抽象代数笔记

詹奇

Last updated: **September 15, 2024**

Contents

1. 域与线性空间 1
   1.1. 定义与例子 1
   1.2. 域的同态 2
   1.3. 域的特征 3
   1.4. 域的扩张 3
2. 环与模 3
3. 群与群作用 3
4. Galois 理论 3

本文是刘思齐老师的抽象代数课程笔记。

1. 域与线性空间

1.1. 定义与例子

定义 1.1.1 (域). 一个域系指以下资料:

1. 集合 F, 有 $1_F, 0_F \in F$ 满足 $1_F \neq 0_F$, 有时简写为 $1, 0$.
2. F 上的加法记为 $+$, 满足加法结合律, 加法交换律, 有加法单位元 0 与加法逆元 $-a$. (这保障了加法逆元是唯一的).
3. F 上的乘法记为 $*$, 满足乘法结合律, 乘法交换律, 有乘法单位元 1, 对于非零元 a, 有乘法逆元 a^{-1}. (这保障了乘法逆元是唯一的).
4. 乘法对加法的分配律成立.

注记. 我们记 F^* 为 F 中所有非零元素的集合.

为了说明为什么我们要求 $0_F \neq 1_F$, 有以下引理:

引理 1.1.1.

1. $0_F \cdot 0_F = 0_F$.
2. $\forall x \in F, x \cdot 0_F = 0_F$

证明.

1. $0_F = 0_F + 0_F = 0_F \cdot 0_F + 0_F \cdot 0_F$, 两边减去 $0_F \cdot 0_F$ 即得.
2. $x \cdot 0_F = x \cdot (0_F + 0_F) = x \cdot 0_F + x \cdot 0_F$, 两边减去 $x \cdot 0_F$ 即得.

□

由此可见, 若 $0_F = 1_F$, 那么 F 中所有元素满足 $x = x \cdot 1_F = x \cdot 0_F = 0_f$, 这显然不是我们所期望的.

同理, 若对于域 F 上的 0_F 有逆元, 那么我们有 $0_F = a \cdot 0_F = 1_F$, 又推出了域中所有元素都是 0_F.

例子 1.1.1 (域).

1. 有理数域 $\mathbb{Q}$, 实数域 $\mathbb{R}$, 复数域 $\mathbb{C}$, 对于我们熟知的加法和乘法运算构成域.
2. $F=\mathbb{Q}\left(\sqrt{2}\right)=\left\{x+\sqrt{2}y \mid x,y\in\mathbb{Q}\right\}$.
3. $F=\mathbb{Q}\left(\sqrt[3]{2}\right)=\left\{x+\sqrt[3]{2}y \mid x,y\in\mathbb{Q}\right\}$
4. $F=\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)=\left\{x_1+x_2\sqrt{2}+x_3\sqrt{3}+x_4\sqrt{4} \mid x_i\in\mathbb{Q}\right\}$.
5. 任取素数 p, $F=\mathbb{Z}_p=\{0,1,2,...,p-1\}$, 其中加法和乘法都是模 p 的. 其中乘法逆的存在是不显然的. 对于 F 中任意一个非零元 k, 有, 我们考虑映射 $T:F_P^*\to F_P^*:y\mapsto ky$, 易证 T 是双射, 从而存在逆元 m 使得 $km=1$.
6. 设 F 是一个域, 则 $F(x)=\left\{\frac{P(x)}{Q(x)} \mid P(x),Q(x)\in F[x],Q(x)\neq 0\right\}$ 同样构成域.
7. $k=\mathbb{C}\left(x,\sqrt{x^3+2}\right)$, 可以视作 $\mathbb{C}(x)(y)$ 其中 $y^2=x^3+2$, 则 $k=\left\{R_1(x)+R_{x(y)} \mid R_1,R_2\in\mathbb{C}(x)\right\}$.

定义 1.1.2 (线性空间). 设 F 是一个域, V 是一个集合, 若 V 上定义了加法运算 $+:V\times V\to V$, 以及数乘运算 $*:F\times V\to V$, 满足以下条件:

1. 对于任意 $u,v,w\in V$, 有 $u+(v+w)=(u+v)+w$.
2. 对于任意 $v\in V$, 有 $v+0=v$.
3. 对于任意 $v\in V$, 存在 $w\in V$, 使得 $v+w=0$.
4. 对于任意 $v\in V$, 有 $1v=v$.
5. 对于任意 $a,b\in F,v\in V$, 有 $a(bv)=(ab)v$.
6. 对于任意 $a\in F,u,v\in V$, 有 $a(u+v)=au+av$.
7. 对于任意 $a,b\in F,v\in V$, 有 $(a+b)v=av+bv$.

线性空间的观点对于研究域的结构有很大的帮助, 例如我们可以将 $\mathbb{Q}\left(\sqrt{2}\right)$ 视作 $\mathbb{Q}$ 上的二维线性空间. $\mathbb{R}$ 可以视作 $\mathbb{Q}$ 上的无穷维线性空间.

例子 1.1.2. $\mathbb{F}_4=\mathbb{F}_2(\alpha)=\{x+\alpha y \mid x,y\in\mathbb{F}_2\}$. 其中的问题是我们该取什么样的 α. 考虑 $\mathbb{F}_2[x]$ 上的所有二次多项式 $f(x)=x^2+px+q$, 及 x^2,x^2+x,x^2+1,x^2+x+1. 其中前三个都是可约的, 所以我们取 α 满足 $\alpha^2+\alpha+1=0$.

