

抽象代数笔记

副标题

Zhang Liang

2025 年 3 月 19 日

前言标题

前言内容

2025 年 3 月 19 日

目录

第一章 域	0
1.1 域的定义	0
1.1.1 域	0
1.1.2 域的性质	0
1.2 域的同态	2
1.3 域的特征	3
1.3.1 域的特征的定义	3
1.3.2 域的特征的性质	4
1.4 域的扩张	4
1.4.1 代数闭包	4
第二章 Galois 理论	5
2.1 Galois 群	5
第三章 附录	6
3.1 一些典型的域	6
3.1.1 F_p	6
3.1.2 \mathbb{Q}	7

第一章 域

1.1 域的定义

1.1.1 域

定义 1.1.1: 域

设 F 是一个集合，如果存在两个运算 $+: F \times F \rightarrow F$ 和 $\cdot: F \times F \rightarrow F$ ，分别称为加法和乘法，并且满足：

- ①（加法单位元存在）存在一个元素 $0_F \in F$ ，称为零元， $\forall x \in F, x + 0_F = 0_F + x = x$
- ②（加法逆存在） $\forall x \in F, \exists (-x) \in F, \text{s.t. } x + (-x) = (-x) + x = 0_F$ ， $(-x)$ 称为 x 的加法逆元
- ③（加法交换律） $\forall x, y \in F, x + y = y + x$
- ④（加法结合律） $\forall x, y, z \in F, (x + y) + z = x + (y + z)$
- ⑤（乘法单位元存在）存在一个元素 $1_F \in F, 1_F \neq 0_F$ ，称为一元， $\forall x \in F, x \cdot 1_F = 1_F \cdot x = x$
- ⑥（乘法逆存在） $\forall x \in F - 0_F, \exists x^{-1} \in F, \text{s.t. } x \cdot x^{-1} = x^{-1} \cdot x = 1$ ， x^{-1} 称为 x 的乘法逆元
- ⑦（乘法交换律） $\forall x, y \in F, x \cdot y = y \cdot x$
- ⑧（乘法结合律） $\forall x, y, z \in F, (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- ⑨（乘法分配律） $\forall x, y, z \in F, x \cdot (y + z) = x \cdot y + x \cdot z$

1.1.2 域的性质

1.

命题 1.1.1. 加法和乘法的单位元是唯一的。

证明: 先考虑加法的单位元。假设命题不成立, 那么我们不妨假设 $0_1, 0_2$ 都是 F 的零元, $0_1 \neq 0_2$

那么 $0_1 = 0_1 + 0_2 = 0_2$, 于是有 $0_1 = 0_2$, 与假设矛盾。于是加法的单位元唯一。

同理可证, 乘法的单位元也是唯一的。□

2.

命题 1.1.2. $\forall a$, 加法的逆 $-a$ 是唯一的。

如果还有 $a \neq 0$, 那么乘法的逆 a^{-1} 也是唯一的。

证明: 先考虑加法逆, 不妨假设命题不成立, 那么 $\exists b, c, a + b = 0, a + c = 0, b \neq c$

于是, $b = b + 0 = b + (a + c) = (a + b) + c = 0 + c = c$, 这与假设矛盾。于是加法逆唯一。

同理可证, 乘法逆也是唯一的。□

3. **证明:** $a \cdot 0 = 0$ □

证明: $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$

$\Rightarrow a \cdot 0 + (-a \cdot a) = a \cdot 0 + a \cdot 0 + (-a \cdot 0)$

$\Rightarrow 0 = a \cdot 0$ □

立即有以下推论:

推论 1.1.1

$$ab = 0 \Rightarrow a = 0 \vee b = 0$$

证明: 假设 $a \neq 0$, 那么 $b = a^{-1} \cdot 0 = 0$, 命题得证 □

4.

