§1.1 域

线性代数的基本研究对象是线性空间和其间的线性映射. 线性空间的概念需要以域的概念为基础来建立. 本节讨论域的基本概念. 粗略地说, 域是一个这样的集合, 其中的元素可以做加法、减法、乘法和除法运算, 并且这些运算满足预期的性质. 严格定义如下.

定义 1.1. 设集合F上给定了两个运算, 称为**加法**和**乘法**, 分别对F中任意两个元素x, y给出F中的元素$x+y$和xy, 并且满足下列性质:

(1) 对任意$x, y, z \in F$有

$$x+y=y+x, \quad xy=yx, \quad (x+y)+z=x+(y+z), \quad x(yz)=(xy)z, \quad x(y+z)=xy+xz.$$

(2) 存在两个不同的元素$0_F, 1_F \in F$满足对任意$x \in F$有$0_F+x=x, 1_F x=x$.

(3) 对任意$x \in F$, 存在$y \in F$满足$x+y=0_F$, 并且当$x \neq 0_F$时, 存在$z \in F$满足$xz=1_F$.

则称集合F(连同它上面的加法和乘法运算)为一个**域**(field).

注 1.1. • 加法和乘法运算指两个映射$\alpha, \mu : F \times F \to F$, $\alpha(x,y)=x+y$, $\mu(x,y)=xy$. 这里$F \times F$指F中元素的有序对构成的集合, 即

$$F \times F = \{(x,y) \mid x, y \in F\}.$$

从集合论的角度, 有序对(x,y)可以定义为$\{\{x\},\{x,y\}\}$(Kuratowski, 1921), 而映射可以定义为其图像.

- 性质(1)中的前两个式子分别称为加法和乘法的交换率, 接下来的两个式子分别称为加法和乘法的结合率, 最后一个式子称为乘法对加法的分配律. 由交换率和结合律, 对任意有限个$x_1, \ldots, x_n \in F$, 表达式$\sum_{i=1}^n x_i$和$\prod_{i=1}^n x_i$有意义. 由分配律, $(\sum_{i=1}^n x_i)(\sum_{j=1}^m y_j)=\sum_{i,j} x_i y_j$.

例 1.1. • 有理数集$\mathbb{Q}$、实数集$\mathbb{R}$和复数集$\mathbb{C}$在数的加法和乘法下是域, 分别称为有理数域、实数域和复数域.

- $\mathbb{Q}(\sqrt{2}) := \{x+\sqrt{2}y \mid x, y \in \mathbb{Q}\}$在数的加法和乘法下是域.
- 整数集$\mathbb{Z}$和正整数集$\mathbb{N}$在数的加法和乘法下不是域.
- 设p是素数. 对$x \in \mathbb{Z}$, 记

$$\bar{x} = \{n \in \mathbb{Z} \mid n \equiv x \mod p\},$$

$$\mathbb{F}_p := \{\bar{x} \mid x \in \mathbb{Z}\}.$$

容易看出, $\mathbb{F}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$. 因此$|\mathbb{F}_p| = p$. 定义

$$\bar{x}+\bar{y}=\overline{x+y}, \qquad \bar{x}\bar{y}=\overline{xy}.$$

容易证明该定义良定, 并且$\mathbb{F}_p$是域(主要是$\bar{x}^{-1}$存在).

- 有理函数域$f/g : \mathbb{C} \smallsetminus \{\text{有限个点}\} \to \mathbb{C}$. □

引理 1.1. 满足性质(2)的元素0_F和1_F是唯一的.

证明. 设$0_F, 0'_F \in F$满足对任意$x \in F$有$0_F+x=x$, $0'_F+x=x$. 在第一个式子中取$x=0'_F$, 得$0_F+0'_F=0'_F$. 在第二个式子中取$x=0_F$, 得$0'_F+0_F=0_F$. 但$0_F+0'_F=0'_F+0_F$. 所以$0'_F=0_F$.

类似地, 设$1_F, 1'_F \in F$满足对任意$x \in F$有$1_F x=x$, $1'_F x=x$. 在第一个式子中取$x=1'_F$, 得$1_F 1'_F=1'_F$. 在第二个式子中取$x=1_F$, 得$1'_F 1_F=1_F$. 但$1_F 1'_F=1'_F 1_F$. 所以$1'_F=1_F$. □

满足性质(2)的唯一元素0_F和1_F分别称为F中的**零元素**和**壹元素**. 当无歧义时, 分别记为0和1.

此时需要注意, 它们一般并不是真正的数, 只是F中的两个特殊元素, 分别用“0”和“1”这两个记号来表示.

引理 1.2. (1) 对任意$x \in F$, 满足性质(3)的元素y是唯一的.

