mathbb{K}$ 是两个数域, 且 $\mathbb{F} \subset \mathbb{K}$, 在 $\mathbb{F}[x]$ 中 $q(x)|f(x)$ 的充分必要条件是在 $\mathbb{K}[x]$ 中 $q(x)|f(x)$?