命题 1.1.3. $-a = (-1) \cdot a$

证明: $a + (-a) = 0 = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a$

$\Rightarrow (-a) + a + (-a) = (-a) + a + (-1) \cdot a$

$\Rightarrow -a = (-1) \cdot a$ □

随后我们即可得出以下推论

推论 1.1.2

$$(-1) \cdot (-x) = x$$

证明: 我们只需证明: $(-1)(-1) = 1$

因为 $(-1)(-1) + (-1) \cdot 1 = 0$

$\Rightarrow (-1)(-1) + (-1) = 0 \Rightarrow (-1)(-1) = 1$

那么, $(-1)(-x) = (-1)(-1) \cdot x = 1 \cdot x = x$ □

推论 1.1.3

$$(-x)(-x) = x \cdot x$$

证明: 运用前面的推论中的结果, $(-x)(-x) = x \cdot (-1)(-1) \cdot x = x \cdot 1 \cdot x = x \cdot x$ □

1.2 域的同态

定义 1.2.1: 域的同态

F_1, F_2 是两个域, 如果存在一个映射 $\varphi: F_1 \rightarrow F_2$, 满足:

- ① $\varphi(0_{F_1}) = 0_{F_2}$
- ② $\varphi(1_{F_1}) = 1_{F_2}$
- ③ $\varphi(x + y) = \varphi(x) + \varphi(y)$
- ④ $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$

值得注意的是, 与我们之前了解到的线性空间同构不同, 域的同态完全没有对映射的满射性、单射性作任何限制。但是,

以下定理证明, 两个域如果同态, 那么同态映射是一个单射

定理 1.2.1: 域同态的单射性

若 $\varphi: F_1 \rightarrow F_2$ 是 F_1 到 F_2 的同态, 那么 φ 是单射

证明: 不妨假设命题不成立。于是, $\exists x_1 \neq x_2$ s.t. $\varphi(x_1) = \varphi(x_2)$

那么有: $\varphi(x_1 - x_2) = \varphi(x_1) - \varphi(x_2) = 0_{F_2}$

因为我们已经假设了 $x_1 \neq x_2$, 于是 $(x_1 - x_2)^{-1}$ 存在。将上式乘以 $\varphi((x_1 - x_2)^{-1})$ 得:

$$1_{F_2} = \varphi(1_{F_1})\varphi((x_1 - x_2)^{-1}(x_1 - x_2)) = \varphi((x_1 - x_2)^{-1})\varphi((x_1 - x_2)) = 0_{F_1}$$

与 $0_{F_2} \neq 1_{F_2}$ 矛盾, 于是命题得证。 □

在证明这一点后, 我们可以类似地引入域的同构:

定义 1.2.2: 域的同构

设 $\varphi: F_1 \rightarrow F_2$ 是 F_1 到 F_2 的同态

如果 φ 还是个满射, 那么我们称 φ 是一个同构;

特别地, 如果有 $F_1 = F_2$, 我们称 φ 是一个自同构。

并且引入自同构的不动域的概念:

定义 1.2.3: 自同构域的不动域

设 $\sigma: F \rightarrow F$ 是 F 的自同构, 那么我们称集合

$\{x \in F | \sigma(x) = x\}$ 为 F 的不动域

“不动域”这一名称是合理的, 因为利用域同构的定义容易证明不动域是一个域, 而且是 F 的一个子域。

1.3 域的特征

1.3.1 域的特征的定义

定义 1.3.1: 域的特征

设 F 是一个域, 定义以下映射 $N: \mathbb{N} \ni n \mapsto n_F \in F$, 满足:

$$N(0) = 0_F, N(n+1) = n_F + 1_F$$

那么, 如果 N 是一个单射, 我们称 F 的特征为 0, 记作 $\text{Char}F = 0$;

否则, 我们将满足 $N(p) = 0_F, p > 0$ 的最小正整数称为 F 的特征, 记作 $\text{Char}F = p$ 。

我们首先需要证明的是, 任何一个域都是具有特征的, 因为对于定义中的第二种情形, 我们并不知道这样的 p 是否一定存在。

定理 1.3.1: 域特征的存在性

任何域 F 的特征 $\text{Char}F$ 均存在

证明: 我们只需要证明第二种情形。

容易证明, $N(m+n) = N(m) + N(n)$ 。(仿照 Peano 公理下证明加法性质的方式即可)

