本科生基础课

近世代数讲义

陆　　俊

华东师范大学数学系

二零一三年九月

前　言

本讲义试图秉承谈胜利教授关于《高等代数与解析几何讲义》改革试点课程的教改思路, 以“解方程” 为主要线索, 逐步展开近世代数的各项丰富内容. 讲义将分为两册. 上册主要介绍近世代数的基本对象以及它们的基本性质, 内容上与传统教材相似, 但顺序上会有所不同. 下册将介绍较为深入的内容和技巧, 如伽罗华理论等等.

作者要感谢谈胜利教授对写作此讲义的热情支持, 讲稿的总体思路也来自于他的建议. 作者同时也要感谢周婷婷同学为我整理输入电子版讲稿, 其工作量是巨大的.

目 录

第一部分

基础篇

第一章　域的基础知识

1.1　数域

数域 (Number field) 是我们在高等代数中接触比较多的代数集合. 常见的数域有
(1) 有理数域 $\mathbb{Q}$,
(2) 实数域 $\mathbb{R}$,
(3) 复数域

$$\mathbb{C} = \{x + y\sqrt{-1} \mid x, y \in \mathbb{R}\}.$$

除此之外, 还有许多其他的数域. 我们首先回顾一下数域的定义.

定义 1.1.1　设 $\mathscr{P} \subseteq \mathbb{C}$ 是一个非空子集合, 如果它对加减乘除四则运算封闭, 就称为数域.

当我们在解方程的时候, 往往会发现方程的求解非常地依赖于数域. 比如方程

$$x^2 + 1 = 0,$$

在有理数域和实数域上无解, 但是在复数域上却有解 $x = \pm\sqrt{-1}$.

数域显然满足以下诸性质. 它们虽然看似显而易见, 但在我们定义抽象域的概念时, 却非常重要.
(A0) 加法封闭性: 对任何 $a, b \in \mathscr{P}$, 都有 $a + b \in \mathscr{P}$,
(A1) 加法结合律: 对任何 $a, b, c \in \mathscr{P}$, 都有 $(a + b) + c = a + (b + c)$,
(A2) 加法交换律: 对任何 $a, b \in \mathscr{P}$, 都有 $a + b = b + a$,
(A3) 加法有零元 $0 \in \mathscr{P}$: 对任何 $a \in \mathscr{P}$, 都有 $0 + a = a + 0 = a$,
(A4) 加法有逆元: 对任何 $a \in \mathscr{P}$, 存在唯一的元素 $-a \in \mathscr{P}$, 满足 $a + (-a) = (-a) + a = 0$,

(M0) 乘法封闭性: 对任何 $a, b \in \mathscr{P}$, 都有 $a \cdot b \in \mathscr{P}$,
(M1) 乘法结合律: 对任何 $a, b, c \in \mathscr{P}$, 都有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
(M2) 乘法交换律: 对任何 $a, b \in \mathscr{P}$, 都有 $a \cdot b = b \cdot a$,
(M3) 乘法有幺元 $1 \in \mathscr{P}$: 对任何 $a \in \mathscr{P}$, 都有 $1 \cdot a = a \cdot 1 = a$,
(M4) 乘法有逆元: 对任何非零元 $a \in \mathscr{P}$, 存在唯一的元素 $a^{-1} \in \mathscr{P}$, 满足 $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

(AM) 分配律: 对任何 $a, b, c \in \mathscr{P}$, 都有 $(a + b) \cdot c = a \cdot c + b \cdot c$,

注 1.1.1　(1) “幺元” 也叫做“单位元”. 现在大部分教材都采用后面的译法.
(2) ”减法” 和”除法” 显然可以用加法和乘法的逆元来定义, 即 $a - b := a + (-b)$, $\frac{a}{b} = a \cdot b^{-1}$. ■

1.2　域的抽象定义

现在我们要把数域的概念推广到更一般的对象上, 并且希望能够保留数域的基本特性

(A)(M) 等等. 考虑一个非空集合 F. 我们首先要解决的事情是: 如何定义所谓的"加法" 和"乘法"运算. 或者更一般地, 我们如何定义所谓的"(代数) 运算"".

定义 1.2.1　集合 F 上的 (代数) 运算 (Operation)是指如下映射

$$\mu : F \times F \to F.$$

比如数域 $\mathscr{P}$ 上的加法运算可以理解为

$$+ : \mathscr{P} \times \mathscr{P} \longrightarrow \mathscr{P}, \quad (a, b) \to a + b.$$

乘法运算就是

$$\cdot : \mathscr{P} \times \mathscr{P} \longrightarrow \mathscr{P}, \quad (a, b) \to a \cdot b.$$

为了方便起见, 我们通常仍采用 $\cdot$ 来表示抽象的运算, 有时就简单地称作"乘法". 如果运算满足交换律, 则往往习惯上改用"+"来表示该运算, 以强调它的交换性, 并简单地称作"加法". 请大家注意, 虽然我们采用了传统的运算符号和称法, 但不代表这样的运算就是我们通常理解的加法或乘法.

例 1.2.1　(1) 三维向量空间 V 有向量的加法运算和叉乘运算, 它们都是代数运算. 但是内积按照我们的定义, 不是代数运算, 因为两个向量的内积是一个数值而非向量.
(2) 给定集合 X, 它的所有子集构成的集族上有"并"和"交"的运算, 它们是代数运算.
(3) 方阵的乘法是代数运算, 它不满足交换律. ■

现在我们可以定义抽象的域的概念.

定义 1.2.2　假设 F 至少含两个元素, 且有两种运算"+"和"$\cdot$"(仍简称做加法和乘法), 满足诸性质 (A0-A4), (M0-M4) 及 (AM). 我们称 F 为域 (Field).

注 1.2.1　(1) 因为运算本身的定义就要求封闭性, 所以 (A0)(M0) 在上面的定义中是自然具有的.
(2) 定义中的零元和幺元虽然仍写成 0 和 1, 但未必是我们通常理解的数域零元和幺元.
(3)和前面的注记类似, 我们可以用加法和乘法的逆元来定义"减法" 和"除法" .
(4) 加法和乘法的逆元唯一性可以从交换律与结合律推出. 比如, 设非零元 a 有两个乘法逆元 b_1, b_2, 即 $ab_1 = ab_2 = 1$, 则

$$b_2 = b_2(ab_1) = (b_2a)b_1 = (ab_2)b_1 = b_1.$$

这就证明了唯一性.

1.3　域的例子

除了常见的数域之外, 我们还有许许多多重要的域. 这里例举一些经典的域.

例 1.3.1 (**有理函数域**)　考虑 $\mathbb{C}$ 上有理函数全体构成的集合

$$\mathbb{C}(x) = \left\{ \frac{f}{g} \,\middle|\, f, g \text{ 是复系数多项式, 且 } g \neq 0 \right\}.$$

我们有自然的加法“+”和乘法“·”. 零元和幺元就是 0 和 1. 这个集合在上述两种运算下构成域. 显然 $\mathbb{C} \subseteq \mathbb{C}(x)$.

如果我们把复数域替换成其他任何域 k, 也可以定义域 k 上的有理函数域 (Field of rational functions) $k(x)$. 比如 $\mathbb{Q}(x), \mathbb{R}(x)$.

特别地, 我们可以归纳地定义多元有理函数全体构成的域

$$k(x_1, x_2, \cdots, x_n) := \tilde{k}(x_n),$$

这里 k 是给定的域, $\tilde{k} = k(x_1, \cdots, x_{n-1})$ 是 $n-1$元有理函数域. ■

例 1.3.2 (二次扩域) 设 d 是非零整数, 并且要求 d 不含平方因子. 我们定义

$$\mathbb{Q}(\sqrt{d}) := \left\{ a + b\sqrt{d} \mid a, b \in \mathbb{Q} \right\}.$$

可以验证, 它在通常的加法和乘法下构成数域. 我们称它为二次扩域 (Quadratic field).

这里, 我们验证一下乘法逆元的存在性, 其余验证留给读者完成.

$$\frac{1}{a+b\sqrt{d}} = \frac{(a-b\sqrt{d})}{(a+b\sqrt{d})(a-b\sqrt{d})} = \frac{(a-b\sqrt{d})}{a^2-db^2} = \frac{a}{a^2-db^2} + \frac{(-b)}{a^2-db^2}\sqrt{d} \in \mathbb{Q}(\sqrt{d}).$$

请注意, 这里 $a^2 - db^2 \neq 0$ (否则 d 是平方数, 与假设矛盾).

$d = -1$ 时的域 $\mathbb{Q}(\sqrt{-1})$, 是数论中非常重要的研究对象–与所谓的二次及四次互反律有着密切的关系. 它是有理数域的自然推广. ■

例 1.3.3 (n 次代数数) 我们可以推广上例到更一般情形. 考虑有理数域 $\mathbb{Q}$ 上的一个不可约多项式

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_i \in \mathbb{Q}.$$

设 $x = \theta$ 是方程 $f(x) = 0$ 的根. 我们称 θ 是 n次代数数.

我们定义集合

$$\mathbb{Q}(\theta) = \{c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1} \mid c_0, c_1 \cdots, c_{n-1} \in \mathbb{Q}\}.$$

我们要证明上述集合是一个数域, 并且其中每个元素都能唯一表成上述形式.

第一步. 我们首先证明: 如果一个有理系数多项式 $g(x)$ 满足 $g(\theta) = 0$, 则 $f(x) | g(x)$.

设 $d(x) = \gcd(f(x), g(x))$. 因为 $d(x) \mid f(x)$ 且 $f(x)$ 不可约, 所以 $d(x) = 1$ 或 $d(x) = f(x)$. 由辗转相除法, 存在有理系数多项式 $s(x), t(x)$, 使得

$$d(x) = s(x)f(x) + t(x)g(x).$$

代入 $x = \theta$ 即得 $d(\theta) = 0$. 这就得到 $d(x) = f(x)$, 因而 $f(x) \mid g(x)$.

第二步. 证明

$$c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1} \tag{1-1}$$

所表之数两两不同. 假设

$$c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1} = d_0 + d_1\theta + \cdots + d_{n-1}\theta^{n-1},$$

且对某个下标 i 有 $c_i \neq d_i$, 则 θ 满足次数不超过 $n-1$ 的有理系数非零多项式方程, 这与第一步结论矛盾.

第三步. 证明加法封闭性和乘法封闭性.

设

$$\alpha = g(\theta) = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1},$$
$$\beta = h(\theta) = d_0 + d_1\theta + \cdots + d_{n-1}\theta^{n-1},$$

显然, $\alpha + \beta$ 仍满足 (1-1) 之形式. 考虑带余数除法,

$$g(x)h(x) = q(x)f(x) + r(x), \quad \deg r < \deg f = n.$$

因为 $f(\theta) = 0$, 故在上式中代入 $x = \theta$ 即得$g(\theta)h(\theta) = r(\theta)$, 该等式右边仍为 (1-1) 之形式.

第四步. 证明加法逆元和乘法逆元存在.

加法逆元显然存在. 今考虑非零元$\alpha = g(\theta)$ 同上. 由第一步及 $f(x)$ 的不可约性知, $g(x), f(x)$ 互素, 因而由辗转相除法, 存在有理系数多项式 $s(x), t(x)$, 使得

$$1 = s(x)f(x) + t(x)g(x).$$

代入 $x = \theta$ 即得 $t(\theta)g(\theta) = 1$, 即 $g(\theta)^{-1} = t(\theta)$.

其他性质都很容易验证, 我们留给读者完成. 当我们取 $f = x^2 - d$, $\theta = \sqrt{d}$, 就得到二次扩域 $\mathbb{Q}(\sqrt{d})$. 此外, $\mathbb{Q}(\theta)$ 也可以看成域 $\mathbb{Q}$ 上的 n 维向量空间, 它有一组基 $1, \theta, \cdots, \theta^{n-1}$. ■

例 1.3.4 (**有限域**) 我们这里先引入剩余类集合. 设 $N > 1$ 是给定正整数. 我们在整数集合上定义等价关系 (称为同余关系, Congruence relation)

$$n \sim m \Longleftrightarrow n \text{ 和 } m \text{ 被 } N \text{ 除的余数相同} \Longleftrightarrow \frac{n-m}{N} \text{ 是整数.}$$

因此我们得到等价类 (称作模 N 的剩余类, Residue class)

$$[n] = \{n + Nk \mid k \in \mathbb{Z}\}$$

考虑等价类全体构成的有限集合 (称作模 N 的完全剩余系, Complete residue system)

$$\mathbb{Z}_N = \{[0], [1], \cdots, [N-1]\}.$$

我们定义加法和乘法

$$[n] + [m] := [n + m], \quad [n] \cdot [m] := [n \cdot m].$$

(请读者验证上述运算的定义是合理的, 即不依赖于代表元的选取). 上面的加法和乘法显然满足交换律、结合律和分配律. 此外, $[0], [1]$ 分别是零元和幺元; 加法的逆元显然存在.

无论如何, 在很多情况下, $\mathbb{Z}_N$ 中的元未必有乘法逆元. 比如在 $\mathbb{Z}_6$ 中 $[2]$ 没有逆元.

我们来证明: *任何非零元都有乘法逆元的充分必要条件是 N 为素数.*

($\Longrightarrow$) 倘若 N 不是素数, 我们将它写成 $N = N_1N_2$, 这里 $N_i > 1$. 因此 $[N_1] \cdot [N_2] = [0]$, 从而

$$[N_1] = [N_1] \cdot ([N_2] \cdot [N_2]^{-1}) = ([N_1] \cdot [N_2]) \cdot [N_2]^{-1} = [0] \cdot [N_2]^{-1} = [0],$$

与假设矛盾!

($\Longleftarrow$) 假设 N 是素数, $[n] \neq [0]$ (即 n 不被 N 整除). 我们说明以下 N 个元素两两不同

$$[n \cdot 0], [n \cdot 1], \cdots, [n \cdot (N-1)].$$

这样的话, 它们恰好构成 $\mathbb{Z}_N$, 因而存在某 m, 使得 $[n\cdot m]=[1]$. 换言之, $[m]=[n]^{-1}$.

不妨假设 $[n\cdot m_1]=[n\cdot m_2]$, 则 $[n\cdot(m_1-m_2)]=[0]$, 即 $n(m_1-m_2)$ 被 N 整除, 从而 m_1-m_2 被 N 整除, 即 $[m_1]=[m_2]$.

因此, 当 N 是素数时, $\mathbb{Z}_N$ 是域, 也称为*模 N 的剩余类域* (Residue class field), 通常也记作 $\mathbb{F}_N$. 特别地, $\mathbb{F}_2=\{[0],[1]\}$ 是最简单的有限域. 对 $\mathbb{Z}_3$, 我们有以下的剩余类加法和乘法表.

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$\times$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

此外, $[2]^{-1}=[2]$, $[1]^{-1}=[1]$.

上述的域与我们常见的数域或函数域完全不同. 首先, 它是有限域. 其次, 每个元素和自身相加有限次后等于零元. 利用初等数论的经典结果, 我们还可以证明该域中存在这样的非零元 $[g]$, 使得任何其他非零元都能写成 $[g]$ 的方幂. 这种元素叫做*原根* (Primitive Root). ■

1.4 域的基本性质

命题 1.4.1 设 F 是域. 我们有如下性质:

(1) 零元和幺元都是唯一的.

(2) 对任何 $a\in F$, 都有 $0\cdot a=a\cdot 0=0$.

(3) 对任何 $a\in F$, 都有 $(-1)\cdot a=a\cdot(-1)=-a$.

(4) 对任何 $a,b\in F$, 都有 $(-a)\cdot b=a\cdot(-b)=-(a\cdot b)$.

(5) $0\neq 1$ 以及 $-0=0$, $1^{-1}=1$ 和 $(-1)^{-1}=-1$.

(6) (无零因子) 若 $ab=0$, 则要么 $a=0$, 要么 $b=0$.

(7) (消去律) 如果 $a\cdot c=b\cdot c$, 且 $c\neq 0$, 那么 $a=b$.

证明 (1) 设 $0,0'$ 都是加法零元. 由零元的定义, 我们有

$$0'=0+0'=0'+0=0.$$

同样地, 设 $1,1'$ 都是乘法幺元. 由幺元的定义, 我们有

$$1'=1\cdot 1'=1'\cdot 1=1.$$

(2) 由分配律

$$0\cdot a+a=0\cdot a+1\cdot a=(0+1)\cdot a=1\cdot a=a.$$

对上式两端加 $(-a)$, 并有结合律得 $0\cdot a=0$.

(3) 来自于 $a+(-1)\cdot a=1\cdot a+(-1)\cdot a=(1+(-1))\cdot a=0\cdot a=0$.

(4) $(-a)\cdot b=((-1)\cdot a)\cdot b=(-1)\cdot(a\cdot b)=-(a\cdot b)$.

(5) 若 $0=1$, 则对任何 $a\in F$, $0=0\cdot a=1\cdot a=a$. 这意味着 F 仅含一个元素, 矛盾!

由零元和幺元的定义易知, $-0=0$, $1^{-1}=1$. 由 (3) 即得 $(-1)^2=1$, 亦即 $(-1)^{-1}=-1$.

(6) 若 $a\cdot b=0$ 且 $b\neq 0$, 那么 $0=(a\cdot b)\cdot b^{-1}=a$, 矛盾!

(7) $0=a\cdot c-b\cdot c=(a-b)\cdot c$ 及 $c\neq 0$ 推出 $a-b=0$, 即 $a=b$. ■

1.5 子域和特征

前面看到, 复数域 C 中包含了很多数域 ($\mathbb{R}$, $\mathbb{Q}$,...). 这就引出了子域的概念.

定义 1.5.1 假设 F 是一个域, $E \subseteq F$ 是一个包含 $0, 1$ 的非空子集. 如果 E 在 F 的加法和乘法下也构成一个域, 则称 E 是 F 的子域 (Subfield), F 称为 E 的扩域 (Extension field).

例 1.5.1 (1) 任何数域 $\mathscr{P}$ 都是复数域 $\mathbb{C}$ 的子域.
(2) 域 k 是有理函数域 $k(x)$ 的子域.
(3) 有理数域 $\mathbb{Q}$ 是二次扩域 $\mathbb{Q}(\sqrt{d})$ 的子域. 更一般地, 对任何代数数 θ, $\mathbb{Q}$ 是 $\mathbb{Q}(\theta)$ 的子域, 后者是 $\mathbb{Q}$ 的扩域, 并且能看成 $\mathbb{Q}$ 上的有限维向量空间. ■

命题 1.5.1 (**子域的判定方法**) 设 F 是一个域, $E \subseteq F$ 是一个包含至少两个元素的非空子集. 那么 E 是 F 的子域当且仅当以下诸性质成立:
(1) 对任何 $a, b \in E$, 都有 $a - b \in E$,
(2) 对任何非零元 $a, b \in E$, 都有 $a \cdot b^{-1} \in E$.

证明 ($\Longrightarrow$) 结论显然.

($\Longleftarrow$) 已知上述性质都成立, 我们来证明 E 是 F 的子域. 由假设条件, E 至少含有一个非零元, 比如 u. 因此 $0 = u - u \in E$, $1 = u \cdot u^{-1} \in E$, 这就证明了性质 (A_3, M_3). 任取 E 中的非零元 a, b, 我们得到 $-a = 0 - a \in E$ 以及 $a^{-1} = 1 \cdot a^{-1} \in E$, 即性质 ($A_4$, M_4) 成立. 现在我们可得运算封闭性 (A_0, M_0):

$$a + b = a - (-b) \in E, \quad a \cdot b = a \cdot (b^{-1})^{-1} \in E \ (\text{若} b \neq 0).$$

其余诸性质都是显然的, 不再赘述. ■

命题 1.5.2 给定域 F.
(1) 任意多个子域的交也是 F 的子域.
(2) 给定子集 $S \subseteq F$, 所有包含 S 的子域的交是包含 S 的最小子域, 称作由 S 生成的子域.
(3) 由单位元 1 生成的子域是唯一的最小子域 (称作素域, Prime filed).

证明 (1) 设 E_α ($\alpha \in I$) 都是 F 的子域, $E = \bigcap\limits_{\alpha \in I} E_\alpha$. 我们用命题 1.5.1 的判定方法来证明 E 是子域. 对任何元素 $a, b \in E$, 由 E 的定义显然有 $a, b \in E_\alpha$, 从而 $a - b \in E_\alpha$ ($\forall \alpha$), 故 $a - b \in E$. 如果 $a, b \neq 0$, 则 $a \cdot b^{-1} \in E_\alpha$ ($\forall \alpha$) 推出 $a \cdot b^{-1} \in E$.

(2) 设 E_α ($\alpha \in I$) 都是包含 S 的全部子域. 由 (1) 知 $E = \bigcap\limits_{\alpha \in I} E_\alpha$ 也是子域, 并且显然也包含 S. 这表明 $E = E_\beta$, 对某个 $\beta \in I$. 由 E 的定义, 我们有 $E \subseteq E_\alpha$, $\forall \alpha \in I$.

(3) 假设 E 是素域. 对任何子域 $H \subseteq F$, 因为 $1 \in H$, 故由 (2) 知, $E \subseteq H$, 即 E 是最小的子域. 假设 E' 是另一个极小的子域 (即不存在更小的子域含于它), 则由 $E \subseteq E'$ 推出 $E = E'$. 这就推出了唯一性. ■

我们可以详细描述 F 的素域 E. 对任何整数 n, 以及任何元素 $a \in F$, 我们定义如下方便的

记号

$$na := \begin{cases} \underbrace{a+\cdots+a}_{n}, & n>0, \\ 0, & n=0, \\ -(\underbrace{a+\cdots+a}_{-n}), & n<0, \end{cases} \quad \text{以及} \quad a^n := \begin{cases} \underbrace{a\cdot\cdots\cdot a}_{n}, & n>0, \\ 1, & n=0, \\ (\underbrace{a\cdot\cdots\cdot a}_{-n})^{-1}, & n<0, \end{cases}$$

有时为了防止意义混淆, 在必要时, 我们也将 na 改记为 $n\cdot a$. 在上述记号下, 我们有

$$E=\{(m1)\cdot(n1)^{-1} \mid m,n\in\mathbb{Z}, n1\neq 0\}. \tag{1-2}$$

命题 1.5.3 *以下条件彼此等价:*
(1) *F 的素域是有限域,*
(2) *存在非零整数 n, 使得 $n1=0$,*
(3) *存在素数 p, 使得 $p1=0$.*
条件成立时, 上述 p 是最小的满足 $p1=0$ 的正整数.

证明 (1) $\Longrightarrow$ (2). 不妨设对任何非零整数 n, 都有 $n1\neq 0$. 此时我们可以说明对任何两个不同整数 m_1,m_2, 都有 $m_1 1\neq m_2 1$. 若不然, 则有 $(m_1-m_2)1=0$, 与假设矛盾! 这样, 素域中包含了无限多个元素, 与假设条件 (1) 矛盾!

(2) $\Longrightarrow$ (3) 设 p 是最小的正整数使得 $p1=0$. 由命题 1.4.1 (5), $p>1$. 假如 p 不是素数, 则 p 可写成两个大于 1 的整数乘积 $p=p'p''$. 此时由 p 的极小性知 $p'1\neq 0$, $p''1\neq 0$. 因此由命题 1.4.1 (6) 知

$$p1=(p'1)\cdot(p''1)\neq 0,$$

矛盾! 故 p 是素数.

(3) $\Longrightarrow$ (1) 由素域的描述 (1-2) 即得, 因此此时根据整数的带余数除法, 形如 $n1$ 的元素只有 $0\cdot 1, 1\cdot 1,\cdots,(p-1)\cdot 1$ 几类. ■

由上面的讨论, 我们可以引入域的一个重要的不变量.