(2) 对任意$x \in F \setminus \{0\}$, 满足性质(3)的元素z是唯一的.

证明. (1) 设$y, y' \in F$满足$x + y = x + y' = 0$. 则

$$y' = 0 + y' = (y + x) + y' = y + (x + y') = y + 0 = y.$$

(2) 设$z, z' \in F$满足$xz = xz' = 1$. 则

$$z' = 1z' = (zx)z' = z(xz') = z1 = z.$$

□

对$x \in F$, 满足$x + y = 0$的唯一元素$y \in F$称为x在F中的**负元素**, 记为$-x$. 当$x \neq 0$时, 满足$xz = 1$的唯一元素$z \in F$称为x在F中的**逆元素**, 记为x^{-1}. 我们可以把这里的负号视为取负元素的操作, 把取逆符号视为取逆元素的操作, 即考虑映射

$$F \to F, x \mapsto -x, \qquad F \setminus \{0\} \to F, x \mapsto x^{-1}.$$

于是, 形如$-(-x)$ 和$-x^{-1}$的表达式有意义. 我们定义减法和除法运算为

$$x - y = x + (-y), \qquad x/y = xy^{-1} \ (y \neq 0).$$

命题 1.3. 给定域F.

(1) (加法消去律)设$x, y, z \in F$. 如果$x + z = y + z$, 则$x = y$.

(2) 对任意$x \in F$有$0x = 0$.

(3) 设$x, y \in F$满足$xy = 0$. 则$x = 0$或$y = 0$.

证明. (1) 两边同时加上$-z$, 得

$$(x + z) + (-z) = (y + z) + (-z).$$

而

$$(x + z) + (-z) = x + (z + (-z)) = x + 0 = x.$$

类似地,

$$(y + z) + (-z) = y.$$

因此$x = y$.

(2) 注意到$0 + 0 = 0$. 因此$(0 + 0)x = 0x$. 这推出$0x + 0x = 0x + 0$. 由(1)得$0x = 0$.

(3) 若$x \neq 0$, 则$x^{-1}(xy) = (x^{-1}x)y = 1y = y$. 另一方面, 由(2)有$x^{-1}(xy) = x^{-1}0 = 0$. 因此$y = 0$. □

注 1.2. 在域的定义中, 我们要求$1 \neq 0$. 从而域中至少有两个元素. 如果不做此要求, 当$1 = 0$时, 由上面命题中的(2)(其证明没有用到$1 \neq 0$), 对任意$x \in F$有$x = 1x = 0x = 0$. 因此$F = \{0\}$. 定义中的要求即是为了排除掉这种情况.

定义 1.2. 域F的子集F'称为F的**子域**(subfield), 如果

(1) $0_F, 1_F \in F'$,

(2) $x, y \in F' \Longrightarrow x + y, -x, xy, x^{-1}$(当$x \neq 0$时) $\in F'$.

注意到子域是域.

例 1.2. $\mathbb{Q}, \mathbb{R}, \mathbb{Q}(\sqrt{2})$都是$\mathbb{C}$的子域.

对$n \in \mathbb{N}$, 记$n_F = \overbrace{1_F + \cdots + 1_F}^{n个}$. 容易看出, 对任意$m, n \in \mathbb{N} \cup \{0\}$有

$$(m+n)_F = m_F + n_F, \qquad (mn)_F = m_F n_F.$$

定义 1.3. 对于域F, 其**特征**(characteristic) $\mathrm{char}(F)$ 定义如下: 如果对任意$n \in \mathbb{N}$有$n_F \neq 0_F$, 则定义$\mathrm{char}(F) = 0$; 否则, 定义

$$\mathrm{char}(F) = \min\{n \in \mathbb{N} \mid n_F = 0_F\}.$$

命题 1.4. 假设$p = \mathrm{char}(F) \neq 0$. 则

(1) p为素数.

(2) 对$n \in \mathbb{N}$有$n_F = 0_F \iff p \mid n$.

证明. (1) 假设p不是素数. 注意到$p \geq 2$. 于是存在$r, s \in \{2, \ldots, n-1\}$满足$n = rs$. 这推出$r_F s_F = n_F = 0_F$. 另一方面, 由特征定义知$r_F, s_F \neq 0_F$, 从而$r_F s_F \neq 0_F$. 矛盾.

(2) "$\Longleftarrow$". 设$n = pq$. 则$n_F = p_F q_F = 0_F q_F = 0_F$.

"$\Longrightarrow$". 设$n = dp + r$, $0 \leq r < p$. 则$0_F = n_F = d_F p_F + r_F = d_F 0_F + r_F = r_F$. 这推出$r = 0$, 即$p \mid n$. □

命题 1.5. 设F'是域F的子域. 则$\mathrm{char}(F') = \mathrm{char}(F)$.