于是, 因为 N 不是单射, 于是一定有 $a, b \in \mathbb{N}, a > b, N(a) = N(b)$

于是有 $N(a - b) = N(a) - N(b) = 0_F$ 。

那么 $\{m | N(m) = 0_F\} \neq \emptyset$, 因此这样的最小整数 $\text{Char} F$ 存在

□

接下来考虑几个性质

1.3.2 域的特征的性质

命题 1.3.1. 设 F 是一个域, 那么或者 $\text{Char} F = 0$, 或者 $\text{Char} F = p$ 是素数

证明: 我们只需要证明当 $\text{Char} F = p > 0$ 时, p 是素数

不妨假设命题不成立, 那么一定有 $1 < q < p, 1 < r < p, p = qr$

容易证明, $N(qr) = N(q)N(r)$ 。(仿照 Peano 公理下证明乘法性质的方式即可)

但是, 因为 $N(qr) = 0$, 于是 $N(q) = 0 \vee N(r) = 0$, 这与定义中 p 是使 $N(x) = 0$ 成立的最小正整数矛盾。

于是命题得证。

□

1.4 域的扩张

定义 1.4.1: 子域

设 E, F 是两个域, $E \subseteq F$

如果 $0_F, 1_F \in E$, 并且 F 中的加法和乘法对 E 形成一个域,

那么我们称 E 是 F 的一个子域, 并称 F 是 E 的一个域扩张,

记作 $F \setminus E$

从以上定义容易看出, F 也可以视为 E 上的一个线性空间。

定义 1.4.2: 域的 n 次扩张

如果 $F \setminus E$, 那么我们记 $[F : E] := \dim_E F$, 并称 F 是 E 由 $[F : E]$ 次扩张得到的。

1.4.1 代数闭包

定义 1.4.3: E 上的代数闭包

设 $E \setminus F$ 是一个域扩张, 那么我们称

$\{\}$

第二章 Galois 理论

2.1 Galois 群

定义 2.1.1: Galois 群

设 E, F 是两个域, $E \setminus F$ 是一个扩张, 那么称

$$\text{Gal}(E \setminus F) = \{\sigma \in \text{Aut}(E) \mid \sigma|_F = \text{id}_F\}$$

是 $E \setminus F$ 的 *Galois* 群

定理 2.1.1: 有限扩张的 Galois 群有限

如果 $E \setminus F$ 是有限扩张, 那么 $\text{Gal}(E \setminus F)$ 是有限群

第三章 附录

这一部分中，对于正文中因为逻辑结构无法提及的部分，进行补充。

3.1 一些典型的域

3.1.1 F_p

首先约定，这一部分的讨论中，都认为 p 是一个素数。

我们首先讨论的是一个典型的有限域——模 p 剩余类域。

定义 3.1.1: F_p

设 F 是一个域， $\text{Char} F \geq p$ 且 p 是一个素数，

我们定义 $F_p = N(\mathbb{Z}_p)$

并定义其中的加法和乘法为：

$$+_F = N^{-1} \circ + \circ N, \cdot_F = N^{-1} \circ \cdot \circ N$$

定理 3.1.1: F_p 没有真子域

设 p 是一个素数，那么域 F_p 不存在真子域，即 $F_p \setminus E \rightarrow E = F_p$

证明：不妨假设命题不成立，那么一定有真子域 $E \subseteq F_p$

不妨假设 $[F_p : E] = d$ ，因为 F_p 是有限域，那么 $|E|, |F_p|$ 都是有限的。

但是， $|F_p| = |E|^d$

$\Rightarrow p = |E|^d$ ，但是 p 是素数，因此只可能 $d = 1$

于是 $|F_p| = |E|$ ，那么只可能 $F_p = E$ ，与假设矛盾，于是命题得证。 □

3.1.2 \mathbb{Q}

定理 3.1.2: \mathbb{Q} 没有真子域

\mathbb{Q} 不存在真子域, 即 $\mathbb{Q} \setminus E \rightarrow E = \mathbb{Q}$

证明: 不妨假设命题不成立, $E \subset \mathbb{Q}$ 是 \mathbb{Q} 真子域。

那么, 因为 $0, 1 \in E$, 由域对加法封闭, 那么一定有 $\mathbb{N} \subseteq E$

进一步, 因为任意元素的加法逆存在, 于是有 $\mathbb{Z} \subseteq E$

于是, 由任意非零元素的逆存在, 一定有 $\mathbb{Q} \subseteq E$ 。

但是, 我们假设 $E \subset \mathbb{Q}$, 矛盾。于是命题成立

□