定义 1.5.2 *设 F 是域. 如果 F 的素域是有限域, p 是满足 $p1=0$ 的最小正整数, 我们就称域 F 有特征 (Characteristic) p, 或者简称其有正特征; 如果 F 的素域是无限域, 就称域 F 有特征 0. 我们将特征记为 $\mathrm{ch}(F)$ 或 $\chi(F)$.*

例 1.5.2 (1) 任何数域的特征都是 0.
(2) 模素数 p 的剩余类域 $\mathbb{F}_p$ (或记为 $\mathbb{Z}_p$) 特征为 p.
(3) 有理函数域 $k(x)$ 与域 k 的特征相同. 更一般地, 一个域与它的子域有相同的特征. ■

推论 1.5.1 *域 F 和它的任何子域必有相同特征.*

推论 1.5.2 *如果域 F 的特征 $\mathrm{ch}(F)=p>0$, 那么对任何元素 $x\in F$, 都有 $px=0$.*

证明 $px=(p1)\cdot x=0$. ■

1.6 域同态

假设 E, F 是两个域. 如果我们希望了解这两个域的结构的相似程度有多大的话, 我们可以建立一个适当的映射

$$f : E \to F$$

来将它们的结构联系起来. 这有点类似于线性代数中研究两个空间结构之间的关系. 我们由此引出如下的概念.

定义 1.6.1 设 $\sigma : E \to F$ 是域之间的映射. 如果它满足以下诸条件, 则称之为域同态 (Field homomorphism):
(1) $\sigma(x+y) = \sigma(x) + \sigma(y)$, $\forall x, y \in E$.
(2) $\sigma(x \cdot y) = \sigma(x) \cdot \sigma(y)$, $\forall x, y \in E$.
进一步, 如果 σ 是单射, 我们就说它是单同态 (monomorphism); 如果是满射, 就称其为满同态 (Epimorphism); 如果存在同态 $\tau : F \to E$ 使得 $\sigma\tau = \mathrm{Id}_F$ 及 $\tau\sigma = \mathrm{Id}_E$, 则称 σ 为域同构 (Isomorphism), $\tau = \sigma^{-1}$ 为逆映射, 有时简记该同构为 $E \cong F$.

注 1.6.1 (1) 请注意上面两式中左右两端的加法和乘法是定义在不同的域中的.
(2) $\sigma : E \to F$ 是域同构当且仅当 σ 既是单同态也是满同态. ■

例 1.6.1 (1) 对任何域 F, 恒同映射 $\mathrm{Id}_F : F \to F$ 显然是域同构.
(2) 零同态 $\sigma : E \to F$ 定义为 $\sigma(x) = 0$, $\forall x \in F$. 我们也称其为平凡同态.
(3) 假设 E 是 F 的子域, 考虑嵌入映射 $i : E \hookrightarrow F$, 即 $i(x) = x$ ($\forall x \in E$). 由定义直接可知它是域同态. ■

例 1.6.2 (**二次扩域的共轭映射**) 设 $F = \mathbb{Q}(\sqrt{d})$ 是二次扩域. 我们定义映射

$$\sigma : F \to F, \quad a + b\sqrt{d} \to a - b\sqrt{d}.$$

我们验证它是域同构, 其逆映射恰好是 σ 本身.

设 $x = a + b\sqrt{d}, y = c + h\sqrt{d} \in F$. 我们有

$$\sigma(x+y) = \sigma((a+c) + (b+h)\sqrt{d}) = (a+c) - (b+h)\sqrt{d} = \sigma(x) + \sigma(y)$$

以及

$$\sigma(x \cdot y) = \sigma((ac+bhd) + (bc+ah)\sqrt{d}) = (ac+bhd) - (bc+ah)\sqrt{d} = \sigma(x) \cdot \sigma(y)$$

因此 σ 是域同态. 因为 $\sigma^2 = \mathrm{Id}_F$, 所以 $\sigma = \sigma^{-1}$ 是域同构.

此外, 容易看到 σ 限制在子域 $\mathbb{Q}$ 上是恒同映射. ■

例 1.6.3 (Frobenius **同态**) 假设 F 的特征 $\mathrm{ch}(F) = p > 0$. 我们定义映射

$$Fr : F \to F, \quad x \to x^p.$$

这实际上是一个域同态!

对任何 $x, y \in F$, 由二项式展开得

$$Fr(x+y) = (x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} C_p^k \cdot x^k y^{p-k}.$$

注意到系数 C_p^k 是 p 的倍数, 因而上式右端除了前两项外, 其余项皆为零. 这样,

$$Fr(x+y) = x^p + y^p = Fr(x) + Fr(y).$$

另一方面, $Fr(x \cdot y) = (x \cdot y)^p = x^p \cdot y^p = Fr(x) \cdot Fr(y)$. 这就证明了 Fr 是同态. 它称为 Frobenius 同态. ■

命题 1.6.1 假设 $\sigma : E \to F$ 是非零域同态, 那么

(1) $\sigma(0) = 0$, $\sigma(1) = 1$,

(2) 对任何非零元 $x \in E$, 我们有

$$\sigma(-x) = -\sigma(x), \quad \sigma(x^{-1}) = \sigma(x)^{-1}.$$

特别地, 非零元的像必定非零.

(3) σ 是单同态, 像集 $\mathrm{Im}\sigma$ 是 F 的子域.

(4) $\sigma : E \to \mathrm{Im}\sigma$ 是域同构.

(5) E, F 有相同特征.

证明 (1) 因为 $\sigma(1) = \sigma(0+1) = \sigma(0) + \sigma(1)$, 所以 $\sigma(0) = 0$.

我们取 $a \in E$, 使得 $\sigma(a) \neq 0$. 由上面讨论, 这样的 a 必是非零元. 因为 $\sigma(a) = \sigma(1 \cdot a) = \sigma(1) \cdot \sigma(a)$, 所以 $\sigma(1) = 1$.

(2) 因为

$$0 = \sigma(0) = \sigma(x + (-x)) = \sigma(x) + \sigma(-x).$$

所以 $\sigma(-x) = -\sigma(x)$. 类似地,

$$1 = \sigma(1) = \sigma(x \cdot x^{-1}) = \sigma(x) \cdot \sigma(x^{-1}).$$

故由命题 1.4.1 (2) 知, $\sigma(x) \neq 0$, 且 $\sigma(x^{-1}) = \sigma(x)^{-1}$.

(3) 假设σ 不是单同态, 那么存在两个不同元素 $x, y \in E$, 使得 $\sigma(x) = \sigma(y)$. 因而

$$\sigma(x - y) = \sigma(x) - \sigma(y) = 0.$$

由 (2) 可知, $x - y = 0$, 即 $x = y$, 矛盾! 故 σ 是单同态.

为说明像集 $\mathrm{Im}\sigma$ 是 F 的子域, 我们使用命题 1.5.1. 首先注意 $0, 1 \in \mathrm{Im}\sigma$. 对任何 $a = \sigma(x), b = \sigma(y) \in \mathrm{Im}\sigma$, 我们有 $a - b = \sigma(x - y) \in \mathrm{Im}\sigma$. 如果 $a, b \neq 0$, 则 $x, y \neq 0$, 从而 $a \cdot b^{-1} = \sigma(x \cdot y^{-1}) \in \mathrm{Im}\sigma$.

(4) 我们验证逆映射 $\sigma^{-1} : \mathrm{Im}\sigma \to E$ 是同态. 任取 $a = \sigma(x), b = \sigma(y) \in \mathrm{Im}\sigma$. 我们有

$$\sigma^{-1}(a+b) = \sigma^{-1}(\sigma(x) + \sigma(y)) = \sigma^{-1}(\sigma(x+y)) = x + y = \sigma^{-1}(a) + \sigma^{-1}(b),$$

以及

$$\sigma^{-1}(a \cdot b) = \sigma^{-1}(\sigma(x) \cdot \sigma(y)) = \sigma^{-1}(\sigma(x \cdot y)) = x \cdot y = \sigma^{-1}(a) \cdot \sigma^{-1}(b).$$

因此 σ^{-1} 是同态.

(5) 由 (3) 及推论 1.5.1, $\mathrm{Im}\sigma$ 与 F 有相同特征. 因此由 (4), 我们可以把讨论归结到 $\sigma : E \to F$ 是域同构的情形. 如果 $\mathrm{ch}(E) = p > 0$, 那么 $p1_F = p \cdot \sigma(1_E) = \sigma(p1_E) = \sigma(0) = 0$, 从而由命题 1.5.3 得 $\mathrm{ch}(F) = p$. 如果 $\mathrm{ch}(E) = 0$, 那么 $\mathrm{ch}(F) = 0$, 否则上面讨论推出 $\mathrm{ch}(E) > 0$, 矛盾! ■

例 1.6.4　取 $F=\mathbb{F}_p$ 为模素数 p 的剩余类域. 考虑 Frobenius 同态 $Fr: F\to F$. 由命题 1.6.1(1), $Fr([n])=Fr(n\cdot[1])=n\cdot Fr([1])=n\cdot[1]=[n]$, 故它是恒同映射. 这就推出 $Fr([n])=[n]^p=[n]$, $\forall n\in\mathbb{Z}$. 换言之, $[n^p]=[n]$, 亦即 $p\mid(n^p-n)$. 这就是初等数论中的费马小定理 . ■

推论 1.6.1　域 F 的素域同构于模 p 的剩余类域 $\mathbb{F}_p$ (如果特征 $\mathrm{ch}(F)=p$) 或有理数域 $\mathbb{Q}$ (如果特征 $\mathrm{ch}(F)=0$).

证明　设 E 是 F 的素域. 我们讨论 $\mathrm{ch}(F)=p>0$ 的情形, 零特征情形类似可证. 我们构造域同态

$$\sigma:\mathbb{F}_p\to E,\quad [n]\to n1$$

以及域同态

$$\tau: E\to\mathbb{F}_p,\quad (n1)\cdot(m1)^{-1}\to[n]\cdot[m]^{-1}.$$

显然 $\tau\sigma=\mathrm{Id}_{\mathbb{F}_p}$.

考虑 E 中任何元素 $a=(n1)\cdot(m1)^{-1}$. 今取整数 m^*, 使得 $[m^*]=[m]^{-1}$, 于是 $[mm^*]=[1]$, 即 (mm^*-1) 是 p 的倍数. 因而

$$(m1_F)\cdot(m^*1_F)=mm^*\cdot 1_F=(mm^*-1)1_F+1_F=1_F.$$

这就推出 $(m\cdot 1_F)^{-1}=m^*1_F$, 故 $a=(nm^*)1_F$. 这样, $\sigma\tau(a)=(nm^*)1_F=a$. 因此 $\sigma\tau=\mathrm{Id}_E$. 这就证明 σ 是域同构. ■

注 1.6.2　域同构给出了域之间的一个等价关系. 我们只需要研究每个等价类中的代表元即可, 这是因为同构的域在代数结构上具有相同的性质. 比如上述命题表明素域的结构其实只有两种可能性, 即剩余类域或有理数域, 所以我们只需要研究这两种域的性质即可了解素域. ■

例 1.6.5　(1) 验证: 不存在从有理函数域 $\mathbb{Q}(x)$ 到二次扩域 $\mathbb{Q}(\sqrt{d})$ 的非平凡域同态.

反证法. 假设 $\sigma:\mathbb{Q}(x)\to\mathbb{Q}(\sqrt{d})$ 是非零域同态, $\sigma(x)=a+b\sqrt{d}$. 因为 $\sigma(1)=1$, 所以 $\sigma(n)=\sigma(n1)=n\cdot\sigma(1)=n$, $\forall n\in\mathbb{Z}$. 因此对任何有理数 $\frac{n}{m}$, 我们有 $\sigma(\frac{n}{m})=\frac{\sigma(n)}{\sigma(m)}=\frac{n}{m}$. 这推出

$$\sigma\left(\left(\frac{x-a}{b}\right)^2\right)=\sigma\left(\frac{x-a}{b}\right)^2=\left(\frac{\sigma(x)-\sigma(a)}{\sigma(b)}\right)^2=\left(\frac{\sigma(x)-a}{b}\right)^2=d=\sigma(d).$$

由域同态的单射性得 $(\frac{x-a}{b})^2=d$. 这与 x 是不定元的事实矛盾!

(2) 验证: 不存在剩余类域 $\mathbb{F}_p$ 到有理数域 $\mathbb{Q}(\sqrt{d})$ 的非平凡域同态.

反证法. 如果存在非平凡同态, 那么由命题 1.6.1 (5), 两个域必须有相同特征. 无论如何, $\mathrm{ch}(\mathbb{F}_p)=p$, $\mathrm{ch}(\mathbb{Q}(\sqrt{d}))=0$, 矛盾! ■

例 1.6.6　证明: 域 $\mathbb{Q}(\sqrt{d})$ 到自身的非零同态仅有两种: 恒同映射和共轭映射 (见例 1.6.2).

证明　假设 $\sigma:\mathbb{Q}(\sqrt{d})\to\mathbb{Q}(\sqrt{d})$ 是非平凡同态. 设 $\sigma(\sqrt{d})=a+b\sqrt{d}$, 类似上例的讨论,

$$d=\sigma(d)=\sigma(\sqrt{d})^2=(a+b\sqrt{d})^2=(a^2+b^2d)+2ab\sqrt{d}.$$

这意味着 $ab=0$, $a^2+b^2d=d$. 如果 $b=0$, 那么 $d=a^2$, 这与 d 不含平方因子的假设条件矛盾! 因此 $a=0$, 从而 $b=\pm1$. 注意到, 对任何 $s+t\sqrt{d}\in\mathbb{Q}(\sqrt{d})$, 有 $\sigma(s+t\sqrt{d})=s+tb\sqrt{d}$. 因此若 $b=1$, σ 就是恒同映射; 若 $b=-1$, σ 就是共轭映射. ■

1.7 补充材料: 代数闭域

解方程有两个中心问题:
(1) 方程在给定的数域内是否存在解? 有多少解?
(2) 能否精确给出方程的公式解?

对复系数多项式

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \quad a_i \in \mathbb{C},$$

高斯证明了如下基本结论:

定理 1.7.1 (**高斯代数学基本定理**) 复系数方程 $f(x) = 0$ 在复数域内恰有 n 个复数根 (重根重复计算).

这个定理有许多不同的证明, 但是任何一类证明都不可能是纯代数的. 也就是说, 代数学基本定理的证明中总是不可避免地包含一部分几何性质的运用 (我们把复数域看成复平面这类几何对象). 事实上这个定理反映的本质是几何的, 尽管表面叙述上看是代数的.

代数学基本定理也可以等价叙述为

推论 1.7.1 复系数多项式 $f(x)$ 必可分解为复数域上一次多项式乘积

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n), \quad \alpha_i \in \mathbb{C}.$$

我们可以从代数学基本定理中提取出代数的信息, 引入如下概念.

定义 1.7.1 如果一个域 k 满足以下性质, 就称之为代数闭域 (Algebraically closed field): 对任何系数取自于域 k 的多项式

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \quad a_i \in k,$$

总是可以分解为一次因式的乘积

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n), \quad \alpha_i \in k.$$

代数学基本定理相当于说复数域是代数闭域. 一个重要的结论说, 任何域 k 都是某个代数闭域 $\bar{k}$ 的子域. 因此从这个意义上讲, 任何多项式方程在扩大域的范围后总是可以求根. 另外请注意, 上面这个结论的证明是代数的, 但是它在数域情形不能推出所得到的代数闭域就是复数域, 也不能用它证明复数域是代数闭域.

解方程的第二个中心问题也同样需要我们研究如何在扩域中求根的问题, 并且需要讨论这样的扩域之间的各种同构等等. 由此引出了扩域论和伽罗华理论. 我们将在下册深入探讨这些理论. 此处不再详细展开了.

本章习题

加 $*$ 号的习题表示有一定难度.

习题 1.1 证明: 除了复数域外, 不存在严格包含实数域的数域.

习题 1.2 验证模 N 的剩余系上的加法和乘法不依赖于剩余类的代表元选取.

习题 1.3 给定非空集合 X, 设 Σ 是 X 的幂集, 即全体子集构成的集族. 试逐一检验 $(\Sigma, \cap, \cup)$ 是否满足域的 11 条性质 $(A_0 - A_4)$, $(M_0 - M_4)$ 及 (AM).

习题 1.4 在有理数域上定义新的运算

$$a \oplus b = a + b - 1,$$
$$a * b = a + b - ab.$$

试问: 有理数域在上述两种运算下是否构成域?

习题 1.5 设 F 是域, $a, b \in F$, $n, m \in \mathbb{Z}$. 证明:
(1) $n(a+b) = na + nb$ 及 $(n+m)a = na + ma$,
(2) $n(ma) = (nm)a$ 及 $n(a \cdot b) = (na) \cdot b = a \cdot (nb)$,
(3) $a^{n+m} = a^n \cdot a^m$, $(a^n)^m = a^{nm}$ 及 $(a \cdot b)^n = a^n \cdot b^n$.

习题 1.6 考虑集合

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.$$

验证它是一个数域, 并证明 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

习题 1.7 证明: $\mathbb{Q}(1 + \sqrt{-1}) = \mathbb{Q}(4 - \sqrt{-1})$.

习题 1.8 证明: $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ 的充分必要条件是存在非零有理数 c, 使得 $d = c^2 d'$.

习题 1.9 设 F 是域, $a \in F$ 是非零元. 证明: 如果 $a \neq 1, -1$, 那么 $a \neq a^{-1}$.

习题 1.10 设 F 是域, E 是 F 的非空子集, 且至少含两个元素. 证明: E 是 F 的子域当且仅当如下条件成立: 对任何 $a, b, c \in E$, 且 $c \neq 0$, 都有 $(a - b) \cdot c^{-1} \in E$.

习题 1.11 验证如下结论: $\sigma : E \to F$ 是域同构当且仅当 σ 既是单同态也是满同态.

习题 1.12 证明或否定如下叙述: $\mathbb{Q}(\sqrt{3})$ 与 $\mathbb{Q}(\sqrt{-3})$ 作为域是同构的.

习题 1.13 设 θ 是 n 次代数数, 证明: 存在从 $\mathbb{Q}(\theta)$ 到二次扩域 $\mathbb{Q}(\sqrt{d})$ 的非平凡域同态的充分必要条件是 $\theta \in \mathbb{Q}(\sqrt{d})$.

习题 1.14 (*) 设 θ, θ' 是代数数, 你能否给出 $\mathbb{Q}(\theta)$ 与 $\mathbb{Q}(\theta')$ 同构的充分必要条件? 试着证明你的结论.

习题 1.15 假设 F_1, F_2 是两个域, E_1, E_2 分别是它们的素域. 设 $\sigma : F_1 \to F_2$ 是非平凡同态. 证明: σ 诱导了素域间的同构 $\sigma : E_1 \to E_2$. 特别地, 当 $F_1 = F_2$ 时, $\sigma : E_1 \to E_2$ 是恒同映射.

习题 1.16 考虑域 $\mathbb{F}_p$ 上的有理函数域 $\mathbb{F}_p(x)$ 之间的 Frobenius 同态

$$Fr : \mathbb{F}_p(x) \to \mathbb{F}_p(x).$$

证明: $Fr(f(x)) = f(x^p)$.

习题 1.17 (*) 证明:实数域 $\mathbb{R}$ 到自身的非零同态只有恒同映射 (提示:证明这样的同态是保序映射).

第二章　环的基础知识

2.1　一些非域的经典例子

上一节我们研究了代数对象 (即具有代数运算的集合) 中最特殊的一类: 域. 它有两种运算, 且满足 11 条基本的运算公理 $(A0-A4)$, $(M0-M4)$ 及 (AM). 在我们曾经学过的各种代数对象中, 有很多却并非是域–尽管它们有两种运算. 在我们开始这一章之前, 先来回顾一下这些熟悉的例子.

例 2.1.1 (整数环)　设 $\mathbb{Z}$ 是所有整数的全体. 它有通常的加法和乘法运算, 且有零元 0 和幺元 1. 对 $\mathbb{Z}$ 中任何不等于 ±1 的非零整数, 都不可能存在乘法逆元. 因此它不满足公理 $(M4)$. 除此之外, 它满足其他所有公理.

顺便提一下, 初等数论的很多不定方程求都关心整数解. 求方程的整数解往往是非常困难的问题. ■

例 2.1.2 (多项式环)　设 $\mathbb{R}[x]$ 是所有实系数多项式构成的集合 (类似地, 可以考虑 $\mathbb{Q}[x], \mathbb{C}[x]$ 等等)

$$\mathbb{Q}[x] = \{f |\ f = a_0 + a_1x + \cdots + a_nx^n, \text{ 诸 } a_i \in \mathbb{R}, \quad n \text{ 是非负整数}\}.$$

它有通常的多项式加法和乘法运算, 且有零元 0 和幺元 1. 和整数环一样, 除了非零常数外, 任何多项式都没有乘法逆元. 因而它不满足公理 $(M4)$, 但满足其他所有公理. ■

例 2.1.3 (矩阵环)　考虑数域 F 上 n 阶方阵全体构成的集合.

$$M_n(F) := \left\{ \left(\begin{array}{ccc} a_{11} & \cdots\cdots & a_{1n} \\ \cdots & \cdots\cdots & \cdots \\ a_{n1} & \cdots\cdots & a_{nn} \end{array} \right) \middle|\ a_{ij} \in F \right\}.$$

它有通常的矩阵加法和乘法, 其零元是零矩阵, 幺元是单位矩阵. 它不仅不满足乘法逆元的存在性公理 $(M4)$, 也不满足乘法的交换律 $(M2)$. 其他公理仍然成立. ■

例 2.1.4 (线性变换)　考虑数域 F 上的 n 维线性空间 V. V 上的线性变换 f 是指 V 到自身的线性映射 $f : V \to V$, 即满足

$$f(k_1v_1 + k_2v_2) = k_1f(v_1) + k_2f(v_2), \quad \forall k_1, k_2 \in F, \quad \forall v_1, v_2 \in V.$$

所有线性变换的全体组成的集合记为 $\mathrm{End}_n(V)$. 它有加法运算

$$f + g : V \longrightarrow V, \quad v \to (f + g)(v) := f(v) + g(v).$$

以及复合运算 (我们将它视作一种"乘法"运算)

$$(f \cdot g) : V \longrightarrow V, \quad v \to (f \cdot g)(v) := f(g(v)).$$

零映射显然是加法零元, 恒同映射则是乘法幺元. 与上例类似, 一般的线性变换都没有乘法逆元 (除非是线性同构). 此外, 它也不满足乘法交换律.

实际上, 由高等代数的经典讨论可以知道, 在选定 V 的一组基后, 矩阵环 $M_n(F)$ 和 $\mathrm{End}(V)$ 之间可以建立一一对应, 这种对应可以保持加法和乘法的兼容性 (今后我们会用"同构"这一术语来描述这样的对应). ■

例 2.1.5 (模 N 剩余类环) 回顾例 1.3.4 中所定义的模 N 的完全剩余系

$$\mathbb{Z}_N = \{[0], [1], \cdots, [N-1]\},$$

这里

$$[n] = \{n + Nk \mid k \in \mathbb{Z}\}$$

是 N 所代表的剩余类, 它是由同余关系

$$n \sim m \Longleftrightarrow n \text{ 和 } m \text{ 被 } N \text{ 除的余数相同} \Longleftrightarrow \frac{n-m}{N} \text{ 是整数.}$$

所定义的等价类. 我们曾定义加法和乘法

$$[n] + [m] := [n+m], \quad [n] \cdot [m] := [n \cdot m].$$

它们满足结合律、交换律和分配律, 且零元和幺元分别为 [0], [1]. 我们已经证明, 如果 N 不是素数, 那么 $\mathbb{Z}_N$ 中必有某个非零元素没有乘法逆元. 比如 $\mathbb{Z}_6$ 中的 [2], [3], [4] 都没有乘法逆元. ■

例 2.1.6 (无幺元) 全体偶数组成的集合 $2\mathbb{Z}$ 有通常的加法和乘法, 它们满足交换律、结合律和分配律. 尽管 $2\mathbb{Z}$ 有加法零元和逆元, 但是却没有乘法幺元和逆元. ■

例 2.1.7 (非结合律) 考虑三维实向量空间 V. V 中的向量有通常的向量加法和叉乘运算 (Cross Product). 但令人遗憾的是, 叉乘运算不满足结合律. 不过它满足以下的雅可比恒等式

$$u \times (v \times w) + v \times (w \times u) + w \times (u \times v) = 0.$$

还有很多例子都不能满足域的全部公理. 我们会在后面逐一介绍它们, 并将这些例子提炼成更一般的抽象概念.