1.2. 域的同态

我们先从线性空间上的同态(线性映射)开始.

定义 1.2.1 (线性映射). 设 V_1,V_2 是域 F 的线性空间, 若映射 $f:V_1\to V_2$ 满足:

1. 对于任意 $u,v\in V_1$, 有 $f(u+v)=f(u)+f(v)$.
2. 对于任意 $a\in F,v\in V_1$, 有 $f(av)=af(v)$.

那么我们称 f 是一个线性空间的同态, 即线性映射.

类似地, 我们可以定义域的同态.

定义 1.2.2 (域的同态). 设 F_1,F_2 是域, 若映射 $f:F_1\to F_2$ 满足:

1. $f\left(0_{F_1}\right)=0_{F_2},f\left(1_{F_1}\right)=1_{F_2}$.
2. 对于任意 $a,b\in F_1$, 有 $f(a+b)=f(a)+f(b)$.
3. 对于任意 $a,b\in F_1$, 有 $f(ab)=f(a)f(b)$.

那么我们称 f 是域的同态.

不同于群和环的同态, 事实上域的同态是一个"没什么用"的概念, 有下面的定理:

定理 1.2.1. 设 F_1,F_2 是域, $f:F_1\to F_2$ 是域的同态, 则 f 是单射.

证明. 设 $a,b\in F_1$ 满足 $f(a)=f(b)$. 设 $x=b-a$. 若 $x\neq 0$, 那么存在 $y\in F_1$, 使得 $xy=1$. 那么有 $0\cdot f(y)=(f(b)-f(a))\cdot f(y)=f(1)=1$, 矛盾. 所以 $x=0$, 即 $a=b$. □

这也就说明若存在一个 $\varphi : F_1 \to F_2$, 那么我们视 F_1 为 F_2 的子域, 所以在研究域的时候, 我们不关心域的同态, 而更关心子域和域扩张的概念.

定义 1.2.3 (子域与扩域). 设 F 是域, 若 E 是 F 的子集, 且 E 也构成域, 那么我们称 E 是 F 的子域, 同时称 F 是 E 的扩域, 记为 F/E.

定义 1.2.4 (域的同构). 设 F_1, F_2 是域, 若存在双射 $\varphi : F_1 \to F_2$, 且满足域的同态, 那么我们称 F_1 与 F_2 是同构的. 若 $F_1 = F_2$, 我们称 φ 是域 F_1 的自同构. 我们称在自同构下不变的元素为域 F_1 的不动域.

例子 1.2.1.

1. $\mathbb{R}/\mathbb{Q}, \mathbb{C}/\mathbb{R}, \mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}, \mathbb{F}_4/\mathbb{F}_2$.
2. $f : \mathbb{C} \to \mathbb{C}, x + iy \mapsto x - iy$ 是域 $\mathbb{C}$ 的自同构, 其中不动域是实数域 $\mathbb{R}$.
3. $\mathbb{Q}\left(\sqrt{2}\right)$ 与 $\mathbb{Q}\left(\sqrt{3}\right)$ 不存在同态.

事实上, $\mathbb{Q}, \mathbb{F}_p$ 是某种程度上的"最小"域, 我们有以下定理:

定理 1.2.2. $\mathbb{Q}, \mathbb{F}_p$ 没有真子域.

定理 1.2.3. 若 F 是 E 的扩域, 则 F 是 E 上的线性空间, 我们记 $[F : E] = \dim_E F$, 称为 F/E 的次数. 若 $[F : E] < \infty$, 则称 F/E 为有限扩张.

1.3. 域的特征

定义 1.3.1 (域的特征). 设 F 是域, 若存在最小的正整数 n, 使得 $n1_F = 0_F$, 那么我们称 n 为域 F 的特征, 记为 $\mathrm{char}(F) = n$. 若不存在这样的 n, 我们称 F 的特征为 0.

容易看出如果域的特征是正的, 那么它一定是素数. 若 $\mathrm{char}(F) = 0$, 那么 $\mathbb{Q}$ 是 F 的子域; 若 $\mathrm{char}(F) = p$, 那么 $\mathbb{F}_p$ 是 F 的子域. (注意这里的子域可以看作是存在一个域同态而不是严格的包含). 这就是说明了每个域都是 $\mathbb{Q}$ 或 $\mathbb{F}_p$ 的扩域.

在正特征的域上有一个有趣的运算. 若 $\mathrm{char}F = p > 0$, 我们考虑 $(x + y)^p$, 由二项式定理, 我们有: $(x + y)^p = x^p + y^p + C_p^1 x^{p-1} y + \ldots + C_p^{p-1} x y^{p-1} + y^p = x^p + y^p$. 我们记 $\sigma : F \to F$ 满足 $x \mapsto x^p$, 由上面的性质容易发现 σ 是一个域同构, 我们称 σ 为域 F 的 Frobenius 自同构.

1.4. 域的扩张

定义 1.4.1. 设 F/E 是一个域扩张, 对于 F 中的子集 S, 有 $E(S)$ 为 F 中包含 $E \cup S$ 的最小子域, 称为 S 在 E 上生成的域. 若 S 是有限的且 $E(S) = F$, 我们称 F 是由 E 上的有限生成扩张.

例子 1.4.1.

1. QQ(sqrt(2)) 是 QQ 上的有限生成扩张, 也是有限扩张.
2. $R(x)$ 有理函数域是 R 上的有限生成扩张, 但不是有限扩张.

2. 环与模

3. 群与群作用

4. Galois 理论