证明. 注意到对任意$n \in \mathbb{N} \cup \{0\}$有$n_F = n_{F'}$. 因此$n_F = 0_F \iff n_{F'} = 0_{F'}$. □

例 1.3. $\mathbb{R}, \mathbb{C}, \mathbb{Q}$的特征为0, $\mathbb{F}_p$的特征为p.

对$n \in \mathbb{N}$和$x \in F$, 定义

$$nx := \overbrace{x + \cdots + x}^{n个} = \overbrace{1_F x + \cdots + 1_F x}^{n个} = (\overbrace{1_F + \cdots + 1_F}^{n个})x = n_F x.$$

注意$n1_F = n_F$. 由于下面的命题, 有时我们需要把特征为0的域与特征非零的域区别对待.

命题 1.6. (1) 如果$\mathrm{char}(F) = 0$, 则$nx = 0_F \Longrightarrow x = 0_F$.

(2) 如果$\mathrm{char}(F) = p > 0$并且$p \nmid n$, 则$nx = 0_F \Longrightarrow x = 0_F$.

(3) 如果$\mathrm{char}(F) = p > 0$并且$p \mid n$, 则对任意$x \in F$有$nx = 0_F$.

证明. (1)+(2) $nx = 0_F \iff n_F x = 0_F$. 在(1)和(2)的条件下有$n_F \neq 0_F$. 因此$x = 0_F$.

(3) 此时总有$n_F = 0$. 因此$nx = n_F x = 0$. □

对于$n \in \mathbb{N}$, $a \in F$, 如果$n_F \neq 0_F$, 定义$\frac{1}{n}a := n_F^{-1} a$. 当$\mathrm{char}(F) = 0$时, $\frac{1}{n}a$总是有定义的. 当$\mathrm{char}(F) = p > 0$ 时, $\frac{1}{n}a$有定义的充要条件是$p \nmid n$. 容易看出, 对这两种情况, 关于$x \in F$的方程$nx = a$有唯一解$x = \frac{1}{n}a$.

习题 1.1. 设F是域.

1. (乘法消去律)设$x, y, z \in F$并且$z \neq 0$. 假设$xz = yz$. 证明$x = y$.
2. 证明映射$\varphi : F \to F$, $\varphi(x) = -x$既单又满, 并且$\varphi^{-1} = \varphi$.
3. 证明对任意$x \in F \setminus \{0\}$有$x^{-1} \neq 0$, 映射$\psi : F \setminus \{0\} \to F \setminus \{0\}$, $\psi(x) = x^{-1}$既单又满, 并且$\psi^{-1} = \psi$.

4. 证明对任意$x \in F$有$(-1)x = -x$.
5. 证明对任意$x \in F \setminus \{0\}$有$(-x)^{-1} = -(x^{-1})$.
6. 证明对任意$x, y \in F$有$(-x)y = x(-y) = -(xy)$, $(-x)(-y) = xy$.
7. 验证$\mathbb{F}_p$在课上定义的加法和乘法运算下是域.
8. 对$x \in F$和$n \in \mathbb{N}$, 定义$0x = 0_F$, $(-n)x = n(-x)$. 证明对任意$x \in F$和$m, n \in \mathbb{Z}$有
$$(m+n)x = mx + nx, \quad n(x+y) = nx + ny, \quad m(nx) = (mn)x, \quad (mx)(ny) = (mn)(xy).$$
9. 对$x \in F$和$n \in \mathbb{N}$, 定义$x^n = \overbrace{x \cdots x}^{n\text{个}}$. 对$x \neq 0_F$和$n \in \mathbb{N}$, 进一步定义$x^0 = 1_F$, $x^{-n} = (x^{-1})^n$. 证明对任意$x \in F \setminus \{0_F\}$和$m, n \in \mathbb{Z}$有
$$x^m x^n = x^{m+n}, \quad (x^m)^n = x^{mn}, \quad (xy)^n = x^n y^n.$$
10. 证明对任意$n \in \mathbb{Z}$有$(-1_F)^{2n} = 1_F$, $(-1_F)^{2n+1} = -1_F$.
11. 设$\mathrm{char}(F) = p \neq 0$. 证明$(x+y)^p = x^p + y^p, \forall x, y \in F$.
12. 设F是有限域, $|F| = q$. 证明对任意$x \in F$有$x^q = x$. (提示: 对$x \in F \setminus \{0\}$, 映射$F \setminus \{0\} \to F \setminus \{0\}$, $y \mapsto xy$即单又满, 所以$\prod_{y \in F \setminus \{0\}} xy = \prod_{y \in F \setminus \{0\}} y$, 因此$x^{q-1} = 1$.)