2.2 除环 (体)

人们对数系的认识从有理数域到实数域, 最终发现了复数域. 这种认识发展和解方程有着密切的关系–通过方程的求根来扩充数系. 一个自然的问题是, 我们能否构造出比复数域更大的数域? 也就是引进所谓的"超复数". 根据前面提及的高斯代数学基本定理, 通过方程求根的经典方法来寻找"超复数"已经是不可能了.

人们转而从其他角度来思考这个问题. 比如将复数域看作二维向量空间, 复数看作其中的向量, 那么"超复数"是否可以类似推广为高维向量呢? 这其实就是三维及高维向量空间分析的历史源头. 正如前面所看到的, 三维向量空间中很难定义一个好的乘法让它满足那些公理 (比如叉乘不满足结合律和交换律, 更没有幺元和乘法逆元的概念).

数学家哈密顿 (Hamilton) 在对这个问题经过长时间思考之后, 终于意识到一件重要的事情: 如果我们要扩充复数域的话, 那么必须放弃乘法交换律! 他于 1843 年发现了著名的四元数体. 这一发现在数学史上具有划时代意义. 因为它将代数学从传统算术中解放出来, 让人们意识到创建各种代数体系未必需要拘泥于域的全部运算公理. 一旦摆脱了这一思维枷锁, 近代的代数学才真正开始发展起来.

2.2.1 哈密顿四元数体

下面我们来介绍哈密顿四元数体 (Hamiltonian quaternions).

考虑如下类型的 2 阶复系数矩阵全体构成的集合

$$\mathbb{H} := \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \middle| \alpha, \beta \in \mathbb{C} \right\},$$

这里 $\bar{x}$ 表示 x 的共轭复数. $\mathbb{H}$ 显然是复矩阵环 $M_2(\mathbb{C})$ 的子集. 任取

$$A = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \quad B = \begin{pmatrix} \gamma & \delta \\ -\bar{\delta} & \bar{\gamma} \end{pmatrix}.$$

在矩阵的通常加法和乘法下, 我们有

$$A + B = \begin{pmatrix} \alpha+\gamma & \beta+\delta \\ \overline{-\beta+\delta} & \overline{\alpha+\gamma} \end{pmatrix} \in \mathbb{H}, \quad A \cdot B = \begin{pmatrix} \alpha\gamma - \beta\bar{\delta} & \alpha\delta + \beta\bar{\gamma} \\ \overline{-\alpha\delta + \beta\bar{\gamma}} & \overline{\alpha\gamma - \beta\bar{\delta}} \end{pmatrix} \in \mathbb{H}$$

因此 $\mathbb{H}$ 满足加法和乘法的封闭性, 即公理 $(A0)$ 和 $(M0)$. 此外 $\mathbb{H}$ 显然包含零阵和单位阵作为零元和幺元, 即满足公理 $(A3)$ 和 $(M3)$. 假设 A 非零阵. 注意到行列式 $\det(A) = |\alpha|^2 + |\beta|^2 > 0$, 我们有

$$-A = \begin{pmatrix} -\alpha & -\beta \\ \bar{\beta} & -\bar{\alpha} \end{pmatrix} \in \mathbb{H}, \quad A^{-1} = \frac{1}{|\alpha|^2 + |\beta|^2} \begin{pmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{pmatrix} \in \mathbb{H}.$$

这就证明了公理 $(A4)$ 和 $(M4)$. 至于结合律 $(A1)(M1)$ 和分配律 (AM) 都是显然的. $\mathbb{H}$ 虽然满足加法交换律 $(A2)$, 但是却不满足乘法交换律! 这是它和域的唯一差别.

$\mathbb{H}$ 中有四个特殊的元素, 我们用以下的黑体记号表示

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}.$$

由定义, $\mathbb{H}$ 中任何元素都能写为 $a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ 的形式; 反之这样形式的元素也必落在 A 中.

定义 2.2.1 *我们将上述 $(\mathbb{H}, +, \cdot)$ 称为哈密顿四元数体. $\mathbb{H}$ 中的元素称为四元数.*

如上所说, $\mathbb{H}$ 可以看作是实数域上的 4-维向量空间, 它有一组基

$$\mathbf{1}, \quad \mathbf{i}, \quad \mathbf{j}, \quad \mathbf{k}.$$

它们之间的乘法满足如下规则:

(1) $\mathbf{i} \cdot \mathbf{i} = \mathbf{j} \cdot \mathbf{j} = \mathbf{k} \cdot \mathbf{k} = -\mathbf{1}$ 及 $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$.

(2) $\mathbf{i} \cdot \mathbf{j} = -\mathbf{j} \cdot \mathbf{i} = \mathbf{k}$, $\mathbf{j} \cdot \mathbf{k} = -\mathbf{k} \cdot \mathbf{j} = \mathbf{i}$ 及 $\mathbf{k} \cdot \mathbf{i} = -\mathbf{i} \cdot \mathbf{k} = \mathbf{j}$.

(3) $\mathbf{1} \cdot \mathbf{i} = \mathbf{i} \cdot \mathbf{1} = \mathbf{i}$, $\mathbf{1} \cdot \mathbf{j} = \mathbf{j} \cdot \mathbf{1} = \mathbf{j}$ 及 $\mathbf{k} \cdot \mathbf{1} = \mathbf{1} \cdot \mathbf{k} = \mathbf{k}$.

(4) $\mathbf{i} \cdot \mathbf{j} \cdot \mathbf{k} = -\mathbf{1}$. 为方便记忆, 我们列成如下的乘法表.

	$\mathbf{1}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	$-\mathbf{1}$	$\mathbf{k}$	$-\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	$-\mathbf{1}$	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	$-\mathbf{1}$

因此我们也可以直接从四维空间出发, 利用上述乘法表以及分配律来重新定义四元数体. 实际上, 人们最初就是这样构造四元数体的. 如果我们就把 $\mathbf{1}$ 看成通常的实数单位 1, 把 $\mathbf{i}$ 看成虚数单位 $\sqrt{-1}$, 那么四元数体相当于包含了复数域. 这就等于扩充了复数域. 遗憾的是, 四元数体不满足乘法交换律.

注 2.2.1　假如我们把 $(\mathbf{i},\mathbf{j},\mathbf{k})$ 看成右手螺旋的三维空间坐标架, 那么它们两两之间的乘法可以按照向量叉乘的右手螺旋法则来对应, 这样比较方便记忆. ■

例 2.2.1　设

$$v = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}, \quad \bar{v} = a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}, \quad \mathcal{N}(v) := a^2 + b^2 + c^2 + d^2.$$

直接验算可得

$$\bar{v} \cdot v = v \cdot \bar{v} = \mathcal{N}(v)\mathbf{1}.$$

我们称 $\mathcal{N}(v)$ 为 v 的范数 (Norm), $\bar{v}$ 称为 v 的共轭元. 任何非零元 v 的乘法逆元

$$v^{-1} = \bar{v} \cdot (|v|\mathbf{1})^{-1} = \frac{a}{|v|}\mathbf{1} - \frac{b}{|v|}\mathbf{i} - \frac{c}{|v|}\mathbf{j} - \frac{d}{|v|}\mathbf{k}.$$

例 2.2.2　设 $\alpha = 3\mathbf{1} + 4\mathbf{i} + \mathbf{k}$, $\beta = \mathbf{j} - 2\mathbf{k}$.
(1) $\alpha + \beta = 3\mathbf{1} + 4\mathbf{i} + \mathbf{j} - \mathbf{k}$.
(2)

$$\begin{aligned}\alpha \cdot \beta &= \alpha \cdot \mathbf{j} - 2\alpha \cdot \mathbf{k} \\ &= (3\mathbf{1} \cdot \mathbf{j} + 4\mathbf{i} \cdot \mathbf{j} + \mathbf{k} \cdot \mathbf{j}) - 2(3\mathbf{1} \cdot \mathbf{k} + 4\mathbf{i} \cdot \mathbf{k} + \mathbf{k} \cdot \mathbf{k}) \\ &= (3\mathbf{j} + 4\mathbf{k} - \mathbf{i}) - 2(3\mathbf{k} - 4\mathbf{j} - \mathbf{1}) \\ &= 2\mathbf{1} - \mathbf{i} + 11\mathbf{j} - 2\mathbf{k}.\end{aligned}$$

类似可得 $\beta \cdot \alpha = 2\mathbf{1} + \mathbf{i} - 5\mathbf{j} - 10\mathbf{k}$.
(3) $\alpha \cdot \beta^{-1} = \alpha \cdot \bar{\beta} \cdot (\mathcal{N}(\beta)\mathbf{1})^{-1} = -\frac{1}{5}\alpha \cdot \beta = -\frac{2}{5}\mathbf{1} + \frac{1}{5}\mathbf{i} - \frac{11}{5}\mathbf{j} + \frac{2}{5}\mathbf{k}$. ■

2.2.2 除环 (体) 的抽象定义

定义 2.2.2　假设 H 是至少含有两个元素的集合, 并具有运算 "+" 和 "·". 如果 H 满足除了乘法交换律以外的所有公理 (即 $(A0-A4)$, $(M0-M1, M3-M4)$ 及 (AM)), 则称之为除环 (Division ring). 进一步, 如果 H 不满足乘法交换律, 则亦称之为体 (Body, Skew filed).

注 2.2.2　(1) 有些书上, 也将除环统译为"体"; 为了强调非交换性, 将体称作斜体 (Skew filed) 或非交换体.
(2) 从定义看, 除环其实只有域 (满足乘法交换律) 和体 (不满足乘法交换律) 两类.
(3) 有时为书写方便, 我们仍然将零元记为 0, 幺元记为 1. ■

例 2.2.3　(1) 域都是除环, 但不是体.
(2) 哈密顿四元数体是体. ■

我们也可以类似引进子除环 (子体) 的概念.

定义 2.2.3　假设 H 是除环, $F \subseteq H$ 是非空子集. 如果 F 在 H 的加法和乘法运算下, 构成一个除环, 则称 F 是 H 的子除环 (Division subring). 如果 F 不满足乘法交换律, 则亦称作子体.

显然, 一个域的子除环就是它的子域, 这两个概念在此时是一样. 体的子除环有可能是域, 也可能不是域.

例 2.2.4　(1) 设

$$F = \{a\mathbf{1} + b\mathbf{i} |\ a, b \in \mathbb{R}\} \subseteq \mathbb{H}.$$

它是四元数体 $\mathbb{H}$ 的子除环, 并且是域 (实际上它和复数域同构).

(2) 设 E 是实数域中的子域. 我们定义

$$\overline{E} = \{a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} |\ a, b, c, d \in E\} \subseteq \mathbb{H}.$$

它是 $\mathbb{H}$ 的子体. ■

例 2.2.5　设 H 是除环. 我们定义集合

$$C(H) = \{a |\ a \cdot x = x \cdot a, \quad \forall x \in H\}.$$

我们来验证, $C(H)$ 是 H 的子除环, 并且是域. 我们称 $C(H)$ 是 H 的中心 (Center), $C(H)$ 中的元素称为中心元素. 由定义, 中心元素就是和除环中任何元素乘法可交换的元.

首先, 显然有 $0, 1 \in H$. 设 $a, b \in C(H)$. 对任何 $x \in H$, 我们有

$$(a \cdot b) \cdot x = a \cdot (b \cdot x) = a(x \cdot b) = (x \cdot b) \cdot a = x \cdot (b \cdot a) = x \cdot (a \cdot b).$$

因而 $a \cdot b \in C(H)$. 类似可证 $a + b \in C(H)$. 当 $a \neq 0$ 时,

$$a^{-1} \cdot x = a^{-1} \cdot x \cdot (a \cdot a^{-1}) = a^{-1} \cdot (x \cdot a) \cdot a^{-1} = a^{-1} \cdot (a \cdot x) \cdot a^{-1} = (a^{-1} \cdot a) \cdot x \cdot a^{-1} = x \cdot a^{-1}.$$

这就推出 $a^{-1} \in C(H)$. 类似可得 $-a \in C(H)$.

由中心的定义, 显见 $C(H)$ 的乘法满足交换律. 其余公理容易验证, 我们不再赘述. ■

同样地, 我们也可引进除环的同态和同构概念.

定义 2.2.4　设 $\sigma : F \to H$ 是除环之间的映射. 如果它满足以下诸条件, 则称之为除环同态:

(1) $\sigma(x + y) = \sigma(x) + \sigma(y)$, $\forall x, y \in F$.

(2) $\sigma(x \cdot y) = \sigma(x) \cdot \sigma(y)$, $\forall x, y \in F$.

进一步, 如果 σ 是单射 (满射), 我们就说它是单同态 (满同态). 如果存在同态 $\tau : H \to F$ 使得 $\sigma\tau = \mathrm{Id}_H$ 及 $\tau\sigma = \mathrm{Id}_F$, 则称 σ 为同构, $\tau = \sigma^{-1}$ 为逆映射, 有时简记该同构为 $F \cong H$. 除环 H 到自身的同构简称为自同构.

例 2.2.6　我们有复数域到四元数体的单同态:

$$\mathbb{C} \hookrightarrow \mathbb{H}, \quad a + b\sqrt{-1} \to a\mathbf{1} + b\mathbf{i}.$$

例 2.2.7　验证四元数体的中心同构于 $\mathbb{R}$.

假设 $v = a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \in C(\mathbb{H})$. 于是 $v\cdot\mathbf{i} = \mathbf{i}\cdot v$. 这就推出 $c = d = 0$. 同样地, 由 $v\cdot\mathbf{j} = \mathbf{j}\cdot v$ 推出 $b = 0$, 因而 $v = a\mathbf{1}$. 反之, 形如 $a\mathbf{1}$ 的元素都在 $C(\mathbb{H})$ 中. 这就表明 $C(\mathbb{H}) = \{a\mathbf{1}|\ a \in \mathbb{R}\}$. 我们可以建立自然的同构

$$\sigma : \mathbb{R} \longrightarrow C(\mathbb{H}), \quad a \to a\mathbf{1}.$$

具体验证留给读者. ■

例 2.2.8 (**内自同构**) 设 H 是除环, $q \in H$ 是给定的非零元. 我们定义映射

$$\sigma_q : H \longrightarrow H, \quad x \to q\cdot x\cdot q^{-1}.$$

对任何 $x, y \in H$, 显然有
(1) $\sigma_q(x+y) = q\cdot(x+y)\cdot q^{-1} = (q\cdot x + q\cdot y)\cdot q^{-1} = q\cdot x\cdot q^{-1} + q\cdot y\cdot q^{-1} = \sigma(x)+\sigma(y)$.
(2) $\sigma_q(x\cdot y) = q\cdot x\cdot y\cdot q^{-1} = q\cdot x\cdot(q^{-1}\cdot q)\cdot y\cdot q^{-1} = (q\cdot x\cdot q^{-1})\cdot(q\cdot y\cdot q^{-1}) = \sigma(x)\sigma(y)$.
因此 σ_q 是除环同态. 另一方面, 考虑 q^{-1} 所诱导的同态

$$\sigma_{q^{-1}} H \longrightarrow H, \quad x \to q^{-1}\cdot x\cdot q.$$

我们有

$$\sigma_q\sigma_{q^{-1}} = \mathrm{Id}_H, \quad \sigma_{q^{-1}}\sigma_q = \mathrm{Id}_H.$$

因此 σ 是除环 H 的自同构. 这种自同构也称为*内自同构* (Inner automorphism).

显然, 如果 H 是域的话, 上述同构就是恒等映射. 但对体来说, 内自同构未必是恒同的. 比如在四元数体 $\mathbb{H}$ 中, 取 $q = \mathbf{i}$, 则有非恒同映射

$$\sigma_q : \mathbb{H} \longrightarrow \mathbb{H}, \quad a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \to a\mathbf{1} + b\mathbf{i} - c\mathbf{j} - d\mathbf{k}.$$

例 2.2.9 (**共轭映射**) 考虑 $\mathbb{H}$ 的共轭映射

$$\sigma : \mathbb{H} \longrightarrow \mathbb{H}, \quad a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \to a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}.$$

对任何 $u, v \in \mathbb{H}$, 我们有

$$\sigma(u+v) = \sigma(u) + \sigma(v), \tag{2-1}$$

我们可以验证如下关系式

$$\sigma(u\cdot v) = \sigma(v)\cdot\sigma(u). \tag{2-2}$$

请注意, 通常 $\sigma(v)\cdot\sigma(u) \neq \sigma(u)\cdot\sigma(v)$. 因此共轭映射不是同态! 我们把满足式 (2-1) 和 (2-2) 的映射称为*反同态*. ■

2.2.3 除环的基本性质

域的很多性质在一般的除环中也成立, 并且证明是完全类似的. 比如命题 (1.4.1) 和命题 (1.6.1) 在除环中也成立. 为方便读者, 这里罗列一下 (我们暂时不讨论特征的问题).

命题 2.2.1 *设 H 是除环, 我们有如下性质:*
(1) *零元和幺元都是唯一的, 每个非零元的加法 (乘法) 逆元也是唯一的.*
(2) *对任何 $a \in H$, 都有 $0\cdot a = a\cdot 0 = 0$.*

(3) 对任何 $a \in H$, 都有 $(-1)\cdot a = a\cdot(-1) = -a$.
(4) 对任何 $a, b \in H$, 都有 $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$.
(5) $0 \neq 1$ 以及 $-0 = 0$, $1^{-1} = 1$ 和 $(-1)^{-1} = -1$.
(6) (无零因子) 若 $ab = 0$, 则要么 $a = 0$, 要么 $b = 0$.
(7) (消去律) 如果 $a\cdot c = b\cdot c$, 且 $c \neq 0$, 那么 $a = b$.
(8) 任意多个子除环的交也是子除环.

设 $\sigma : F \to H$ 是非平凡的除环同构. 我们有
(9) $\sigma(0) = 0$, $\sigma(1) = 1$,
(10) 对任何非零元 $x \in E$, 我们有

$$\sigma(-x) = -\sigma(x), \quad \sigma(x^{-1}) = \sigma(x)^{-1}.$$

特别地, 非零元的像必定非零.
(11) σ 是单同态, 像集 $\mathrm{Im}\sigma$ 是 F 的子除环.
(12) $\sigma : F \to \mathrm{Im}\sigma$ 是除环同构.

注 2.2.3　由于体没有乘法交换律，一些在域中平凡的性质在体中则未必显而易见, 甚至未必正确. 比如在除环 H 中,
(1) 我们有以下恒等式 (见习题 2.8)

$$(a\cdot b)^{-1} = b^{-1}\cdot a^{-1}, \quad \forall a, b \in H.$$

如果 H 不是域的话, 上式右边 a^{-1} 和 b^{-1} 的位置不能随便调换.
(2) 对于一个等式 $a = b$, 我们两边乘以元素 c 时, 一定要注意必须同时右乘或同时左乘, 这样才能保持等号成立, 即 $ac = bc$ 或 $ca = cb$.
(3) 在体中, 我们实际上能定义两种除法$a\cdot b^{-1}$ 与 $b^{-1}\cdot a$. 它们通常不相同, 所以不能混淆地写成 $\frac{a}{b}$ (但在域中通常不会有歧义). ■

类似地, 给定非空子集 $S \subseteq H$, 我们也可以定义由 S 生成的子除环, 也就是 S 中的元素通过加、乘及求逆运算得到的各种可能的元素的全体. 特别地, 也可以定义素域和特征的概念. 此处不再赘述. 现在我们希望研究除环的中心和除环本身相差多大. 对域来说, 这两者是相同的. 我们给出如下结论.

定理 2.2.1　设 H 是一个体, $a \in F$ 是中心以外的元素. 设

$$S_a = \{q\cdot a\cdot q^{-1} \mid q \in H,\ q \neq 0\}.$$

那么 H 由 S_a 生成, 这里 S_a 称为 a 的共轭类.

为证此结论, 我们需要一个引理.

引理 2.2.1　设 $a, b \in H$ 满足 $a\cdot b \neq b\cdot a$. 令 $c = (b-1)^{-1}\cdot a\cdot(b-1)$, 则

$$b = (a-c)\cdot(b^{-1}\cdot a\cdot b - c)^{-1}.$$

特别地, b 落在由 S_a 生成的子除环中 (定义见定理 2.2.1).

证明　这来自于直接计算. 具体如下:

$$b\cdot(b^{-1}\cdot a\cdot b - c) = a\cdot b - b\cdot c = a\cdot b - ((b-1)\cdot c + 1\cdot c)$$

$$= a \cdot b - (a \cdot (b-1) + c) = (a \cdot b - a \cdot (b-1)) - c$$
$$= a - c.$$

现在我们说明 $b^{-1} \cdot a \cdot b - c \neq 0$. 若不然, 由上式推出 $a = c$, 因而由 c 的定义得 $(b-1)a = a(b-1)$, 整理即得 $ab = ba$, 与命题条件矛盾! 由此即得结论. ■

注 2.2.4　我们也可以证明上述结论中 $b^{-1} \cdot a \cdot b - c \neq 0$. 若不然可得

$$(b-1)b^{-1}ab = a(b-1).$$

上式左边等于 $(1-b^{-1})ab = ab - b^{-1}ab = a(b-1) + a - b^{-1}ab$, 因此就得到等式 $a = b^{-1}ab$, 即 $ab = ba$, 矛盾! ■

引理 2.2.2　*设 K 是由 S_a 生成的子除环. 我们有*
(1) *如果 $K \neq H$, 那么对任何 $b \in H \backslash K$, b 与 K 中的任何元素都乘法可交换.*
(2) *K 中必有两个元素乘法不可交换.*

证明　(1) 如果 b 与 S_a 中每个元素乘法可交换, 那么它当然也和 K 中每个元素交换 (因为 K 是由 S_a 生成的). 不妨假设 b 与 K 中某个元素乘法不可交换, 那么由上讨论, 它和 S_a 中某元素, 不妨设为 a, 乘法不可交换. 因此由引理 2.2.1, $b \in K$, 这与 b 的选取矛盾!

(2) 假设 K 中任何两个元素乘法可交换. 任取 $y \in K$, $z \in H$. 如果 $z \notin K$, 则由 (1) 知, $y \cdot z = z \cdot y$. 如果 $z \in K$, 则由假设亦知 y, z 乘法可交换. 因此 $y \in C(H)$, 从而 $K \subseteq C(H)$, 矛盾! ■

定理 2.2.1 的证明: 我们相当于要证 $K = H$. 不妨假设 $K \neq H$, 即存在元素 $x \in H \backslash K$. 首先由引理 2.2.2 (2), 可找到两个元素 $b_1, b_2 \in K$, 使得 $b_1 \cdot b_2 \neq b_2 \cdot b_1$. 因为 x, $x \cdot b_1 \notin K$, 故由引理 2.2.2 (1), 它们和 K 中元素乘法可交换. 这样, 我们有

$$(x \cdot b_1) \cdot b_2 = b_2 \cdot (x \cdot b_1) = (b_2 \cdot x) \cdot b_1 = (x \cdot b_2) \cdot b_1,$$

在上式两端左乘 x^{-1}, 即得 $b_1 \cdot b_2 = b_2 \cdot b_1$, 矛盾! ■

我们这里介绍一个和除环有关的著名结论.

定理 2.2.2 (Wedderburn **小定理**)　*有限除环必定是域.*

它有一个简洁优美的初等证明 (由 Ernst Witt 于 1931 年给出). 限于本书的篇幅, 我们不再详细介绍, 而是将它放在习题 2.12 至习题 2.15 中.

关于除环的其他性质, 我们也不再详细介绍了. 有兴趣的读者可以参看 [HW10, 第一章, §9 – §11]. 我们将其中一部分内容留作习题供读者练习.

2.3 整环与交换幺环

在研究了体之后, 我们希望了解其他的代数对象, 比如前面所提到的整数环等等. 很多熟知的代数对象都满足乘法交换律, 但一般没有乘法逆元. 相对而言, 有乘法交换律的代数对象往往比没有交换律的对象有更好的性质 (回想一下四元数体和数域的比较, 或者数域和矩阵环的比较). 因此我们现在把研究目光放在有乘法交换律的代数对象上.

2.3.1 定义

定义 2.3.1 设 R 是至少含两个元素的集合, 并有加法"+" 和"·" 乘法两种运算. 假设 R 除了乘法逆元存在性公理 (M4) 外, 满足其他所有公理 (即 (A0-A4), (M0-M3), (AM)), 则称 R 是交换幺环 (Commutative ring).

乘法逆元存在性公理是保证除法运算的, 交换幺环失去了这条公理, 很多域上的性质就不再能保留下来. 比如有理数域上的线性方程 $ax = b$ 总是有解, 但是在整数环上, 这个方程则未必有解. 初等数论的整除概念以及整除理论也就是由此引出的.

我们希望用一些其他公理替代公理 (M4), 尽量弥补公理 (M4) 缺损所带来的损失. 让我们回顾域上的一条性质:

(**乘法**) **消去律**: 设 $a, b, c \in R$, $c \neq 0$. 如果 $ac = bc$, 则 $a = b$.

当公理 (M4) 成立时, 上述消去律很容易得到. 但是在交换幺环中, 消去律未必存在. 因此我们可以先考察如下类型的交换幺环.

定义 2.3.2 如果交换幺环 R 满足消去律, 那么我们称 R 为整环 (Domain).

注 2.3.1 上面的乘法交换律也称为右消去律. 同样也有左消去律, 即由 $ca = cb$ 推知 $a = b$. 但由于在交换幺环中乘法满足交换律, 因此左消去律和右消去律没有差别, 所以我们不再强调"左"和"右"了. ■

今后我们会定义更一般的环. 为读者方便, 我们这里也罗列一下这些概念. 后面我们再考察这样的对象. 这一章节主要关心整环和交换幺环.

定义 2.3.3 如果 R 是非空集合, 并有加法"+" 和"·" 乘法两种运算, 满足公理 (A0-A4), (M0,M1), (AM), 我们就称 R 为环. 进一步, 如果一个环 R 有幺元 (即满足公理 (M3)), 则称幺环.

容易看到

$$\text{域} \subseteq \text{整环} \subseteq \text{交换幺环} \subseteq \text{幺环} \subseteq \text{环}.$$

我们也可以定义环同态和环同构的概念.

定义 2.3.4 设 $\sigma : R \to R'$ 是环之间的映射. 如果它满足以下诸条件, 则称之为环同态:

(1) $\sigma(x + y) = \sigma(x) + \sigma(y)$, $\forall x, y \in R$.

(2) $\sigma(x \cdot y) = \sigma(x) \cdot \sigma(y)$, $\forall x, y \in R$.

进一步, 如果 σ 是单射 (满射), 我们就说它是单同态 (满同态). 如果存在同态 $\tau : R' \to R$ 使得 $\sigma\tau = \mathrm{Id}_{R'}$ 及 $\tau\sigma = \mathrm{Id}_R$, 则称 σ 为同构, $\tau = \sigma^{-1}$ 为逆映射, 有时简记该同构为 $R \cong R'$. 环 R 到自身的同构简称为自同构.

2.3.2 例子

我们先回顾几个经典的例子.

例 2.3.1 (1) 如上所说, 所有的域都是整环.

(2) 整数环 $(\mathbb{Z}, +, -)$ 是整环.

(3) 有理系数多项式环 $\mathbb{Q}[x]$ (类似地, $\mathbb{R}[x]$, $\mathbb{C}[x]$) 是整环. ■

下面介绍一个重要的环, 它在代数数论中具有重要的意义.

例 2.3.2 (高斯整数环)

$$\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}.$$

我们来验证它在通常加法和乘法下构成整环. 首先, $0, 1 \in \mathbb{Z}[\sqrt{-1}]$ 是显然的. 加法和乘法的封闭性以及加法的逆元存在性可以从下式直接看出来:

$$\begin{aligned}(a + b\sqrt{-1}) + (c + d\sqrt{-1}) &= (a + c) + (b + d)\sqrt{-1},\\ (a + b\sqrt{-1}) \cdot (c + d\sqrt{-1}) &= (ac - bd) + (bc + ad)\sqrt{-1},\\ -(a + b\sqrt{-1}) &= (-a) + (-b)\sqrt{-1}.\end{aligned}$$

■

注意到 $\mathbb{Z}[\sqrt{-1}] \subseteq \mathbb{Q}[\sqrt{-1}]$, 所以它自然满足加法和乘法的结合律、交换律、分配律和消去律.

类似地, 也可以定义如下整环. 设 d 是不含平方因子的整数,

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

例 2.3.3 (模 N 的剩余类环) 设 $\mathbb{Z}_N$ 同例 2.1.5. 它是交换环, 并且当 N 是素数时, 它也是域. 如果 N 不是素数, 我们来证明 $\mathbb{Z}_N$ 不是整环.

假设 $N = n_1 n_2$, 其中 $n_1, n_2 > 1$. 注意到 $[n_1] \neq [0]$, 但是

$$[n_1] \cdot [n_2] = [0] = [0] \cdot [n_2].$$

这说明消去律不成立. ■

例 2.3.4 (对角矩阵) 设 F 是数域, 考虑矩阵环 $M_n(F)$ (见例 2.1.3) 中的子集合, 即所有对角阵全体

$$R = \left\{ \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix} \in M_n(F) \,\middle|\, a_i \in F,\ i = 1, \cdots, n \right\}$$

R 的零元是零阵, 幺元是单位阵. 容易验证 R 是交换幺环 (尽管矩阵环 $M_n(F)$ 不满足乘法交换). 但当 $n > 1$ 时, R 不是整环. 比如取

$$E_i = \begin{pmatrix} 0 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \ddots \\ & & & & 0 \end{pmatrix} \quad \text{第 } i \text{ 行}$$

当 $i \neq j$ 时, 我们有 $E_i \cdot E_j = 0 \cdot E_j$, 但 $E_i \neq E_j$. 因此不满足乘法消去律. 这个环其实可以看作数域 F 上的 n 维向量空间. ■

本节最后, 我们举几个例子简要说明交换幺环的同态一般不满足命题 2.2.1 的诸性质. 我们将环同态性质放到后面再详细探讨.

例 2.3.5 (**同余映射**)

$$\sigma : \mathbb{Z} \longrightarrow \mathbb{Z}_N, \quad n \to [n].$$

它不是单同态, 比如 $\sigma(0) = \sigma(N) = [0]$. 这也说明非零元的像可能为零元. ■

例 2.3.6 考虑例 2.3.4 的定义在数域 F 上的对角矩阵环 R. 我们有环同态

$$\sigma : F \longrightarrow R, \quad a \to \begin{pmatrix} a & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix}$$

虽然它是单同态, 但 $\sigma(1_F)$ 却不是 R 的幺元. ■

2.3.3 基本性质

我们来考察一下, 除环的基本性质 (命题2.2.1) 中还有哪些可以在交换幺环或整环中保留下来, 哪些不再成立.

命题 2.3.1 *设 R 是交换幺环, 我们有如下性质:*
(1) *零元和幺元都是唯一的, 每个非零元的加法 (乘法) 逆元也是唯一的.*
(2) *对任何 $a \in R$, 都有 $0 \cdot a = a \cdot 0 = 0$.*
(3) *对任何 $a \in R$, 都有 $(-1) \cdot a = a \cdot (-1) = -a$.*
(4) *对任何 $a, b \in R$, 都有 $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.*
(5) *$0 \neq 1$ 以及 $-0 = 0$, $1^{-1} = 1$ 和 $(-1)^{-1} = -1$.*

无论如何交换幺环未必满足命题2.2.1 中的无零因子性和消去律. 下面我们要证明这两条性质其实是等价的. 为此我们给出如下定义.

定义 2.3.5 *设 R 是交换幺环, $a, b \in R$ 是非零元满足 $a \cdot b = 0$, 那么我们称 a, b 为 R 的零因子* (Zero divisor).

注 2.3.2 严格地说, 上述定义中, a 称为左零因子, b 称为右零因子. 但是在交换幺环中, 乘法满足交换律, 因此我们不再区分左右的限制. ■

例 2.3.7 (1) 整数环 $\mathbb{Z}$ 和有理系数多项式环 $\mathbb{Q}[x]$ (类似地, $\mathbb{R}[x], \mathbb{C}[x]$) 都没有零因子.
(2) 模 N 的剩余类环在 N 不是素数时必有零因子. 此时设 $N = n_1 n_2$, $n_1, n_2 > 1$, 则

$$[n_1] \cdot [n_2] = [0], \quad [n_i] \neq [0],$$

从而 $[n_1], [n_2]$ 都是零因子.
(3) 例 2.3.4 的对角阵构成的交换幺环中, E_i 都是零因子. ■

命题 2.3.2 *R 是整环当且仅当 R 是无零因子的交换幺环.*

证明 ($\Longrightarrow$) 已知R 是整环, 我们证明 R 不含零因子. 不妨假设存在零因子 a, b 使得 $a \cdot b = 0$. 因此我们有

$$0 = a \cdot b = a \cdot b - 0 \cdot b,$$

因而 $a \cdot b = 0 \cdot b$. 因此由消去律以及 $b \neq 0$ 推得 $a = 0$, 矛盾! 故 R 没有零因子.

($\Longleftarrow$) 已知交换幺环 R 不含零因子, 我们来证它是整环, 即满足消去律. 假设 $a \cdot c = b \cdot c$ ($c \neq 0$), 则得

$$(a - b) \cdot c = a \cdot c - b \cdot c = 0.$$

由于 R 无零因子且 $c \neq 0$, 所以 $a - b = 0$, 即 $a = b$. ■

类似除环中的 Wedderburn 小定理, 我们也有如下关于整环的结论.

命题 2.3.3 *有限整环必是域.*

证明 设 $R = \{a_1, a_2, \cdots, a_n\}$ 是有限整环, $a_1 = 1$. 我们只需要证明 R 中每个非零元都有逆元. 对任何非零元 $a \in R$, 我们先说明

$$aa_1, aa_2, \cdots, aa_n$$

两两不同. 假设 $aa_i = aa_j$, 我们用消去律得到 $a_i = a_j$, 即 $i = j$.

因此诸 aa_i 不重复地跑遍 R 中所有元素. 这样, 存在某个 a_i, 使得 $aa_i = 1$. 这就说明每个非零元都有乘法逆元, 因而 R 是域. ■

推论 2.3.1 (**推广的费马小定理**) *设 R 是有限整环, 那么对任何非零元 $a \in R$ 都有 $a^{n-1} = 1$, 这里 n 是 R 中元素个数.*

证明 采用命题 2.3.3 的证明中的所有记号与假设. 不妨设 $a_n = 0$. 现在我们有相同的集合

$$\{a_1, a_2, \cdots, a_{n-1}\} = R \setminus \{0\} = \{aa_1, aa_2, \cdots, aa_{n-1}\}.$$

因此

$$\prod_{i=1}^{n-1} a_i = \prod_{i=1}^{n-1} (aa_i) = a^{n-1} \prod_{i=1}^{n-1} a_i.$$

因为 $a_i \neq 0$ ($i = 1, \cdots, n-1$), 且 R 是整环, 所以 $a_1 \cdots a_{n-1} \neq 0$. 对上面的等式应用消去律, 即得 $a^{n-1} = 1$. ■

在上述推论中取模素数 p 的剩余类域 $R = \mathbb{F}_p$, 即得费马小定理 $[a^{p-1}] = [1]$.

2.3.4 构造方法 (I): 子幺环

以下几节, 我们尝试从各种不同的途径来构造交换幺环和整环.

模仿子域的概念, 我们也可以定义环中的子环.

定义 2.3.6 *设 R 是环, L 是 R 的非空子集. 如果 L 在 R 的运算下也构成环, 我们就称其为 R 的子环. 如果 R 是幺环, 并且 L 是包含 1_R 的子环, 则称 L 是 R 的子幺环.*

注 2.3.3 (1) 交换幺环的子幺环直接继承了乘法交换性.
(2) 子幺环定义中的条件"L 包含单位元 1_R" 非常重要. 我们下面的例子表明, 一个交换幺环 R 的子环 L 可以是幺环, 但是其幺元 $1_L \neq 1_R$, 因而不是子幺环. ■

例 2.3.8 (**非子幺环**)　考虑例 2.3.4 的 2 阶对角阵构成的交换幺环

$$R=\left\{\left.\begin{pmatrix} a & \\ & b \end{pmatrix}\in M_2(F)\right| a,b\in F\right\}$$

以及它的子集合

$$L=\left\{\left.\begin{pmatrix} a & \\ & 0 \end{pmatrix}\in M_2(F)\right| a\in F\right\}$$

可以验证 R 与 L 都是交换幺环, 它们的单位元分别是

$$1_R=\begin{pmatrix} 1 & \\ & 1 \end{pmatrix},\quad 1_L=\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$$

因此 L只是 R 的子环, 而不是子幺环. ■

注 2.3.4　在除环中, 我们没有强调子除环和除环本身的幺元一致, 这是因为该情形下很容易利用乘法逆元存在性证明这件事. 假设 $E\subseteq F$ 是除环 F 的子除环. 因为 1_E 也是 F 中的非零元, 所以

$$1_F=1_E\cdot 1_E^{-1}=(1_E\cdot 1_E)\cdot 1_E^{-1}=1_E\cdot(1_E\cdot 1_E^{-1})=1_E\cdot 1_F=1_E.$$

例 2.3.9　(1) $\mathbb{Z}\subseteq\mathbb{Q}$ 是 $\mathbb{Q}$ 的子幺环.
(2) $\mathbb{Z}\subseteq\mathbb{Z}[\sqrt{d}]$ 是 $\mathbb{Z}[\sqrt{d}]$ 的子幺环.
(3)

$$R=\left\{\left.\begin{pmatrix} a & \\ & b \end{pmatrix}\in M_2(\mathbb{Q})\right| a,b\in\mathbb{Q}\right\}$$

有子幺环

$$L=\left\{\left.\begin{pmatrix} a & \\ & b \end{pmatrix}\in M_2(\mathbb{Q})\right| a,b\in\mathbb{Z}\right\}$$

我们留给读者验证. ■

类似子域的判定条件, 我们也可以给出子环的判定条件.

命题 2.3.4　*设 R 是环, L 是 R 的非空子集, 则 L 是 R 的子环的充分必要条件为: 对任何 $a,b\in L$, 总有*
(1) $a-b\in L$,
(2) $a\cdot b\in L$.

特别地, 如果 R 是幺环, 并且 L 包含 1_R, 那么 L 是 R 的子幺环当且仅当它满足上述两个条件.

证明　类似命题 1.5.1 的证明. 但请注意, 此处的条件 (2) 是乘法封闭性条件, 而不是命题 1.5.1 中的除法封闭性条件 (此时没有除法的概念). ■

命题 2.3.5　*整环的子幺环必为整环. 特别地, 域中的子幺环总是整环.*

证明　因为消去律在原来的整环中已经成立, 因而在子幺环中自然成立. ■

我们也可以模仿域的情形定义由某个非空子集生成的子幺环.

定义 2.3.7　设 R 是环, $S \subseteq R$ 是非空子集, 所有包含 S 的子环的交也是子环 (留给读者验证), 称作由 S 生成的子环. 进一步, 如果 R 是幺环, S 包含 1_R, 则由 S 生成的子环也叫做子幺环.

如果取 $S = \{1_R\}$, 我们就得到最小的子幺环

$$L = \{n1_R |\, n \in \mathbb{Z}\}. \tag{2-3}$$

这里 $n1_R$ 定义类似于式 (1.5.1). 当 R 是整环时, 这个子幺环被称为素环 (由命题 2.3.5, 它也是整环).

命题 2.3.6　设 R 是整环, 则以下条件彼此等价:
(1) R 的素环是有限整环 (因而是有限域),
(2) 存在素数 p, 使得 $p1 = 0$.
条件成立时, 上述 p 是最小的满足 $p1 = 0$ 的正整数, 且其素环同构于 $\mathbb{F}_p$.

证明　证明与命题 1.5.3 类似. 为方便读者, 我们利用已知结论给出一个简化证明.

(1) $\Longrightarrow$ (2) 由命题 2.3.5, 它是有限域. 由命题 1.5.3 即得 (2).

(2) $\Longrightarrow$ (1) 由素环的定义式 (2-3) 立知它是有限整环. ■

因此我们也可以定义整环的特征: 如果对某个素数 p 有 $p1_R = 0$, 就称整环有特征 p; 否则就称它有特征 0. 我们简记特征为 $\mathrm{ch}(R)$.

例 2.3.10　$\mathbb{Z}$, $\mathbb{Z}[\sqrt{d}]$ 的特征都是零. ■

例 2.3.11　我们举例说明非整环的交换幺环未必存在素数满足命题 2.3.6 (2). 比如 $R = \mathbb{Z}_6$ 中满足 $n[1] = [0]$ 的最小正整数 $n = 6$. ■

2.3.5 构造方法 (II): 整环与分式域

以下总假设 R 是整环, $R^* = R\backslash\{0\}$. 我们的目标是要构造一个域 F, 使得 $R \subseteq F$, 并且这样的域是最小的. 最简单的例子是 $R = \mathbb{Z}$, 我们可以找到这样的域 $\mathbb{Q}$. 整环和域的主要差别在于乘法逆元, 因此这个构造的关键是, 如何引进乘法逆元. 考虑集合

$$R \times R^* = \{(a, b) |\, a \in R,\ b \in R^*\}$$

引理 2.3.1　定义 $R \times R^*$ 上的关系

$$(a, b) \sim (c, d) \Longleftrightarrow ad = bc,$$

则它是等价关系.

证明　(1) 自反性: 因为 $ab = ba$, 所以 $(a, b) \sim (a, b)$.
(2) 对称性: 设 $(a, b) \sim (c, d)$, 则 $ad = bc$, 因而 $cb = da$, 即 $(c, d) = (a, b)$.
(3) 传递性: 设 $(a, b) \sim (c, d)$, $(c, d) \sim (e, f)$, 即 $ad = bc$, $cf = de$. 如果 $c = 0$, 则由 $d \neq 0$ 推出 $a = e = 0$, 从而 $af = be$, 即 $(a, b) \sim (e, f)$. 今假设 $c \neq 0$. 此时

$$(ad)(cf) = (bc)(de).$$

由消去律可得 $af = be$, 即 $(a, b) \sim (e, f)$. ■

定义等价类

$$\left[\frac{a}{b}\right] := \{(c,d)|\ (a,b) \sim (c,d)\}$$

我们把所有等价类全体记为 F. 现在定义 F 上的加法运算

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] := \left[\frac{ad+bc}{bd}\right],$$

以及乘法运算

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] := \left[\frac{ac}{bd}\right].$$

引理 2.3.2　上述加法和乘法运算是合理的.

证明　假设 $\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right]$, $\left[\frac{c}{d}\right] = \left[\frac{c'}{d'}\right]$, 即 $a'b = ab'$, $c'd = cd'$.

$$(ad+bc)b'd' = adb'd' + bcb'd' = (ab')(dd') + (cd')(b'b) = (a'b)(dd') + (c'd)(b'b) = (a'd' + b'c')bd,$$

因而

$$\left[\frac{ad+bc}{bd}\right] = \left[\frac{a'd'+b'c'}{b'd'}\right].$$

同样地,

$$(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd)$$

蕴含着 $\left[\frac{ac}{bd}\right] = \left[\frac{a'c'}{b'd'}\right]$. ■

定理 2.3.1　F 在上述两种运算下构成域, 并且存在单同态

$$\sigma : R \longrightarrow F, \quad a \to \left[\frac{a}{1}\right].$$

证明　先验证 F 满足结合律公理 $(A1)(M1)$.

$$\left(\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right]\right) + \left[\frac{e}{f}\right] = \left[\frac{ad+bc}{bd}\right] + \left[\frac{e}{f}\right] = \left[\frac{(ad+bc)f + (bd)e}{bdf}\right] = \left[\frac{adf+bcf+bde}{bdf}\right],$$

$$\left[\frac{a}{b}\right] + \left(\left[\frac{c}{d}\right] + \left[\frac{e}{f}\right]\right) = \left[\frac{a}{b}\right] + \left[\frac{cf+de}{df}\right] = \left[\frac{a(df) + b(cf+de)}{bdf}\right] = \left[\frac{adf+bcf+bde}{bdf}\right],$$

$$\left(\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right]\right) \cdot \left[\frac{e}{f}\right] = \left[\frac{ac}{bd}\right] \cdot \left[\frac{e}{f}\right] = \left[\frac{ace}{bdf}\right],$$

$$\left[\frac{a}{b}\right] \cdot \left(\left[\frac{c}{d}\right] \cdot \left[\frac{e}{f}\right]\right) = \left[\frac{a}{b}\right] \cdot \left[\frac{ce}{df}\right] = \left[\frac{ace}{bdf}\right].$$

再验证交换律公理 $(A2)(M2)$.

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad+bc}{bd}\right] = \left[\frac{cb+da}{db}\right] = \left[\frac{c}{d}\right] + \left[\frac{a}{b}\right],$$

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right] = \left[\frac{ca}{db}\right] = \left[\frac{c}{d}\right] \cdot \left[\frac{a}{b}\right].$$

零元和幺元的验证如下

$$\left[\frac{0}{1}\right] + \left[\frac{a}{b}\right] = \left[\frac{0b+1a}{1 \cdot b}\right] = \left[\frac{a}{b}\right],$$

$$\left[\frac{1}{1}\right]\cdot\left[\frac{a}{b}\right]=\left[\frac{1\cdot a}{1\cdot b}\right]=\left[\frac{a}{b}\right]$$

加法逆元存在

$$\left[\frac{-a}{b}\right]+\left[\frac{a}{b}\right]=\left[\frac{(-a)+a}{b}\right]=\left[\frac{0}{b}\right]=\left[\frac{0}{1}\right].$$

乘法逆元存在

$$\left[\frac{a}{b}\right]\cdot\left[\frac{b}{a}\right]=\left[\frac{a\cdot b}{b\cdot a}\right]=\left[\frac{ab}{ab}\right]=\left[\frac{1}{1}\right].$$

分配律公理 (AM):

$$\left(\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right]\right)\cdot\left[\frac{e}{f}\right]=\left[\frac{ad+bc}{bd}\right]\cdot\left[\frac{e}{f}\right]=\left[\frac{ade+bce}{bdf}\right],$$
$$\left[\frac{a}{b}\right]\cdot\left[\frac{e}{f}\right]+\left[\frac{c}{d}\right]\cdot\left[\frac{e}{f}\right]=\left[\frac{ae}{bf}\right]+\left[\frac{ce}{df}\right]=\left[\frac{ade+bce}{bdf}\right].$$

这样, 我们就证明了 F 是域. 我们定义映射

$$\sigma:R\longrightarrow F,\quad a\to\left[\frac{a}{1}\right].$$

注意到

$$\sigma(a+b)=\left[\frac{a+b}{1}\right]=\left[\frac{a}{1}\right]+\left[\frac{b}{1}\right]=\sigma(a)+\sigma(b),\quad \sigma(a\cdot b)=\left[\frac{a\cdot b}{1}\right]=\left[\frac{a}{1}\right]\cdot\left[\frac{b}{1}\right]=\sigma(a)\cdot\sigma(b).$$

因此 σ 是同态. 另一方面, 假设 $\sigma(a)=\sigma(b)$, 则 $\left[\frac{a}{1}\right]=\left[\frac{b}{1}\right]$. 由等价类定义得 $a=b$. 这就证明了 σ 是单同态. ■

上述构造的域 F 称作 R 的分式域(Field of fractions) 或商域 (field of quotients) .

推论 2.3.2 *设 R 是含于域 E 中的整环, F 是 R 的分式域, 那么存在域的单同态 $\phi:F\to E$. 特别地, 我们可以说 F 是包含 R 的最小域.*

证明 定义映射

$$\phi:F\longrightarrow E,\quad \left[\frac{a}{b}\right]\to a\cdot b^{-1}.$$

首先说明这个映射是合理的. 设 $\left[\frac{a}{b}\right]=\left[\frac{a'}{b'}\right]$, 即 $ab'=ba'$. 因而

$$a\cdot b^{-1}=ab'\cdot(b')^{-1}\cdot b^{-1}=ba'\cdot(b')^{-1}\cdot b^{-1}=a'\cdot(b')^{-1}.$$

容易验证 ϕ 是域同态, 因而是单同态. ■

上面的分式域 F 实际上同构于 E 的子域

$$F'=\{a\cdot b^{-1}|\ a\in R,b\in R^*\},$$

这里 $R^*=R\setminus\{0\}$.

推论 2.3.3 *整环的分式域在同构意义下是唯一的, 并且它和该整环有相同的特征.*

例 2.3.12 (1) $\mathbb{Z}[\sqrt{d}]$ 的分式域同构于二次扩域 $\mathbb{Q}(\sqrt{d})$.
(2) 有理系数多项式环 $\mathbb{Q}[x]$ 的分式域同构于有理函数 $\mathbb{Q}(x)$. ■

2.3.6 构造方法 (III): 交换幺环上的多项式环

这一节我们总假设 R 是交换幺环. 我们希望能定义环 R 上的多项式环

$$R = \{a_0 + a_1x + \cdots + a_nx^n |\ a_i \in R,\ \forall i\}.$$

在 $R = \mathbb{Q}$ ($\mathbb{R}$, $\mathbb{C}$) 时, 我们已经接触过多项式环 $\mathbb{Q}[x]$ ($\mathbb{R}[x]$,$\mathbb{C}[x]$), 但是对于不定元 x 的概念却没有一个严格清晰的理解. 下面我们将采用一种稍微抽象的方式, 来严格地定义不定元.

考虑无限序列

$$\alpha = (a_0, a_1, a_2, \cdots)$$

全体构成的集合, 我们记作 $R[[x]]$. 我们定义 $R[[x]]$ 上的加法和乘法运算 (取 $\beta = (b_0, b_1, b_2, \cdots)$):

$$\begin{aligned}\alpha + \beta :=& (a_0 + b_0, a_1 + b_1, a_2, b_2, \cdots,),\\ \alpha \cdot \beta :=& (c_0, c_1, c_2, \cdots),\end{aligned}$$

这里

$$c_n = a_0b_n + a_1b_{n-1} + \cdots + a_nb_0 = \sum_{i+j=n} a_ib_j.$$

引理 2.3.3 *$R[[x]]$ 在上述运算下构成交换幺环, 其幺元 $1 = (1, 0, 0, \cdots)$. 我们称 $R[[x]]$ 为一元形式幂级数环* (Ring of formal power series in one indeterminate).

证明 对上述定义的加法运算, 很容易验证其满足 (A0-A4), 这里不再赘述. 此外, 容易看到

$$(1, 0, 0, \cdots) \cdot (a_0, a_1, a_2, \cdots) = (a_0, a_1, a_2, \cdots) \cdot (1, 0, 0, \cdots) = (a_0, a_1, a_2, \cdots).$$

下面我们先来验证分配律. 设 α, β 同前, $\gamma = (r_0, r_1, r_2, \cdots)$.

$$(\alpha + \beta) \cdot \gamma = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \cdots) \cdot \gamma = ((a_0 + b_0)\gamma_0, \cdots, \sum_{i+j=n} (a_i + b_i)r_j, \cdots).$$

另一方面,

$$\begin{aligned}\alpha \cdot \gamma + \beta \cdot \gamma &= (a_0r_0, \cdots, \sum_{i+j=n} a_ir_j, \cdots) + (b_0r_0, \cdots, \sum_{i+j=n} b_ir_j, \cdots)\\ &= ((a_0 + b_0)r_0, \cdots, \sum_{i+j=n} (a_i + b_i)r_j, \cdots).\end{aligned}$$

其次验证乘法交换律:

$$\alpha \cdot \beta = (a_0b_0, \cdots, \sum_{i+j=n} a_ib_j, \cdots) = (b_0a_0, \cdots, \sum_{i+j=n} b_ia_j, \cdots) = \beta \cdot \alpha.$$

最后验证乘法结合律 $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$. 设

$$\alpha = (a_0, \cdots, a_i, \cdots), \quad \beta = (b_0, \cdots, b_j, \cdots), \quad \gamma = (r_0, \cdots, r_k, \cdots).$$

于是

$$(\alpha \cdot \beta) \cdot \gamma = (c_0, \cdots, c_l, \cdots) \cdot \gamma = (c'_0, \cdots, c'_m, \cdots),$$

这里 $c_l = \sum\limits_{i+j=l} a_i b_j$, $c'_m = \sum\limits_{l+k=m} c_l r_k = \sum\limits_{i+j+k=m} a_i b_j r_k$. 另一方面,

$$\alpha \cdot (\beta \cdot \gamma) = \alpha \cdot (d_0, \cdots, d_l, \cdots) = (d'_0, \cdots, d'_m, \cdots),$$

这里 $d_l = \sum\limits_{j+k=l} b_j c_k$, $d'_m = \sum\limits_{i+l=m} a_i d_l = \sum\limits_{i+j+k=m} a_i b_j r_k$. ■

注 2.3.5 (1) $R_0 = \{(a_0, 0, \cdots) | \, a_0 \in R\}$ 是 $R[[x]]$ 的幺子环, 且同构于 R. 因此以后为了方便起见, 我们将 a_0 和 $(a_0, 0, 0\cdots)$ 等同起来.
(2) $R[[x]]$ 可以定义如下类似"数乘"运算: $a \cdot \alpha := (aa_0, aa_1, aa_2, \cdots)$. 实际上, 这就是$(a, 0, 0, \cdots) \cdot \alpha = a \cdot \alpha$. ■

现在我们令

$$x = (0, 1, 0, 0\cdots).$$

易知

$$x^n := \underbrace{x \cdot x \cdot \cdots \cdot x}_{n} = (0, 0, \cdots, 0, a_n, 0, \cdots),$$

这里 $a_n = 1$. 因而

$$(a_0, a_1, a_2, \cdots, a_n, \cdots) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

上式称为一元形式幂级数 (Formal power series in one indeterminate). x 称作不定元 (Indeterminate).

定义 2.3.8 $R[[x]]$ 中由集合 $R \cup \{x\}$ 生成的子幺环称作一元多项式环, 记作 $R[x]$.

由定义, $R[x]$ 中的元素都可以写为

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

我们称之为一元多项式 (Polynomial in one indeterminate). 换言之, 这样的元素可写为 $(a_0, a_1, \cdots, a_n, 0, 0, \cdots)$, 即除了有限个分量 $a_0, \cdots, a_n$ 外, 其余分量都为零.

例 2.3.13 (1) 数域 F 上的多项式环 $F[x]$. 比如我们熟悉的 $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$.
(2) 模素数 p 的剩余类域 $\mathbb{F}_p$ 上的多项式环 $\mathbb{F}_p[x]$.
(3) 整数环 $\mathbb{Z}$ 上的多项式环 $\mathbb{Z}[x]$. ■

注 2.3.6 (1) $a_0 + a_1 x + \cdots + a_n x^n = 0$ 当且仅当 $a_0 = a_1 = \cdots = a_n = 0$.
(2) 进一步, 两个多项式

$$a_0 + a_1 x + a_2 x^2 + \cdots = b_0 + b_1 x + b_2 x^2 + \cdots$$

相等, 当且仅当对应的系数相等 $a_i = b_i$ $(\forall i)$. ■

例 2.3.14 (**多元多项式环**) 设 R 是交换幺环, $R_1 = R[x]$ 是一元多项式环.

(1) 我们先考虑环 R_1 上的多项式环 $R_2 = R_1[y]$, 这里 y 是不定元. 由定义可知, $R_1[y]$ 中的元素可以写为

$$a_0(x) + a_1(x) y + \cdots + a_n(x) y^n,$$

其中 $a_i(x) \in R[x]$ 是关于 x 的多项式. 因此, 这样的元素也可以写成

$$\sum_{i,j=0}^{N} a_{ij}x^i y^j, \quad a_{ij} \in R.$$

我们就称 R_2 为二元多项式环.

(2) 我们可以归纳地定义 n 元多项式环

$$R[x_1, \cdots, x_n] := R'[x_n],$$

这里 $R' = R[x_1, \cdots, x_{n-1}]$. 该环中的多项式可以写成

$$f(x_1, \cdots, x_n) = \sum_{i_1, \cdots, i_n=0}^{N} a_{i_1 i_2 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} \quad a_{i_1 \cdots i_n} \in R.$$

$x_1, \cdots, x_n$ 是 n 个不定元.

此外, $0 \in R[x]$ 也称为零多项式. ■

命题 2.3.7 设 R 是交换幺环, $R[x_1, \cdots, x_n]$ 是 R 上 n 元多项式环. 设 S 是交换幺环, $u_1, \cdots, u_n \in S$ 是给定的元. $\sigma : R \to S$ 是环同态, 且 $\sigma(1_R) = 1_S$. 那么 σ 可以唯一扩充为同态

$$\sigma_u : R[x_1, \cdots, x_n] \longrightarrow S,$$

使得 $\sigma_u(x_i) = u_i$.

证明 我们对 n 施归纳法. 先考虑 $n = 1$ 的情形.

取 $f(x) = a_0 + a_1 x + \cdots a_n x^n \in R[x]$. 我们定义映射 σ_u 如下,

$$\sigma_u(f(x)) = \sigma(a_0) + \sigma(a_1)u + \cdots + \sigma(a_n)u^n,$$

这里 $u \in S$ 是给定的元素.

设 $g(x) = b_0 + b_1 x + \cdots + b_m x^m$. 容易验证 $\sigma_u(f(x) + g(x)) = \sigma_u(f(x)) + \sigma_u(g(x))$. 现在来验证 σ_u 的乘法兼容性, 设 $f(x)g(x) = c_0 + c_1 x + \cdots + c_{n+m}x^{n+m}$, 此处 $c_k = \sum_{i+j=k} a_i b_j$. 我们有

$$\sigma_u(f(x) \cdot g(x)) = \sigma_u(c_0) + \sigma_u(c_1)u + \cdots + \sigma_u(c_{n+m})x^{n+m}$$

注意到

$$\sigma_u(c_k) = \sigma_u\left(\sum_{i+j=k} a_i b_j\right) = \sum_{i+j=k} \sigma_u(a_i)\sigma_u(b_j),$$

故得 $\sigma_u(f(x) \cdot g(x)) = \sigma_u(f(x)) \cdot \sigma_u(f(x))$. 因此 σ_u 是环同态.

今假设 $< n$ 的情形已证. 设 $R' = R[x_1, \cdots, x_{n-1}]$. 由归纳假设, 我们已有扩充环同态

$$\sigma'_u : R' \to S,$$

使得 $\sigma'_u(x_i) = u_i$ $(i = 1, \cdots, n-1)$. 根据上面的论证, σ'_u 可以扩充为环同态 $\sigma_u : R'[x_n] \to S$, 使得 $\sigma_u(x_n) = u_n$. 注意到 $R[x_1, \cdots, x_n] = R'[x_n]$, 所以 σ_u 就是我们想要的环同态. 另一方面, σ_u 是由 σ 和诸 $u_i = \sigma(x_i)$ 确定的, 所以这样的同态是唯一确定的. ■

假设 R 是 S 的子幺环, σ 是嵌入同态, $u_1,\cdots,u_n\in S$ 是给定元素. 我们有自然的同态

$$\sigma_u : R[x_1,\cdots,x_n]\longrightarrow S,\quad f(x_1,\cdots,x_n)\to f(u_1,\cdots,u_n).$$

我们记

$$R[u_1,\cdots,u_n]:=\{f(u_1,\cdots,u_n)|\ f(x_1,\cdots,x_n)\in R[x_1,\cdots,x_n]\}.$$

它实际上是 S 中由集合 $R\cup\{u_1,\cdots,u_n\}$ 生成的子幺环. 为方便叙述, 我们称 $R[u_1,\cdots,u_n]$ 为由元素 $u_1,\cdots,u_n$ 生成的子环. 这样的环也叫做 R 的有限生成环. 因此, 上述映射给出了满同态

$$\sigma_u : R[x_1,\cdots,x_n]\longrightarrow R[u_1,\cdots,u_n](\subseteq S).$$

例 2.3.15　考虑环同态

$$\sigma : \mathbb{Z}[x]\longrightarrow \mathbb{Z}[\sqrt{d}],\quad f(x)\to f(\sqrt{d}).$$

定义 2.3.9　设 R 是交换幺环, $R[x]$ 是 R 上的多项式环,

$$f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x],\quad a_n\neq 0.$$

我们定义

$$\deg f(x):=\begin{cases} n, & \text{如果 } f(x) \text{ 非零多项式},\\ -\infty, & \text{如果 } f(x) \text{ 是零多项式}.\end{cases}$$

引理 2.3.4　我们有以下的不等式

$$\begin{aligned}\deg(f(x)+g(x))&\le\max\{\deg f(x),\deg g(x)\},\\ \deg(f(x)\cdot g(x))&\le\deg f(x)+\deg g(x).\end{aligned}$$

当 $\deg f\neq\deg g$ 时, 第一个不等式等号成立. 当 f 或 g 的首项系数不是 R 的零因子时 (特别当 R 是整环时), 第二个不等式的等号成立.

推论 2.3.4　假设 $f,g\in R[x]$ 是非零多项式. 如果 f 或 g 的首项系数不是零因子, 则 $f(x)g(x)\neq 0$.

定理 2.3.2　如果 R 是整环, 那么 $R[x_1,\cdots,x_n]$ 也是整环. 进一步, $R[x_1,\cdots,x_n]$ 中的乘法可逆元就是 R 中的乘法可逆元.

特别地, 域上的多项式环必定是整环.

证明　利用归纳法, 我们只需要讨论一元多项式环情形. 考虑 $R[x]$ 的非零元 $f(x),g(x)$. 由于 R 是整环, 所以它们的首项系数都不是零因子. 由推论 2.3.4, $f(x)g(x)\neq 0$. 这意味着 f,g 不可能是零因子, 因而 $R[x]$ 是整环.

假如 $f(x)\cdot g(x)=1$, 则 $\deg f=\deg g=0$, 即 f,g 都是非零常数, 因而 f,g 是 R 中的可逆元. ■

我们可以把数域上的一元多项式的带余除法推广到交换环上的多项式环情形.

定理 2.3.3 (**带余除法**)　设 R 是交换幺环, $R[x]$ 是 R 上的多项式环, $f(x),g(x)\in R[x]$, 且 $g(x)\neq 0$ 的首项是 R 中可逆元, 那么存在唯一的多项式 $q(x),r(x)\in R[x]$, 使得

$$f(x)=q(x)g(x)+r(x),\quad \deg r(x)<\deg g(x).$$

证明 先证存在性. 设 f,g 表达式为

$$f(x)=a_0+a_1x+\cdots+a_nx^n,$$
$$g(x)=b_0+b_1x+\cdots+b_mx^m.$$

我们对 $n=\deg f$ 施归纳法. $n=\infty,0$ 时, 结论显然. 假设 $<n$ 的情形已证. 令

$$f_1(x)=f(x)-(a_n\cdot b_m^{-1})\cdot x^{n-m}\cdot g(x).$$

显见 $\deg f_1(x)<\deg f(x)$.

由归纳假设, 存在 $q_1(x),r(x)\in R[x]$ 满足

$$f_1(x)=q_1(x)g(x)+r(x),\quad \deg r(x)<\deg g(x).$$

这就推出

$$f(x)=(q_1(x)+(a_n\cdot b_m^{-1})\cdot x^{n-m})g(x)+r(x).$$

再证唯一性. 设 $f(x)=\tilde{q}(x)g(x)+\tilde{r}(x)$ 是另一带余除式. 我们得到

$$(q(x)-\tilde{q}(x))g(x)=\tilde{r}(x)-r(x).$$

由引理 2.3.4, 上式右边的次数 $\deg(\tilde{r}-r)\leq\max\{\deg\tilde{r},\deg r\}<\deg g$. 如果上式右边不等于零的话, 则次数至少是 $\deg g$, 矛盾! 因此 $(q(x)-\tilde{q}(x))g(x)=0$. 由推论 2.3.4, $q(x)=\tilde{q}(x)$, 进而 $\tilde{r}=r$. ■

特别地, 上述结论在域上的多项式环中总成立, 这是因为此时非零多项式的首项系数总是乘法可逆的.

例 2.3.16 设 $R=\mathbb{Z}_N$. 当 N 是素数时, $\mathbb{Z}_N[x]$ 是整环. 当 N 不是素数时, $\mathbb{Z}_N[x]$ 不是整环. 比如 $N=6$, $\mathbb{Z}_6[x]$ 中有零因子 $[2],[3],[4]$ 以及 $[2]x+[2]$ 等等. ■

推论 2.3.5 设 $c\in R$, $f(x)\in R[x]$, 则

(1) (**余数定理**) $f(x)$ 可表为

$$f(x)=q(x)(x-c)+f(c).$$

(2) (**因式定理**) $(x-c)\mid f(x)$ 当且仅当 c 是 $f(x)$ 的根.

推论 2.3.6 设 R 是整环, $f(x)\in R[x]$ 是 n 次多项式, 则 $f(x)$ 在 R 内最多有 n 个根.

证明 我们对 $n=\deg f$ 施归纳法. $n=0,1$ 时, 结论显然. 假设 $<n$ 的情形已证.

如果 $f(x)$ 无 R 中的解, 则命题已成立. 不妨假设 $a\in R$ 是 $f(x)$ 的根. 由因式定理, $f(x)=(x-a)f_1(x)$. 如果 a 也是 $f_1(x)$ 的根, 则进一步有 $f_1(x)=(x-a)f_2(x)$, 因而 $f(x)=(x-a)^2f_2(x)$,..... 依次类推, 我们可得到 $f(x)=(x-a)^hg(x)$, 这里 $g(x)$ 是 R 中多项式, 且 $g(a)\neq0$.

假如 $f(x)$ 没有其他根, 则 f 的根的个数 $h<n$. 不妨设 $b\in R$ 是 $f(x)$ 的另一根. 于是

$$0=f(b)=(b-a)^h\cdot g(b).$$

由于 $b-a\neq0$ 且 R 是整环, 故上式推出 $g(b)=0$. 因为 $\deg g=n-h$, 故由归纳假设, $g(x)$ 最多有 $n-h$ 个根. 这样, $f(x)$ 最多有 n 个根. ■

注 2.3.7　上面的证明其实可以推出

$$f(x) = (x-a)^h(x-b)^k\cdots(x-c)^l g(x),$$

$g(x)$ 在 R 中没有解. ■

例 2.3.17　(1) 数域 F 上的多项式至多有 F 中的 n 个根.
(2) 设 $\mathbb{F}_p$ 是模素数 p 的剩余类域. $\mathbb{F}_p[x]$ 中的多项式有可能没有任何解. 比如$x^2+[1]=[0]$ 在 $\mathbb{F}_3$ 中无解.
(3) 设 $R=\mathbb{Z}_6$ 是模 6 的剩余类环, $x^3-x\in\mathbb{Z}_6[x]$ 在 $\mathbb{Z}_6$ 中有六个解. 这说明推论 2.3.6 里 R 的无零因子条件不可或缺.
(4) 设 $R=\mathbb{H}$ 是哈密顿四元数体, $x^2+\mathbf{1}=0$ 在 $\mathbb{H}$ 中至少有三个根 $\mathbf{i},\mathbf{j},\mathbf{k}$. 这说明推论 2.3.6 里 R 的乘法交换律条件也不可或缺. ■

推论 2.3.7 (**费马小定理应用**)　设 $\mathbb{F}_p$ 是模素数 p 的剩余类域.
(1) 在 $\mathbb{F}_p[x]$ 中, 我们有分解因式

$$x^{p-1}-[1]=(x-[1])(x-[2])\cdots(x-[p-1]). \tag{2-4}$$

(2) (Wilson **定理**) 在 $\mathbb{F}_p$ 中, 有 $[(p-1)!]=[-1]$.

证明　(1) 由费马小定理, $x^{p-1}-[1]$ 恰有 $p-1$ 个根 $[1],\cdots,[p-1]$. 这就得到上数因式分解.

(2) 将式 (2-4) 右边展开, 由注记 2.3.6(2), 比较两边的常数项即得结论. ■

例 2.3.18　设 R 是整环, F 是 R 的分式域, 则 $R[x]$ 的分式域是域 F 上的有理函数域

$$F(x)=\left\{\frac{f}{g}\;\middle|\; f,g\in R[x],\ g\neq 0\right\}.$$

我们有包含关系 $R\subseteq R[x]\subseteq F[x]\subseteq F(x)$. ■

2.3.7　构造方法 (IV): 理想与商环

让我们从环同态开始. 考虑一个环同态

$$\sigma: R\to S.$$

我们定义集合

$$\mathrm{Ker}\sigma := \{a\in R\mid \sigma(a)=0_S\}.$$

它称作 σ 的核 (Kernel).

命题 2.3.8　核 $\mathrm{Ker}\sigma$ 是 R 的子环, 并且满足如下性质 (也称做吸收性):

$$ra,\ ar\in\mathrm{Ker}\sigma,\quad \forall r\in R,\ \forall a\in\mathrm{Ker}\sigma.$$

证明　对任何 $a,b\in\mathrm{Ker}\sigma$, 我们有 $\sigma(a-b)=\sigma(a)-\sigma(b)=0$, 因而 $a-b\in\mathrm{Ker}\sigma$. 进一步, 对任何 $r\in R$, 有

$$\sigma(ra)=\sigma(r)\sigma(a)=\sigma(r)\cdot 0_S=0_S.$$

同理也有 $\sigma(ar)=0_S$. 因此 $ra,ar\in\mathrm{Ker}\sigma$. 特别地, 如取 $r\in\mathrm{Ker}\sigma$, 则得 $\mathrm{Ker}\sigma$ 的乘法封闭性. 由子环判别法即得所需结论. ■

推论 2.3.8　$\mathrm{Ker}\sigma = \{0_R\}$ 当且仅当 σ 是单同态.

证明　($\Longrightarrow$) 假设 $\sigma(a) = \sigma(b)$, 则 $\sigma(a-b) = 0_S$, 即 $a - b \in \mathrm{Ker}\sigma$. 由条件, $\mathrm{Ker}\sigma = 0$, 因而 $a = b$.

($\Longleftarrow$) 设 $a \in \mathrm{Ker}\sigma$, 即 $\sigma(a) = \sigma(0_R)$. 由 σ 的单射性即得结论. ■

例 2.3.19　考虑整数环到模 N 的剩余类环的同态

$$\sigma : \mathbb{Z} \to \mathbb{Z}_N, \quad n \to [n].$$

它的核

$$\mathrm{Ker}\sigma = \{Nk \mid k \in \mathbb{Z}\}.$$

上述集合也通常记作 $N\mathbb{Z}$. ■

例 2.3.20　给定实数 a, 考虑环同态

$$\sigma : \mathbb{R}[x] \longrightarrow \mathbb{R}, \quad f(x) \to f(a).$$

我们来证明

$$\mathrm{Ker}\sigma = \{(x-a)g(x) \mid g(x) \in \mathbb{R}[x]\}.$$

显然上式右边集合含于左边集合. 今假设 $f \in \mathrm{Ker}\sigma$, 即 $f(a) = 0$. 由因式定理 (见推论 2.3.5(2)), 即得 $f = (x-a)g$. 这就证明上式左边也含于右边集合. 有时我们也将上述核简记为 $(x-a)$. ■

例 2.3.21　考虑例 2.3.4 的 2 阶对角阵构成的交换幺环

$$R = \left\{ \begin{pmatrix} a & \\ & b \end{pmatrix} \in M_2(F) \,\middle|\, a, b \in F \right\}$$

以及它的子环

$$L = \left\{ \begin{pmatrix} a & \\ & 0 \end{pmatrix} \in M_2(F) \,\middle|\, a \in F \right\}, \qquad M = \left\{ \begin{pmatrix} 0 & \\ & b \end{pmatrix} \in M_2(F) \,\middle|\, b \in F \right\}.$$

我们有两个环同态

$$\sigma : R \to M, \quad \begin{pmatrix} a & \\ & b \end{pmatrix} \to \begin{pmatrix} 0 & \\ & b \end{pmatrix},$$

以及

$$\tau : R \to L, \quad \begin{pmatrix} a & \\ & b \end{pmatrix} \to \begin{pmatrix} a & \\ & 0 \end{pmatrix}.$$

直接计算可知, $\mathrm{Ker}\sigma = L$, $\mathrm{Ker}\tau = M$. ■

例 2.3.22　考虑剩余类环的同态

$$\sigma : \mathbb{Z}_6 \to \mathbb{Z}_2, \quad [n] \to [n].$$

它的核 $\mathrm{Ker}\sigma = \{[0], [2], [4]\}$. ■

同态的核是很特殊的子环, 满足吸收性. 我们可以把这类子环抽象出来.

定义 2.3.10　设 R 是一个环, I 是 R 的子环, 并且对任何 $r \in R$, $a, b \in I$, 都满足 $ra \in I$ (相应地, $ar \in I$), 那么我们就称 I 是 R 的左理想 (相应地, 右理想). 如果 I 既是左理想又是右理想, 则称为理想 (Ideal, 或双边理想).

我们主要关心双边理想的情形. 特别地, 交换环中的左理想、右理想就是双边理想, 所以我们就简单地称为理想.

注 2.3.8　因为吸收性本身蕴含了乘法封闭性, 所以理想相当于满足以下条件的子集合:
(i) $a - b \in I$, $\forall a, b \in I$,
(ii) $ra, ar \in I$, $\forall r \in R$, $\forall a \in I$. ■

注 2.3.9　假设 R 是幺环.
(1) 理想 I 含有 1_R 当且仅当 $I = R$.
(2) $I = \{0_R\}$ 是理想. 我们把上述理想 $I = \{0_R\}, R$ 称作平凡理想. ■

例 2.3.23　任何环同态 $\sigma : R \to S$ 的核都是 R 的理想. ■

例 2.3.24　域 F 没有非平凡理想. 不妨假设 I 是非平凡理想. 对任何非零元 $a \in I$, 都有

$$1_F = a^{-1} \cdot a \in I.$$

因此 $I = F$, 矛盾!

特别地, 结合例 2.3.23, 我们可以断言, 任何域到环的非零同态必定是单同态.

反过来, 我们来证明: 如果交换幺环 R (至少含两个元) 只有平凡理想, 则它必是域. 任取非零元 $a \in R$, 考虑理想

$$(a) := \{ar | \, r \in R\}.$$

由假设条件, $(a) = R$, 即 $1_R \in (a)$, 亦即存在非零元 r 使得 $1_R = ra$. 这就说明 a 有乘法逆元. 由 a 的任意性, 即知 R 是域. ■

例 2.3.25　考虑整数环中的子环

$$n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}.$$

它是理想. 反过来, $\mathbb{Z}$ 中任何理想都形如 $d\mathbb{Z}$ ($d \geq 0$). 我们来简单证明一下. 假设 I 是 $\mathbb{Z}$ 的理想. 如果 I 是平凡理想, 则 $I = 0\mathbb{Z}, \mathbb{Z}$ 显然满足条件. 不妨设 I 非平凡. 此时 I 含有非零元, 因而也必含有正整数. 不妨设 $d \in I$ 是其中最小的正整数. 因为 $I \neq \mathbb{Z}$, 所以 $d > 1$. 显然 $d\mathbb{Z} \subseteq I$.

另一方面, 对任何 $n \in I$, 考虑带余除法

$$n = dq + r, \quad 0 \leq r < d.$$

显见 $r = n - dq \in I$. 由 d 的最小性立知 $r = 0$, 即 $d \mid n$. 这就推出 $I \subseteq d\mathbb{Z}$. 因此 $I = d\mathbb{Z}$. ■

命题 2.3.9　设 R 是环, 则
(1) 任意多个理想的交仍是理想.
(2) 给定非空集合 $E \subseteq R$, 所有包含 E 的理想的交是包含 E 的最小理想, 称作由 E 生成的理想.

特别地, 如果 R 是交换幺环, $E=\{a_1,\cdots,a_n\}$ 是有限子集. 由 E 生成的理想记作

$$(a_1,\cdots,a_n)=\{r_1a_1+\cdots+r_na_n|\ r_1,\cdots r_n\in R\}.$$

特别地, 由一个元素 a 生成的理想 (a) 通常叫做主理想. 比如 $(N)=N\mathbb{Z}$ 就是 $\mathbb{Z}$ 的主理想.

例 2.3.26　设 $I\subseteq R$ 是交换环 R 的理想, 我们定义如下集合

$$\sqrt{I}=\{a\in R|\ a^n\in I,\text{ 对某个正整数 }n\}.$$

显见 $I\subseteq\sqrt{I}$. 我们来证明 $\sqrt{I}$ 也是 R 的理想, 称作根理想.

任取 $a,b\in\sqrt{I}$. 由定义, 存在正整数 n,m, 使得 $a^n,b^m\in I$. 考虑如下二项式展开 (注意 R 是交换环)

$$(a-b)^{n+m}=a^{n+m}-(n+m)a^{n+m-1}b+\cdots+(-1)^kC_{n+m}^ka^{n+m-k}b^k+\cdots+(-1)^{n+m}b^{n+m}.$$

观察右式的任一单项式 $a^{n+m-k}b^k$. 如果 $k\le m$, $a^{n+m-k}b^k=(a^{m-k}b^k)a^n\in I$. 如果 $k>m$, $a^{n+m-k}b^k=(a^{n+m-k}b^{k-m})b^m\in I$. 因此 $(a-b)^{n+m}\in I$, 故 $a-b\in\sqrt{I}$. 对任何 $r\in R$, $(ra)^n=r^na^n\in I$, 故 $ra\in\sqrt{I}$. 因而 $\sqrt{I}$ 是理想. ■

例 2.3.27　设 k 是代数闭域 (见第 1.7 节), $k[x_1,\cdots,x_n]$ 是 k 上的多项式环, $f_1,\cdots,f_r\in k[x_1,\cdots,x_n]$. 我们有如下理想

$$I=(f_1,\cdots,f_r)=\{f_1g_1+\cdots+f_rg_r|\ g_1,\cdots,g_r\in k[x_1,\cdots,x_n]\}.$$

方程组

$$\begin{cases}f_1(x_1,\cdots,x_n)=0,\\ f_2(x_1,\cdots,x_n)=0,\\ \cdots\cdots\\ f_r(x_1,\cdots,x_n)=0\end{cases}$$

在 k 中的解集称作代数簇, 它和根理想 $\sqrt{I}$ 存在一一对应. 这种对应将几何图形的性质和方程的代数性质 (即上述理想) 联系起来. 这就是代数几何的一个主要思想–推广了古典解析几何. ■

现在我们要利用理想来构造新的环. 设 R 是环, I 是 R 的理想. 我们定义 R 上的等价关系 (请读者自己验证)

$$a\sim_I b\Longleftrightarrow a-b\in I.$$

我们用

$$[a]_I:=\{b\in R|\ a\sim_I b\}$$

来表示 a 所在的等价类, 有时也简记为 $[a]$ 或 $\bar{a}$. 全体等价类构成的集合记作 R/I. 我们在 R/I 上定义加法和乘法运算

$$[a]+[b]:=[a+b],\quad [a]\cdot[b]:=[a\cdot b].$$

首先, 当然需要验证上述两种运算的合理性. 假设 $[a]=[a']$, $[b]=[b']$. 由定义, $r=a-a'\in I$, $s=b-b'\in I$. 因此

$$(a+b)-(a'+b')=r+s\in I,$$

即 $[a+b]=[a'+b']$. 这就证明了加法运算的合理性. 进一步, 由理想的吸收性可得

$$a'b'-ab=(a-r)(b-s)-ab=-rb-as+rs\in I.$$

因此 $[a'b']=[ab]$. 这就证明乘法运算的合理性.

命题 2.3.10 设 R 是环, I 是 R 的理想, 则
(1) R/I 是环, 称作商环. 特别地, 如果 R 是交换幺环, 那么 R/I 也是交换幺环, 其幺元为 $[1]$.
(2) 存在自然同态

$$\pi: R\longrightarrow R/I,\quad a\to[a],$$

它是满同态并且 $\mathrm{Ker}\pi=I$. 特别地, 任何理想都是某环同态的核.

证明 (1) 前面已验证两类运算合理性, 其余的环公理验证留给读者完成.

(2) 我们这里只验证 $\mathrm{Ker}\pi=I$, 其余结论验证留给读者完成. 设 $a\in\mathrm{Ker}\pi$, 即 $[0]=\pi(a)=[a]$, 因而 $a\in I$. 这推出 $\mathrm{Ker}\pi\subseteq I$. 另一方面, 对任何 $a\in I$, $\pi(a)=[a]=[0]$, 即 $a\in\mathrm{Ker}\pi$. 这就证明 $I\subseteq\mathrm{Ker}\pi$. ■

注 2.3.10 请注意, R/I 与 $R\backslash I$ 是完全不同的两个记号. 前者表示商环, 后者表示 I 在 R 中的补集. ■

例 2.3.28 假设 R 是环, I 是 R 的平凡理想.
(1) 如果 $I=(0)$, 那么 $R/I\cong R$. 事实上, 对 $a\in R$, 它的等价类 $[a]=\{a\}$. 因此我们有显然的同构

$$R\longrightarrow R/I,\quad a\to[a].$$

(2) 如果 $I=R$, 那么 $R/I=\{[0]\}$. 这是因为 R 中所有元素都在同一个等价类中, 即 I. 我们就不妨取 0 作为代表元, $I=[0]$. ■

例 2.3.29 设 $N\mathbb{Z}=(N)$ 是 $\mathbb{Z}$ 的理想. 此时商环 $\mathbb{Z}/N\mathbb{Z}=\mathbb{Z}_N$. ■

例 2.3.30 证明 $\mathbb{Z}[\sqrt{-1}]/(1+\sqrt{-1})$ 是二元域.

任取 $a+b\sqrt{-1}\in\mathbb{Z}[\sqrt{-1}]$. 如果 a,b 同奇同偶, 那么

$$a+b\sqrt{-1}=(1+\sqrt{-1})\left(\frac{a+b}{2}+\frac{b-a}{2}\sqrt{-1}\right)\in[0].$$

如果 a,b 一奇一偶, 那么

$$a+b\sqrt{-1}=1+(1+\sqrt{-1})\left(\frac{a+b-1}{2}+\frac{b-a+1}{2}\sqrt{-1}\right)\in[1].$$

因此 $\mathbb{Z}[\sqrt{-1}]/(1+\sqrt{-1})=\{[0],[1]\}\cong\mathbb{F}_2$. ■

例 2.3.31 在例 2.3.20 的记号假设下, 我们来验证 $\mathbb{R}(x)/(x-a)\cong\mathbb{R}$.

构造映射

$$\bar{\sigma}:\mathbb{R}(x)/(x-a)\cong\mathbb{R},\quad [f(x)]\to f(a).$$

先说明映射的合理性. 假设 $[f(x)]=[g(x)]$, 则 $f-g=(x-a)h$, 这里 $h\in\mathbb{R}[x]$. 因而 $f(a)=g(a)$.

其次容易验证, 这是一个同态. 易知它是满同态, 因为对任何 $r \in \mathbb{R}$, 都有 $\bar{\sigma}([r]) = r$. 我们验证它是单同态. 由推论 2.3.8, 我们只需要验证核 $\mathrm{Ker}\bar{\sigma} = \{[0]\}$. 假设 $[f] \in \mathrm{Ker}\bar{\sigma}$, 则 $0 = \sigma([f]) = f(a)$. 这表明 $f \in \mathrm{Ker}\sigma = (x-a)$ (见例 2.3.20 的记号), 即 $[f] = [0]$. ■

例 2.3.31 的结论可以推广到更一般的结论.

定理 2.3.4 (环同态基本定理) 设 $\sigma : R \to S$ 是环的满同态, 那么
(1) 存在唯一的环同构 $\bar{\sigma} : R/\mathrm{Ker}\sigma \to S$, 满足 $\sigma = \bar{\sigma} \circ \pi$, 这里 $\pi : R \to R/\mathrm{Ker}\sigma$ 是自然同态.
(2) 设

$$A = \{R \text{ 中所有包含 } \mathrm{Ker}\sigma \text{ 的理想}\},$$
$$B = \{S \text{ 中所有理想}\}.$$

存在一一对应

$$\Phi : A \longrightarrow B, \quad I \to \sigma(I).$$

证明 为书写方便, 我们记 $J = \mathrm{Ker}\sigma$.

(1) 我们定义映射

$$\bar{\sigma} : R/J \to S, \quad [a] \to \sigma(a).$$

先验证这个映射的合理性. 假如 $[a] = [b]$, 那么 $a - b \in J$, 即 $\sigma(a-b) = 0$, 故 $\sigma(a) = \sigma(b)$. 其次, 验证它是同态, 这来自于

$$\bar{\sigma}([a] + [b]) = \bar{\sigma}([a+b]) = \sigma(a+b) = \sigma(a) + \sigma(b) = \bar{\sigma}[a] + \bar{\sigma}([b])$$
$$\bar{\sigma}([a] \cdot [b]) = \bar{\sigma}([a \cdot b]) = \sigma(a \cdot b) = \sigma(a) \cdot \sigma(b) = \bar{\sigma}[a] \cdot \bar{\sigma}([b])$$

再证明它是单同态. 设 $[a] \in \mathrm{Ker}\bar{\sigma}$, 则 $0 = \bar{\sigma}([a]) = \sigma(a)$. 因此 $a \in J$, 即 $[a] = [0]$. 最后说明 $\bar{\sigma}$ 是满射. 这是因为, 对任何 $r \in S$, 由 σ 的满射条件, 存在 $a \in R$ 满足 $\sigma(a) = r$. 因此 $\bar{\sigma}([a]) = \sigma(a) = r$. 这样, 我们就得到环同构 $\bar{\sigma}$. 显见

$$\sigma(a) = \bar{\sigma}([a]) = \bar{\sigma}(\pi(a)) = (\bar{\sigma} \circ \pi)(a), \quad \forall a \in R.$$

因此 $\sigma = \bar{\sigma} \circ \pi$.

最后, 我们来说明 $\bar{\sigma}$ 的唯一性. 假设有同态 $\tau : R/J \to S$ 满足 $\sigma = \tau \circ \pi$. 因而对任意 $[a] \in R/J$, 有

$$\tau([a]) = \tau(\pi(a)) = (\tau \circ \pi)(a) = \sigma(a) = \bar{\sigma}([a]).$$

这就迫使 $\tau = \bar{\sigma}$.

(2) 首先说明, 对任何包含 J 的理想 I, $\sigma(I)$ 必定是 S 的理想. 设 $\sigma(a), \sigma(b) \in \sigma(I)$, 这里 $a, b \in I$. 因为 $a - b \in I$, 所以 $\sigma(a) - \sigma(b) = \sigma(a-b) \in \sigma(I)$. 对任何 $s \in S$, 注意到 σ 是满射, 故存在 $r \in R$, 使得 $s = \sigma(r)$. 因为 $ra, ar \in I$, 所以 $s\sigma(a) = \sigma(ra) \in \sigma(I)$, 同理 $\sigma(a)s \in \sigma(I)$. 这就证明 $\sigma(I)$ 是 S 的理想. 因此映射 $\Phi : A \to B$ 是合理的.

其次说明 Φ 是满射. 对任何 S 中的理想 K, 定义

$$\sigma^{-1}(K) = \{a \in R | \ \sigma(a) \in K\}.$$

它是一个理想. 这是因为对任何 $a, b \in \sigma^{-1}(K)$, $\sigma(a-b) = \sigma(a) - \sigma(b) \in K$, 因而 $a - b \in \sigma^{-1}(K)$;

对任何 $r \in R$, $\sigma(ra) = \sigma(r)\sigma(a) \in K$, 故 $ra \in \sigma^{-1}(K)$, 同理 $ar \in \sigma^{-1}(K)$. 显见 $J \subseteq \sigma^{-1}(K)$. 此外, 注意到 σ 是满射, 所以 $\sigma(\sigma^{-1}(K)) = K$.

最后说明, Φ 是单射. 假设 I, I' 都是 R 中包含 J 的理想, 满足 $\sigma(I) = \sigma(I')$. 设 $a \in I$, 则 $\sigma(a) \in \sigma(I) = \sigma(I')$, 故存在 $a' \in I'$, 使得 $\sigma(a') = \sigma(a)$, 即 $\sigma(a - a') = 0$, 亦即 $a - a' \in J$. 因为 $J \subseteq I'$, 所以 $a - a' \in I'$, 从而 $a = (a - a') + a' \in I'$. 由 a 的任意性得 $I \subseteq I'$. 同理可得 $I' \subseteq I$, 故 $I = I'$. ■

注 2.3.11 (1) 定理 2.3.4 中的理想之间的对应是保序的. 具体言之, 如果 $I_1 \subseteq I_2$ 是 R 中的两个理想, 那么对应的 S 中的理想 $\sigma(I_1) \subseteq \sigma(I_2)$ 也满足包含关系.
(2) 由环同态基本定理的证明, 我们也得到如下结论: $\sigma^{-1}(\sigma(I)) = I$, $\sigma(\sigma^{-1}(K)) = K$. ■

推论 2.3.9 设 $\sigma : R \to S$ 是环同态, 则 $\mathrm{Im}\sigma$ 是 S 的子环, 并且 $R/\mathrm{Ker}\sigma \cong \mathrm{Im}\sigma$.

推论 2.3.10 设 R 是环, I 是 R 的理想, 那么R 中包含 I 的理想与 R/I 中的理想存在一一对应, 即

$$K \mapsto K/I.$$

特别地, I 对应 R/I 的零理想.

证明 在定理 2.3.4 中直接取 $S = R/I$, $\sigma = \pi : R \to R/I$ 即得. ■

推论 2.3.11 设 $\sigma : R \to S$ 是环的满同态, H 是包含 $\mathrm{Ker}\sigma$ 的理想, 那么 σ 诱导环同构

$$\bar{\sigma} : R/H \longrightarrow S/\sigma(H), \quad [a]_H \to [\sigma(a)]_{\sigma(H)}.$$

证明 首先诱导复合映射 $\sigma' : R \to S/\sigma(H)$ 如下:

$$R \xrightarrow{\sigma} S \xrightarrow{\pi} S/\sigma(H).$$

因为 σ, π 都是满同态, 所以 σ' 也是满的. 现在我们只需要证明 $\mathrm{Ker}\sigma' = H$, 就可由同态基本定理得到所需结论, 也就是说 σ' 诱导同构 $\bar{\sigma}$.

首先, 对任何 $a \in H$, 显然有 $\sigma'(a) = \pi(\sigma(a)) = [0]_{\sigma(H)}$. 因此 $a \in \mathrm{Ker}\sigma'$. 由 a 的任意性即得 $H \subseteq \mathrm{Ker}\sigma'$. 反过来, 对任何 $a \in \mathrm{Ker}\sigma'$, $[0]_{\sigma(H)} = \sigma'(a) = \pi(\sigma(a))$, 因此 $\sigma(a) \in \sigma(H)$, 从而 $a \in \sigma^{-1}(\sigma(H))$. 由 a 的任意性, $\mathrm{Ker}\sigma' \subseteq \sigma^{-1}(\sigma(H)) = H$. 综上即得 $H = \mathrm{Ker}\sigma'$. ■

注 2.3.12 在推论 2.3.11 中取 $H = \mathrm{Ker}\sigma$, 就得到同态基本定理所诱导的同构映射. 因此它是同态基本定理的推广. ■

推论 2.3.12 设 I 是 R 的理想, 那么 $\pi : R \to R/I$ 是自然同态, H 是包含 I 的任何理想, 则 π 诱导同构

$$\bar{\pi} : R/H \longrightarrow (R/I)/(H/I), \quad [a]_H \to [\sigma(a)]_{H/I}.$$

证明 在推论 2.3.11 中取 $S = R/I$ 即得. ■

利用上述同态定理, 我们可以计算很多商环的结构.

例 2.3.32 设 θ 是 n 次代数数, 即它为某个 n 次有理系数不可约多项式 $f(x)$ 的根. 我们定义同态

$$\sigma : \mathbb{Q}[x] \to \mathbb{Q}(\theta), \quad h(x) \to h(\theta).$$

由例 1.3.3 的讨论, $\mathbb{Q}(\theta)$ 中的元素都可以写作 $h(\theta)$ 的形式, 这里 $h \in Q[x]$ 是次数不超过 $n-1$ 的多项式. 因而 σ 是满同态.

今设 $g \in \mathrm{Ker}\sigma$, 即 $g(\theta) = 0$. 由例 1.3.3 的讨论, $f \mid g$, 即 $g \in (f)$. 因而 $\mathrm{Ker}\sigma \subseteq (f)$. 反之显见, $(f) \subseteq \mathrm{Ker}\sigma$, 故 $\mathrm{Ker}\sigma = (f)$.

由环同态基本定理, 我们得到同构

$$\mathbb{Q}[x]/(f) \cong \mathbb{Q}(\theta).$$

比如取 $\theta = \sqrt{d}$ (d 不含平方因子), 则有

$$\mathbb{Q}[x]/(x^2 - d) \cong \mathbb{Q}(\sqrt{d}).$$

例 2.3.33 设 R 是交换幺环, $u_1, \cdots, u_n \in R$ 是给定元素. 由命题 2.3.7, 我们得到满的扩充同态

$$\sigma_u : R[x_1, x_2, \cdots, x_n] \to R, \quad f(x_1, \cdots, x_n) \to f(u_1, \cdots, u_n).$$

我们来证明

$$\mathrm{Ker}\sigma_u = (x_1 - u_1, \cdots, x_n - u_n).$$

只需证 $\mathrm{Ker}\sigma_u \subseteq (x_1 - u_1, \cdots, x_n - u_n)$. 任取 $f \in \mathrm{Ker}\sigma_u$, 即 $f(u_1, \cdots, u_n) = 0$. 我们对 n 施归纳法. 当 $n = 1$ 时, 由因式定理 (见推论 2.3.5(3)) 立得 $f \in (x_1 - u_1)$. 今假设 $< n$ 情形已证.

由余数定理 (见推论 2.3.5(2)), $f(x_1, \cdots, x_n) = (x_n - u_n)g + f(x_1, \cdots, x_{n-1}, u_n)$. 注意到 $f(x_1, \cdots, x_{n-1}, u_n) \in R[x_1, \cdots, x_{n-1}]$, 因此由归纳假设,

$$f(x_1, \cdots, x_{n-1}, u_n) \in (x_1 - u_1, \cdots, x_{n-1} - u_{n-1}).$$

这就推出 $f \in (x_1 - u_1, \cdots, x_n - u_n)$. 综上可知结论成立.

这样, 有环同态基本定理即得

$$R[x_1, \cdots, x_n]/(x_1 - u_1, \cdots, x_n - u_n) \cong R.$$

特别地, $R[x]/(x - u) \cong R$. 这就是例 2.3.31 的情形. ■

例 2.3.34 证明 $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

事实上, 我们有满同态

$$\sigma : \mathbb{R}[x] \to \mathbb{C}, \quad f(x) \to f(\sqrt{-1}).$$

对任何 $a + b\sqrt{-1} \in \mathbb{C}$, 显然有 $\sigma(a + bx) = a + b\sqrt{-1}$, 因而 σ 是满射.

剩下的, 我们只需证明 $\mathrm{Ker}\sigma \subseteq (x^2 + 1)$. 设 $f(x) \in \mathrm{Ker}\sigma$. 由带余除法,

$$f(x) = (x^2 + 1)q(x) + ax + b,$$

这里 $a, b \in \mathbb{R}$. 因为 $\sigma(f) = f(\sqrt{-1}) = 0$, 所以 $a\sqrt{-1} + b = 0$, 这就迫使 $a = b = 0$, 即 $(x^2 + 1) \mid f(x)$, 亦即 $f \in (x^2 + 1)$. ■

例 2.3.35 我们来说明 $\mathbb{C}[x]/(x^2+1) \ncong \mathbb{C}$.

首先 $[x+\sqrt{-1}] \neq [0]$, 否则 $x+\sqrt{-1} \in (x^2+1)$, 即 $x^2+1 \mid x+\sqrt{-1}$, 矛盾! 同理 $[x-\sqrt{-1}] \neq [0]$. 注意到 $[x+\sqrt{-1}]\cdot[x-\sqrt{-1}] = [x^2+1] = [0]$, 这表明 $[x+\sqrt{-1}], [x-\sqrt{-1}]$ 是零因子. 但 $\mathbb{C}$ 是域, 故两者不可能同构.

如果令 $\theta = [x]$, 那么

$$\mathbb{C}[x]/(x^2+1) \cong \{a+b\theta |\ a,b \in \mathbb{C},\ \theta^2 = -1\}.$$

右边环中的元素 θ 看上去像是一个"纯虚数", 但实际上它根本就不是"数". 显然这个交换幺环包含了复数域, 但遗憾的是它有零因子. ■

例 2.3.36 我们可以用同态基本定理证明如下同构

$$\mathbb{Z}[\sqrt{-1}]/(a+b\sqrt{-1}) \cong \mathbb{Z}_{a^2+b^2}, \quad [s+t\sqrt{-1}] \to [s-act],$$

这里 a, b 是互质的整数, c 是满足 $a^2+b^2 \mid bc-1$ 的整数. 由此同构可知, 如果 a^2+b^2 是素数, 那么 $(a+b\sqrt{-1})$ 是 $\mathbb{Z}[\sqrt{-1}]$ 的极大理想. ■

利用商环, 我们还能造出许多奇怪的环.

例 2.3.37 设 F 是交换幺环, 主理想 (x^2+1) 给出商环

$$R[x]/(x^2+1) \cong \{a+b\theta |\ \theta^2 = -1,\ a,b \in R\}.$$

当 $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ 时, 由前讨论, 它就是 $\mathbb{Z}[\sqrt{-1}]$,$\mathbb{Q}(\sqrt{-1})$, $\mathbb{C}$. 当 $R = \mathbb{C}$ 时, 即上例.

今取 $R = \mathbb{F}_p$ 为模素数 p 的剩余类环, 则记

$$\mathbb{F}_p[\sqrt{-1}] := \mathbb{F}_p[x]/(x^2+1) \cong \{[n]+[m]\theta |\ \theta^2 = -1,\ [n],[m] \in \mathbb{F}_p\}.$$

这是一个有限环, 它实际上有 p^2 个元素. 比如当 $p = 3$ 时, $\mathbb{F}_3[\sqrt{-1}]$ 实际上是域. 后面我们会探讨, 这样的环何时是域. ■

例 2.3.38 求 $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ 的所有理想.

考虑自然同态

$$\mathbb{Z} \longrightarrow \mathbb{Z}_N, \quad n \to [n].$$

根据推论 2.3.10, $\mathbb{Z}_N$ 的理想和 $\mathbb{Z}$ 中包含 $N\mathbb{Z}$ 的理想一一对应. 由例 2.3.25, $\mathbb{Z}$ 中的理想都是主理想 $(d) = d\mathbb{Z}$. $N\mathbb{Z} \subseteq d\mathbb{Z}$, 当且仅当 $d \mid N$. 因此 $\mathbb{Z}_N$ 的理想恰好就是 $d\mathbb{Z}/N\mathbb{Z} = ([d])$, 这里 d 跑遍 N 的所有正因子.

譬如, $\mathbb{Z}_6$ 的理想有 $([0])$, $([1])(= \mathbb{Z}_6)$, $([2]) = \{[0],[2],[4]\}$, $([3]) = \{[0],[3]\}$.

当 N 是素数时, N 的正因子只有 1 和 N, 它们恰好对应 $\mathbb{Z}_N$ 的平凡理想.

推论 2.3.12 在该例中相当于如下同构 $\mathbb{Z}_d \cong \mathbb{Z}_N/([d])$. ■

本节最后, 我们均假设 R 是交换幺环. 设 I 是 R 的理想. 此时 R/I 显然也是交换幺环. 我们的问题是: (1) R/I 何时是域? (2) R/I 何时是整环?

先考虑第一个问题. R/I 是域当且仅当它仅有平凡理想 (见例 2.3.24) 至少含两个元, 也当且仅当 R 中没有包含 I 的非平凡理想 (推论 2.3.10) 且 $I \neq R$.

再看第二个问题. R/I 是整环当且仅当它没有零因子 (命题 2.3.2), 即 $[a][b]=[0]$ 总蕴含 $[a]=[0]$ 或 $[b]=[0]$. 这个条件相当于 $ab\in I$ 总蕴含 $a\in I$ 或 $b\in I$.

由此, 我们可以引入两类重要的理想.

定义 2.3.11 设 R 是交换幺环, $I\neq R$ 是 R 的理想.
(1) 如果不存在包含 I 的非平凡理想, 则称 I 是极大理想 (Maximal Ideal).
(2) 如果 I 满足如下性质就称为素理想 (Prime Ideal): $ab\in I$ 总蕴含 $a\in I$ 或 $b\in I$.

上面的讨论相当于说

命题 2.3.11 设 R 是交换幺环, $I\neq R$ 是 R 的理想.
(1) I 是极大理想当且仅当 R/I 是域.
(2) I 是素理想当且仅当 R/I 是整环.

特别地, 极大理想必是素理想.

例 2.3.39 域中的零理想是极大理想; 整环中的零理想是素理想. ■

例 2.3.40 $\mathbb{Z}$ 中的理想 $d\mathbb{Z}=(d)$ 是素理想当且仅当 d 素数, 也当且仅当它是极大理想. ■

例 2.3.41 $\mathbb{Q}[x]$ 中的主理想 $(f(x))$ 是素理想当且仅当 $f(x)$ 是 $\mathbb{Q}[x]$ 内的不可约多项式. 例 2.3.32 表明, 此时 $\mathbb{Q}[x]/(f)$ 同构于某个代数数的扩域, 因而素理想也是极大理想. ■

例 2.3.42 $\mathbb{R}[x,y]$ 中有极大理想 $(x-a,y-b)$. 设 (x^2+y) 是 $\mathbb{R}[x,y]$ 的素理想, 但不是极大理想, 这是因为它严格含于极大理想 $(x,x^2+y)=(x,y)$ 之中. ■

推论 2.3.13 设 R 是交换幺环, $\sigma:R\to S$ 是环的满同态, 则
(1) R 是域当且仅当零理想是极大理想.
(2) R 是整环当且仅当零理想是素理想.
(3) R 中包含 $\mathrm{Ker}\sigma$ 的极大理想与 S 的极大理想一一对应.
(4) R 中包含 $\mathrm{Ker}\sigma$ 的素理想与 S 的素理想一一对应.

证明 (1)(2)(3) 都是显然推论. 我们这里验证 (4).

设 P 是 R 中包含 $\mathrm{Ker}\sigma$ 的素理想. 由推论 2.3.11, 我们有同构 $R/P\cong S/\sigma(P)$. 因为 R/P 是整环, 所以 $S/\sigma(P)$ 也是整环, 因而 $\sigma(P)$ 是 S 的素理想. 反过来, 对 S 中的素理想 K, $R/\sigma^{-1}(K)\cong S/K$ 是整环, 故 $\sigma^{-1}(K)$ 是 R 的素理想. ■

例 2.3.43 由推论 2.3.13 (4), $\mathbb{Z}_N$ 中的素理想必是 $([p])$, 这里 p 是 N 的素因子. ■

命题 2.3.12 设 P 是交换幺环 R 的素理想, 则 $P=\sqrt{P}$.

证明 显然 $P\subseteq\sqrt{P}$. 今证反过来的包含关系. 设 $a\in\sqrt{P}$, 则存在 $m>0$, 使得 $a^m\in P$. 不妨设这样的 m 取到最小. 如果 $m>1$, 那么 $a^m=a\cdot a^{m-1}\in P$. 由于 P 是素理想, 因此 $a\in P$ 或 $a^{m-1}\in P$, 与 m 的最小性矛盾! 故 $m=1$, 即 $a\in P$. 这就推出 $\sqrt{P}\subseteq P$. ■

定理 2.3.5 (**素理想存在性**) 设 R 是交换幺环, $a\in R$ 不是幂零元, 则 R 中存在一个素理想 P, 使得 P 不含 a 的任何方幂 a^m, $m>0$.

这个结论的证明需要用到集合论中的佐恩引理. 我们此处不再详细展开了.

定理 2.3.6 (**极大理想存在性**) 任何交换幺环都含有极大理想.

证明 在定理 2.3.5 中取 $a = 1$ 即得. ■

推论 2.3.14 设 R 是交换幺环, 则 R 的所有素理想的交, 记作 $r(R)$, 恰好是由 R 的全体幂零元组成, 即 $r(R) = \sqrt{(0)}$. 它称作诣零根 (Nilradical).

证明 设 a 是幂零元, $a^m = 0$. 设 P 是 R 的任何素理想, 存在整数 $r > 0$, 使得 $a^r \in P$. 由命题 2.3.12, $a \in \sqrt{P} = P$. 由 P 的任意性, $a \in r(R)$.

反之, 设 $a \in r(R)$. 如果 a 不是幂零元, 则存在不包含 a 的素理想 P, 因而 $a \notin r(R)$, 矛盾! 故 a 必是幂零元. ■

2.3.8 构造方法 (V): 环的直和

对任何环 $R_1, \cdots, R_r$, 我们考虑笛卡尔积

$$R_1 \times \cdots \times R_r = \{(a_1, \cdots, a_r) |\ a_i \in R_i,\ i = 1, \cdots, r\}.$$

现在我们要在上述集合上引入加法和乘法运算:

$$(a_1, \cdots, a_n) + (b_1, \cdots, b_n) := (a_1 + b_1, \cdots, a_r + b_r),$$
$$(a_1, \cdots, a_n) \cdot (b_1, \cdots, b_n) := (a_1 \cdot b_1, \cdots, a_r \cdot b_r).$$

可以验证这是一个环, 其零元素为 $(0_{R_1}, \cdots, 0_{R_r})$. 它称为环 $R_1, \cdots, R_r$ 的直和 (Direct sum), 我们把它重新记为

$$R := R_1 \oplus \cdots \oplus R_r.$$

如果 $R_1, \cdots, R_r$ 都是交换幺环, 那么直和 R 也是交换幺环, 其幺元素为 $1_R = (1_{R_1}, \cdots, 1_{R_r})$.

例 2.3.44 回顾例 2.3.4,

$$R = \left\{ \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix} \in M_n(F) \,\middle|\, a_i \in F,\ i = 1, \cdots, n \right\},$$

这里 F 是给定的数域.

我们可以构造同构映射

$$\sigma : R \longrightarrow \underbrace{F \oplus F \oplus \cdots \oplus F}_{n}, \quad \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix} \mapsto (a_1, \cdots, a_n).$$ ■

例 2.3.45 (中国剩余定理) 设 $1 < m_1 < m_2 < \cdots < m_r$ 是 r 个两两互质的整数, $M = m_1 m_2 \cdots m_r$. 中国剩余定理断言如下同余方程组

$$\begin{cases} x \equiv n_1, & (\mathrm{mod}\ m_1), \\ x \equiv n_2, & (\mathrm{mod}\ m_2), \\ \cdots\cdots & \cdots\cdots \\ x \equiv n_r, & (\mathrm{mod}\ m_r) \end{cases}$$

在模 M 下有唯一剩余类解 $x \equiv n\ (\mathrm{mod}\ M)$. 翻译成剩余类环的语言, 就是说, 存在唯一的元素 $[n]_M \in \mathbb{Z}_M$, 满足 $[n]_{m_i} = [n_i]_{m_i} \in \mathbb{Z}_{m_i}$. 确切地说, 中国剩余定理的代数版本如下:

$$\mathbb{Z}_M \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}.$$

我们来证明这个结论.

今构造映射

$$\sigma : \mathbb{Z}_M \longrightarrow \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}, \quad [n]_M \to ([n]_{m_1}, [n]_{m_2}, \cdots, [n]_{m_r}).$$

首先说明映射的合理性. 设 $[n]_M = [n']_M$. 由定义, $M \mid (n - n')$. 因而 $m_i \mid (n - n')\ (\forall i)$, 即 $[n]_{m_i} = [n']_{m_i}$.

容易验证, σ 是环同态. 今证它是单同态. 设 $[n]_M \in \mathrm{Ker}\sigma$, 即 $[n]_{m_i} = [0]_{m_i}\ (\forall i)$, 亦即 $m_i \mid n\ (\forall i)$. 由于诸 m_i 是两两互质的, 所以 $M \mid n$, 即 $[n]_M = [0]_M$.

注意到 $\mathbb{Z}_M$ 有 M 个元素, $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}$ 的元素个数为 $m_1 \cdot m_2 \cdots m_r = M$. 因为 σ 是单射, 所以这意味着 σ 也是满射. 因此这就证明了 σ 是同构.

特别地, 设 $M > 1$ 是正整数, 有标准的素因子分解式

$$M = p_1^{\alpha_1} \cdots p_s^{\alpha_s},$$

这里 $p_1 < \cdots < p_s$ 都是素数. 那么我们有

$$\mathbb{Z}_M \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\alpha_s}}.$$

这一分解在适当的顺序下是唯一的. ■

注 2.3.13 直和 $R = R_1 \oplus \cdots \oplus R_r$ 中有 r 个理想:

$$R_i' = \{(0, \cdots, a_i, \cdots, 0) |\ a_i \in R_i\}, \quad i = 1, \cdots, r.$$

容易验证, $R_i \cong R_i'$. ■

例 2.3.46 设 R_1, R_2 是交换幺环, 则 $R = R_1 \oplus R_2$ 有零因子 $(1,0)$ 和 $(0,1)$, 因而不可能是整环. 对任何理想 $I \subseteq R$, 我们都有 $I = I_1 \oplus I_2$, 这里 I_i 是 R_i 的理想 $(i = 1, 2)$. 进一步, 由同态基本定理可得

$$R/I \cong R_1/I_1 \oplus R_2/I_2.$$

由此可知, R 中的素理想 (相应地, 极大理想) 都可以写为 $R_1 \oplus P_2$ 或 $P_1 \oplus R_2$, 这里 P_i 是 R_i 的素理想 (相应地, 极大理想). ■

2.4 整环上的整除理论

在这一章中, 我们将初等数论里的整除理论推广到更一般的整环上.

2.4.1 基本概念与性质

以下各节中, 我们均假设 R 是整环. 首先, 我们引入整除的概念.

定义 2.4.1 设 $a,b\in R$. 如果存在 $c\in R$, 使得 $a=bc$, 则称 b 整除 a, 简记作 $b\mid a$. a 称为 b 的倍数, b 称为 a 的因子.

整除关系满足
(1) (自反性) $a\mid a$.
(2) (传递性) 若 $c\mid b$, $b\mid a$, 则 $c\mid a$.
(3) 若 $c\mid a$, $c\mid b$, 则 $c\mid au+bv$, $\forall u,v\in R$.
(4) $1\mid a$, $a\mid 0$.

例 2.4.1 (1) $R=\mathbb{Z}$ 上有经典的整除概念. $b\mid a$ 相当于 $\frac{a}{b}\in\mathbb{Z}$.
(2) $R=\mathbb{Z}[\sqrt{-1}]$ 中, $(1+\sqrt{-1})\mid 2$, 因为 $2=(1+\sqrt{-1})(1-\sqrt{-1})$.
(3) $R=\mathbb{Q}[x]$ 中, $x^2+1\mid x^4-1$. ■

定义 2.4.2 (1) 如果 $b\mid a$, 且 $a\mid b$, 则称 a,b 是相伴的.
(2) 如果 $b\mid a$, $a\nmid b$, 且 b 不是乘法可逆元, 则称 b 是 a 的真因子.

可以验证: 相伴关系是等价关系. 为方便起见, 我们通常用 $a\sim b$ 表示 a,b 相伴.

命题 2.4.1 (1) a,b 是相伴的非零元的充分必要条件是存在乘法可逆元 u, 使得 $a=bu$.
(2) $v\in R$ 是乘法可逆元当且仅当 v 与 1 相伴. 我们也称这样的元素为单位.
(3) $b\mid a$ 当且仅当 $(a)\subseteq(b)$. 特别地, a,b 相伴当且仅当 $(a)=(b)$.

证明 (2) 是 (1) 的直接推论. 下面证明 (1).

($\Longrightarrow$) 设 $a=bu$, $b=av$, $u,v\in R$. 我们有 $a=auv$. 因为 $a\neq 0$, 故由消去律得 $1=uv$.

($\Longleftarrow$) 由 $b=au^{-1}$ 立得.

(3) 是显然的. ■

定义 2.4.3 设 a 是非零非单位的元素,
(1) 如果 a 没有真因子, 则称之为不可约元.
(2) 如果从 $a\mid bc$, 恒能推出 $a\mid b$ 或 $a\mid c$, 则称 a 为素元.

例 2.4.2 (1) $\mathbb{Z}$ 中的单位是 ±1. 两个整数相伴当且仅当 $|a|=|b|$. 素数是 $\mathbb{Z}$ 中的不可约元, 也是素元.
(2) 域 F 的多项式环 $F[x]$ 中的单位是 F 中的所有非零元. $F[x]$ 中的不可约多项式是不可约元, 也是素元. ■

例 2.4.3　取 $R=\mathbb{Z}[\sqrt{-5}]$, 设 $a=s+r\sqrt{-5}\in R$ 是非零元. 我们定义

$$N(a)=|a|^2=s^2+5r^2\in\mathbb{Z}$$

它称为 a 的范数. $N(a)=1$ 当且仅当 $a=\pm1$. 如果 $a\neq\pm1$, 则 $N(a)\geq 4$.

我们来证明 2 是不可约元, 但不是素元.

假设 $2=bc$, $b,c\in\mathbb{Z}[\sqrt{-5}]$. 于是

$$4=N(2)=N(b)N(c).$$

因此 $N(b),N(c)$ 中有一个等于 1. 因此 b,c 中有一个是可逆元. 因而 a 是不可约的.

注意

$$2\mid 6=(1+\sqrt{-5})(1-\sqrt{-5}).$$

假如 $2\mid 1\pm\sqrt{-5}$, 那么 $N(2)\mid N(1\pm\sqrt{-5})$ (整数环内), 即 $4\mid 6$, 矛盾! 故 $2\nmid 1\pm\sqrt{-5}$. ■

命题 2.4.2　(1) *$a\in R$ 是素元当且仅当 (a) 是非零素理想.*
(2) *素元必是不可约元.*

证明　(1) ($\Longrightarrow$) 设 a 是素元. 假设对 $b,c\in R$, 有 $bc\in(a)$. 这相当于 $a\mid bc$. 由于 a 是素元, 故 $a\mid b$ 或 $a\mid c$, 即 $b\in(a)$ 或 $c\in(a)$. 因此 (a) 是非零素理想.

($\Longleftarrow$) 假设对 $b,c\in R$, 有 $a\mid bc$. 这相当于 $bc\in(a)$. 由于 (a) 是素理想, 因此 $b\in(a)$, 或 $c\in(a)$, 即 $a\mid b$, $a\mid c$. 因此 a 是素元.

(2) 设 a 是素元. 假设 $a=bc$, 且 b,c 是真因子. 因此 $a\mid b$, 或 $a\mid c$. 这就迫使 a,b 相伴或者 a,c 相伴, 矛盾! 故 a 是不可约元. ■

定义 2.4.4　*若 $c\mid a$, $c\mid b$, 则 c 称作 a,b 的公因子. 如果公因子 c 还满足以下性质, 则称为最大公因子: 对 a,b 的任何公因子 c', 恒有 $c'\mid c$.*

上述概念与 $\mathbb{Z}$ 或 $F[x]$ (F 是数域) 中的定义是完全一致的. 对一般的交换幺环来说, 任何两个元 a,b 总有公因子 1, 但是 a,b 未必有最大公因子.

例 2.4.4　在 $\mathbb{Z}[\sqrt{-5}]$ 中, 取 $a=6$, $b=2(1+\sqrt{-5})$. 2 和 $1+\sqrt{-5}$ 都是 a,b 的公因子. 但是 $2\nmid 1+\sqrt{-5}$ 且 $1+\sqrt{-5}\nmid 2$. 因此 $2,1+\sqrt{-5}$ 都不是最大公因子. 我们说明 a,b 没有最大公因子.

假设存在最大公因子 c. 那么

$$2\mid c,\quad 1+\sqrt{-5}\mid c,\quad c\mid b,$$

从而 $4\mid N(c)$, $6\mid N(c)$, $N(c)\mid 24$ (在整数环中). 这表明 $N(c)=12,24$.

设 $d\in\mathbb{Z}[\sqrt{-5}]$, 满足 $b=cd$. 如果 $N(c)=12$, 则 $N(d)=2$, 这不可能 (因为非可逆元的范数至少是 4). 如果 $N(c)=24$, 则 $N(d)=1$, 即 $d=\pm1$, 因而 $c=\pm b$. 这蕴含着 $b\mid a$, 矛盾! 因此 a,b 没有最大公因子. ■

2.4.2　特殊整环 (I): 欧几里德整环

我们先来研究一种非常特殊的整环.

定义 2.4.5　设 R 是整环, $R^*=R\setminus\{0\}$. 如果存在一个 R^* 上取值于正整数的函数 $d(x)$, 使得对任何元素 $a,b\in R$, $b\neq 0$, 都存在一对元素 $q,r\in R$, 满足

$$a=qb+r, \tag{2-5}$$

其中要么 $r=0$, 要么 $r\neq 0$ 且 $d(r)<d(b)$, 那么 R 称为欧几里德整环 (Euclidean domain).

例 2.4.5　先举两个经典例子.
(1) $R=\mathbb{Z}$ 是欧几里德整环, 我们取 $d(a)=|a|$, $\forall a\in R^*$. 此时 (2-5) 就是通常的带余除法.
(2) $R=F[x]$ (F 是域), 我们取 $d(f):=1+\deg f$. 此时 (2-5) 就是定理 2.3.3 中的带余数除法. ■

例 2.4.6 (**高斯整数环**)　设 $R=\mathbb{Z}[\sqrt{-1}]$. 对任何 $a=u+v\sqrt{-1}\in R$, 取 $d(a)=|a|^2=u^2+v^2$. 现在我们来验证带余除法 (2-5), 因而 $\mathbb{Z}[\sqrt{-1}]$ 是欧几里德整环. 设 $\alpha,\beta\in R$, $\beta\neq 0$. 令

$$\frac{\alpha}{\beta}=s+t\sqrt{-1},\quad s,t\in\mathbb{Q}.$$

取整数 u,v, 满足 $|s-u|\leq\frac{1}{2}$, $|t-v|\leq\frac{1}{2}$. 令

$$q=u+v\sqrt{-1},\quad r_1=(s-u)+(t-v)\sqrt{-1},$$

则得 $\frac{\alpha}{\beta}=q+r_1$, 因而

$$\alpha=q\beta+r_1\beta.$$

因为 $\alpha,q,\beta\in\mathbb{Z}[\sqrt{-1}]$, 故 $r_1\beta\in\mathbb{Z}[\sqrt{-1}]$.

注意

$$d(r_1)=(s-u)^2+(t-v)^2\leq\frac{1}{4}+\frac{1}{4}<1.$$

因此 $d(r_1\beta)=d(r_1)d(\beta)<d(\beta)$. 取 $r=r_1\beta$, 由此即得式 (2-5).

比如 $\alpha=3$, $\beta=1+\sqrt{-1}$, 则 $\alpha=q\beta+r$ 满足 (2-5), 这里 $q=2-2\sqrt{-1}$, $r=-1$. 但我们也有 $\alpha=q'\beta+r'$, 这里 $q'=1-\sqrt{-1}$, $r'=1$. 它也满足式 (2-5). 这表明欧几里德整环定义的带余除法未必是唯一的. ■

例 2.4.7　仿照 2.4.5, 我们可以验证 $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$ 都是欧几里德整环. ■

例 2.4.8　令 $\theta=-\frac{1}{2}+\frac{\sqrt{-3}}{2}$ 是三次单位根. 考虑整环$R=\mathbb{Z}[\theta]=\{a+b\theta|\ a,b\in\mathbb{Z}\}$. 由环同态基本定理可知, $\mathbb{Z}[\theta]\cong\mathbb{Z}[x]/(x^2+x+1)$. 对任何 $a=s+t\theta\in\mathbb{Z}[\theta]$, 取函数 $d(a)=|a|^2=s^2-st+t^2$. 对 $\alpha,\beta\in R$, $\beta\neq 0$, 设

$$\frac{\alpha}{\beta}=s+t\theta,\quad s,t\in\mathbb{Q}.$$

先取整数 v, 满足 $|t-v|\leq\frac{1}{2}$, 再取整数 u, 满足 $|2s-t-2u+v|\leq 1$. 令

$$q=u+v\theta,\quad r_1=(s-u)+(t-v)\theta.$$

类似前例可证 $r_1\beta\in\mathbb{Z}[\theta]$. 由计算得

$$d(r_1)=(s-u)^2-(s-u)(t-v)+(t-v)^2=\left(\frac{2s-t-2u+v}{2}\right)^2+3\left(\frac{t-v}{2}\right)^2\leq\frac{1}{4}+\frac{3}{16}<1.$$

因此 $d(r_1\beta)<d(\beta)$. 这就证明了 R 是欧几里德整环. ■

2.4.3 特殊整环 (II): 主理想整环

定义 2.4.6 *如果整环 R 中的任何理想都是主理想, 则称 R 为主理想整环* (Principal ideal domain).

我们先证明如下重要结论.

定理 2.4.1 *欧几里德整环是主理想整环.*

证明 设 R 是欧几里德整环, $d(x)$ 是定义 2.4.5 中的函数. 设 I 是 R 的理想.若 I 是零理想 (0) 或环 $R = (1)$, 则显然是主理想. 以下不妨设 I 不是平凡理想. 在 I 中取一个非零元 b, 使得 $d(b)$ 达到最小, 即 $d(b) \leq d(r)$, $\forall r \in I$. 对 I 中任何元素 a, 由于 R 是欧几里德整环, 故 $a = bq + r$, 其中 $r = 0$ 或 $d(r) < d(b)$. 因此 $r = a - bq \in I$. 由 $d(b)$ 的最小性, 即得 $r = 0$, 即 $a \in (b)$,由此得 $I \subseteq (b)$. 另一方面, 显然有 $(b) \subseteq I$, 因此 $(b) = I$. ■

例 2.4.9 任何域都是主理想整环, 因为它只有平凡理想 (0) 和 (1). ■

例 2.4.10 $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-1}]$, $F[x]$ (这里 F 是域) 等等都是主理想整环, 因为它们是欧几里德整环. ■

命题 2.4.3 *设 R 是主理想整环, 则*
(1) *如果 a 是不可约元, 那么 (a) 是极大理想.*
(2) *不可约元就是素元.*
(3) *每个非零素理想都是极大理想.*
(4) *设理想 $(a, b) = (d)$, 则 d 是 a, b 的最大公因子.*

证明 (1) 设 a 是不可约元. I 是 R 中包含 (a) 的理想. 因为 R 是主理想整环, 故可设 $I = (b)$, 从而 $(a) \subseteq (b)$. 这就是说, $a = bc$, 这里 $c \in R$. 因为 a 不可约, 所以要么 a, b 相伴, 要么 b 是乘法可逆元 (见命题 2.4.1). 这相当于 $I = (a)$ 或 $I = R$.

(2) 由 (1) 知, (a) 也是素理想, 因此再由命题 2.4.2, 即知 a 是素元.

(3) 设 P 是 R 的非零素理想. 因为 R 是主理想整环, 故 $P = (d)$. 再由命题 2.4.2, d 是素元, 因而是不可约元. 再由 (1) 知 $P = (a)$ 是极大理想.

(4) 因为 $(a) \subseteq (d)$, 所以 $d \mid a$. 同理 $d \mid b$. 设 c 也是 a, b 的公因子, $(a) \subseteq (c)$, $(b) \subseteq (c)$. 因此 $(d) = (a, b) \subseteq (c)$, 即 $c \mid d$. ■

例 2.4.11 欧几里德整环中的不可约元都是素元. ■

例 2.4.12 证明: $(2, x^2 + 1)$ 不是 $\mathbb{Z}[x]$ 的主理想.

假设 $(2, x^2 + 1) = (f(x))$, 则由 $2 \in (f)$, 可知 $f \mid 2$, 从而 $f(x) = \pm 1, \pm 2$ 是常值多项式. 但是另一方面, $f \in (2, x^2 + 1)$ 蕴含着 $f(x) = 2u(x) + (x^2 + 1)v(x)$, 这里 $u, v \in \mathbb{Z}[x]$. 取 $x = 1$, 即得 $f(1) = 2(u(1) + v(1))$, 这就蕴含着 $f(x) = \pm 2$. 也就是说, $(2, x^2 + 1) = (2)$, 从而 $x^2 + 1 \in (2)$, 即 $2 \mid x^2 + 1$, 矛盾! ■

推论 2.4.1 设 R 是主理想整环, a 非零非单位的元. 那么以下条件彼此等价:
(1) a 是素元,
(2) a 是不可约元,
(3) $R/(a)$ 是整环,
(4) $R/(a)$ 是域.

例 2.4.13 (**高斯整环中的素元**) 因为 $\mathbb{Z}[\sqrt{-1}]$ 是主理想整环, 所以它的不可约元和素元是一回事. 我们来证明: 它们有以下几类 (在相伴意义下):
(1) $1+\sqrt{-1}$,
(2) $a+b\sqrt{-1}$, 这里 $p=a^2+b^2$ 是 $\mathbb{Z}$ 中模 4 余 1 的素数,
(3) p, 这里 p 是 $\mathbb{Z}$ 中模 4 余 3 的素数.

首先验证上面三类高斯整数是不可约的. 我们记 $N(a+b\sqrt{-1})=a^2+b^2$. 设 π 是 (1)(2) 类型. 如果 $\pi=\alpha\cdot\beta$, 则

$$p=N(\pi)=N(\alpha)N(\beta)$$

蕴含着 $N(\alpha),N(\beta)$ 中的一个等于 1, 也就是说 α,β 中有一个是单位元. 因此 π 是不可约的.

设 π 是类型 (3), $\pi=\alpha\cdot\beta$, 则

$$p^2=N(\pi)=N(\alpha)N(\beta).$$

如果 $p=N(\alpha)=N(\beta)$, 这就推出 p 可以表为两整数的平方和, 因而 $p\equiv 1 \pmod 4$, 矛盾! 因此 $N(\alpha),N(\beta)$ 中的一个等于 1, 再次推出 π 是不可约的.

其次证明每个不可约元必相伴于其中一类. 设 π 是不可约元. 将 $N(\pi)$ 在整数内分解为素数乘积

$$N(\pi)=\pi\bar{\pi}=p_1p_2\cdots p_s,$$

这里诸 p_k 是素数 (允许相同). 在 $\mathbb{Z}[\sqrt{-1}]$ 里看, 由于 π 也是素元, 所以 $\pi\mid p_k$ 对某个 p_k 成立. 因此 $N(\pi)\mid N(p_k)=p_k^2$. 如果 $N(\pi)=p_k$, 设 $\pi=a+b\sqrt{-1}$, 则 $p_k=a^2+b^2$, 这表明 π 相伴于类型 (1)(2) 的不可约元.

如果 $N(\pi)=p_k^2$, 那么由 $N(p_k)=p_k^2$ 可知 π,p_k 相伴. 因而 p_k 必须是类型 (3) 的不可约元 (否则由前面讨论, 它可以被前两类不可约元整除). ■

注 2.4.1 费马和欧拉证明: 整数中模 4 余 1 的奇素数都可以写成两个平方数的和, 其余的奇素数不可能写成两个平方数之和. 我们这里给一个简要证明. 如果奇素数 p 可以写作两个平方数之和 $p=a^2+b^2$, 则显然 a,b 一奇一偶, 因而 a^2,b^2 在模 4 下一个为 1, 另一个为 0, 这就推出 p 模 4 余 1.

反过来, 假设 p 是模 4 余 1 的奇素数. 根据平方剩余的结论, 可找到 x 满足 $p\mid x^2+1$. 因此在 $\mathbb{Z}[\sqrt{-1}]$ 中, $p\mid(x+\sqrt{-1})(x-\sqrt{-1})$. 因为 $\frac{x}{p}\pm\frac{1}{p}\sqrt{-1}\notin\mathbb{Z}[\sqrt{-1}]$, 所以 $p\nmid x\pm\sqrt{-1}$ (在 $\mathbb{Z}[\sqrt{-1}]$ 中), 这表明 p 不是素元, 因此不是不可约的 (推论 2.4.1). 不妨假设 $p=\alpha\beta$, $\alpha,\beta\in\mathbb{Z}[\sqrt{-1}]$ 是真因子. 因此 $p^2=N(p)=N(\alpha)N(\beta)$. 由假设, $N(\alpha)$ 和 $N(\beta)$ 都大于 1, 所以 $N(\alpha)=N(\beta)=p$. 不妨设 $\alpha=a+b\sqrt{-1}$, 所以 $p=a^2+b^2$. ■

例 2.4.14 设 $R=\mathbb{Z}[\sqrt{-1}]$.

(1) 验证 $I_1=(1+2\sqrt{-1})$ 是极大理想.

这是因为 $1+2\sqrt{-1}$ 是素元, R 是主理想整环, 所以由推论 2.4.1 可知 I_1 是极大理想.

(2) 验证 $I_2=(1+3\sqrt{-1})$ 不是素理想. 这是因为 $1+3\sqrt{-1}=(1+\sqrt{-1})(2+\sqrt{-1})$ 不是不可约的, 所以推论 2.4.1 推知 I_2 不是素理想.

事实上, 我们也能直接验证商环 R/I_2 有零因子. 今设 $\theta=[\sqrt{-1}]\in R/I_2$. θ 满足如下关系式

$$[1]+[3]\theta=[0],\quad \theta^2=[-1].$$

因此

$$[-9]=[9]\cdot[-1]=[9]\theta^2=([3]\theta)^2=(-[1])^2=[1].$$

这就推出 $[2]\cdot[5]=[10]=[9]-[-1]=[0]$. 假若 $[2]=[0]$, 则 $1+3\sqrt{-1}\mid 2$, 从而 $N(1+3\sqrt{-1})\mid N(2)$, 矛盾! 故 $[2]\neq[0]$. 类似可得 $[5]\neq[0]$. 这表明 $[2],[5]$ 是 R/I_2 的零因子. ■

定义 2.4.7 设 R 是整环,

(1) 如果理想序列 $\{I_i\}_{i=1}^{\infty}$ 满足

$$I_1\subseteq I_2\subseteq\cdots\subseteq I_i\subseteq\cdots$$

我们就说 $\{I_i\}_{i=1}^{\infty}$ 是理想升链. 如果存在 $m>0$, 使得 $I_m=I_{m+1}=\cdots$, 则称该理想升链满足诺特条件.

(2) 如果 R 中的元素序列 $\{a_i\}_{i=1}^{\infty}$ 满足

$$a_{i+1}\mid a_i,\quad i=1,2\cdots.$$

我们就说 $\{a_i\}_{i=1}^{\infty}$ 是因子降链. 如果存在 $m>0$, 使得 $a_m\sim a_{m+1}\sim\cdots$ (即彼此相伴), 则称该因子降链满足因子链条件.

显然, 在主理想整环中, 因子降链 $\{a_i\}_{i=1}^{\infty}$ 对应主理想升链 $\{(a_i)\}_{i=1}^{\infty}$; 反之亦然.

命题 2.4.4 设 R 是主理想整环, 则

(1) 任一理想升链 $\{(a_i)\}$ 都满足诺特条件.

(2) 任一因子降链 $\{a_i\}$ 都满足因子链条件.

证明 (1)(2) 是等价的. 我们只需证 (1).

令 $I=\cup_{i=1}^{\infty}(a_i)$. 首先说明 I 是理想. 任取 $a,b\in I$, 不妨设 $a\in(a_r)$, $b\in(a_s)$), $r\leq s$. 由于 $(a_r)\subseteq(a_s)$, 所以 $a-b\in(a_s)\subseteq I$. 对任何 $c\in R$, 我们有 $ca\in(a_r)\subseteq I$. 这就证明了 I 是理想.

由于 R 是主理想整环, 所以 $I=(d)$. 由 $d\in I$ 知, $d\in(a_m)$ (对某个正整数 m), 因而 $I=(d)\subseteq(a_m)$. 反过来显然有 $(a_m)\subseteq I$. 这就推出 $I=(a_m)$. 因此 $(a_m)=(a_{m+1})=\cdots$. ■

2.4.4 特殊整环 (III): 唯一因子分解整环

定义 2.4.8 设 R 是整环, 如果 R 满足如下两个条件, 则 R 称为唯一因子分解整环 (Unique factorization domain), 或高斯整环:

(1) R 任一非零非单位的元素 a 总可以写为有限多个不可约元的积

$$a=p_1p_2\cdots p_s.$$

(2) 上述分解在相伴意义下是唯一的, 即若 a 由另一不可约因子的分解

$$a = q_1 q_2 \cdots q_r,$$

则 $r = s$, 且在合适的排序下, p_i, q_i 是相伴的 $(i = 1, 2, \cdots, s)$.

定理 2.4.2　整环 R 如果满足如下两个条件, 则必是唯一因子分解整环:
(i) 因子链条件.
(ii) 每个不可约元都是素元.

证明　先证明每个非零非单位元都可以分解成有限个不可约元的乘积. 假若存在一个非零非单位元 $a \in R$, 它不满足此性质, 那么它是可约的. 设 $a = bc$, b, c 是 a 的真因子. 此时 b, c 中必有一个仍然不能分解成有限个不可约元的乘积, 否则就与 a 的选取矛盾! 不妨设 b 是这样的元素, 因而它也是可约的. 依次类推, 我们可以得到一个因子降链$a, b, \cdots$, 其中每一项都是前一项的真因子. 这就与因子链条件矛盾! 故不存在这样的 a.

再证上述不可约元分解式的唯一性 (在相伴意义下). 设 $\pi \in R$, 假设有两种不可约元分解式

$$\pi = p_1 p_2 \cdots p_s = q_1 q_2 \cdot q_r.$$

因为 $q_1 \mid \pi$, 且 q_1 也是素元, 所以由第一个分解式可知 $q_1 \mid p_i$ (对某个下标 i). 注意到 p_i 是不可约的, 所以 p_i, q_1 必是相伴的. 通过合适的排序, 我们可以假设 $i = 1$, 即 p_1, q_i 相伴, 亦即 $u = p_1/q_1$ 是单位.

$$u p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_r.$$

重复上述讨论, 在有限步后, 我们得到 p_i, q_i 相伴, $r = s$ (经过适当的排序). ■

推论 2.4.2　主理想整环必是唯一因子分解整环. 特别地, 欧几里德整环必是唯一因子分解整环.

唯一因子分解整环和整数环一样, 我们可以在上面讨论算术基本定理 (来自定义).

例 2.4.15 (**高斯整数环**)　$\mathbb{Z}[\sqrt{-1}]$ 是欧几里德整环, 因而是主理想整环, 进而是唯一因子分解整环. 因此每个高斯整数都有素因子分解式, 且在相伴意义下是唯一的. 设

$$\alpha = 3 + \sqrt{-1}, \quad \beta = 2.$$

我们有素因子分解 (在相伴意义下)

$$\alpha = -\sqrt{-1} \cdot (1 + \sqrt{-1}) \cdot (1 + 2\sqrt{-1}), \quad \beta = -\sqrt{-1}(1 + \sqrt{-1})^2,$$

这里 $-\sqrt{-1}$ 是单位, $1 + \sqrt{-1}$ 和 $1 + 2\sqrt{-1}$ 都是素元. 由此易知 α, β 的最大公因子 (在相伴意义下) 为 $1 + \sqrt{-1}$. ■

例 2.4.16　类似地, $\mathbb{Z}[\theta]$ (θ 是三次单位根) 也是唯一因子分解整环. 利用这个环和 $\mathbb{Z}[\sqrt{-1}]$ 的算术基本定理 (即唯一分解性), 可以证明三次和四次费马方程无整数解:

$$X^n + Y^n = Z^n, \quad XYZ \neq 0, \quad n = 3, 4.$$

限于篇幅, 此处不再详细展开. ■

例 2.4.17　$\mathbb{Z}[\sqrt{-5}]$ 不是唯一分解整环, 比如

$$6 = 2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$$

是两种不同的分解. ■

定理 2.4.3　*若 R 是唯一因子分解整环, 那么 $R[x]$ 也是唯一因子分解整环.*

2.5 非交换幺环

在这一节中, 我们简要介绍一些非交换的幺环, 即不满足乘法交换律的含幺环.

2.5.1 一些简单例子

例 2.5.1　这里举几个简单例子.
(1) 任何体都是非交换幺环. 特别地, 四元数体是非交换幺环.
(2) 考虑四元数体的子幺环

$$R = \{a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H} \mid a, b, c, d \in \mathbb{Z}\}.$$

它是非交换幺环. ■

例 2.5.2　回顾例 2.1.4. 考虑数域 F 上的 $n(\geq 2)$ 维线性空间 V. V 上的*线性变换* 全体组成的集合 $\mathrm{End}_n(V)$ 在加法运算

$$f + g : V \longrightarrow V, \quad v \to (f+g)(v) := f(v) + g(v).$$

以及复合运算

$$(f \cdot g) : V \longrightarrow V, \quad v \to (f \cdot g)(v) := f(g(v))$$

下构成非交换幺环. 它的零映射是加法零元, 恒同映射是乘法幺元. ■

例 2.5.3　回顾例 2.1.3. 数域 F 上 n 阶方阵全体构成的集合

$$M_n(F) := \left\{ \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix} \middle| \, a_{ij} \in F \right\}.$$

在通常的矩阵加法和乘法下构成非交换幺环, 其零元是零矩阵, 幺元是单位矩阵. ■

2.5.2 矩阵环

这里我们要利用已知的含幺环构造出新的非交换幺环. 设 R 是任一含幺环. 我们定义 R 上的 n 阶矩阵

$$A = \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix},$$

这里诸系数 $a_{ij} \in R$. R 上的全体 n 阶矩阵构成的集合记作 $M_n(R)$.

我们定义 $M_n(R)$ 上的加法运算

$$\begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} & \cdots & \cdots & b_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & \cdots & \cdots & b_{nn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & \cdots & \cdots & a_{1n}+b_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1}+b_{n1} & \cdots & \cdots & a_{nn}+b_{nn} \end{pmatrix}$$

以及乘法运算

$$\begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & \cdots & \cdots & b_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & \cdots & \cdots & b_{nn} \end{pmatrix} = \begin{pmatrix} \sum\limits_{k=1}^{n} a_{1k}b_{k1} & \cdots & \cdots & \sum\limits_{k=1}^{n} a_{1k}b_{kn} \\ \cdots & \cdots & \cdots & \cdots \\ \sum\limits_{k=1}^{n} a_{nk}b_{k1} & \cdots & \cdots & \sum\limits_{k=1}^{n} a_{nk}b_{kn} \end{pmatrix}$$

我们还能定义零矩阵和单位矩阵

$$O = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix}, \quad I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

类似高等代数的讨论, 我们可以验证 $M_n(R)$ 是非交换的幺环, O 是零元, I 是幺元. 我们称之为 R 上的**矩阵环**.

注 2.5.1 (1) 即使 R 是交换幺环, $M_n(R)$ 也不满足交换律.
(2) 当 R 是非交换幺环时, 在矩阵的乘法定义中, $\sum\limits_{k=1}^{n} a_{ik}b_{kj}$ 不能写成 $\sum\limits_{k=1}^{n} b_{kj}a_{ik}$. ■

例 2.5.4 我们可以利用已学过的幺环构造一系列矩阵环, 比如

$$M_n(\mathbb{Z}), \quad M_n(\mathbb{H}), \quad M_n(\mathbb{Z}_n), \cdots$$

例 2.5.5 四元数体 $\mathbb{H}$ 显然是 $M_n(\mathbb{C})$ 的子幺环. ■

例 2.5.6 设 R 是幺环, $R_1 = M_n(R)$ 是 R 上的矩阵环, 我们可以继续构造 R_1 上的矩阵环 $M_m(R_1)$. $M_m(R_1)$ 中的矩阵形如

$$\begin{pmatrix} A_{11} & \cdots & \cdots & A_{1m} \\ \cdots & \cdots & \cdots & \cdots \\ A_{m1} & \cdots & \cdots & A_{mm} \end{pmatrix},$$

这里 $A_{ij} \in R_1$ 是 R 上的 n 阶矩阵. $M_m(R_1)$ 中的矩阵实际上就是所谓的**分块矩阵**. ■

在 R 是交换幺环时, 我们也能仿照高代情形, 定义矩阵

$$A = \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix},$$

的行列式

$$\det A := \sum_{i_1 \cdots i_n} \operatorname{sgn}(i_1 \cdots i_n) a_{1i_1} a_{2i_2} \cdots a_{ni_n}.$$

这里 $(i_1 \cdots i_n)$ 取遍所有的 n 阶置换, $\mathrm{sgn}(i_1 \cdots i_n)$ 是符号. 类似可以定义代数余子式和伴随矩阵等等.

命题 2.5.1　设 R 是交换幺环, $A, B \in M_n(R)$, 则
(1) $\det AB = \det A \cdot \det B$.
(2) A 是 $M_n(R)$ 中的单位 (即乘法可逆元) 当且仅当 $\det A$ 是 R 中的单位. 特别地, 如果 R 是域, 那么 A 可逆的充要条件是 $\det A \neq 0$.

2.6 无幺环

前面我们讨论的环都含有幺元. 这一节将介绍无幺环.

2.6.1 一些例子

这里我们举一些简单例无幺环例子.

例 2.6.1　任何交换幺环 R 中的非平凡理想 I 都是无幺环. 比如$n\mathbb{Z}$ 就是无幺环. ■

例 2.6.2　设 $R_1, \cdots, R_r$ 是环, 并且其中至少有一个是无幺环, 那么直和

$$R_1 \oplus \cdots \oplus R_r$$

是无幺环. ■

例 2.6.3　考虑 $\mathbb{Q}[x]$ 的子幺环

$$\mathbb{Q}[x^2] = \{f(x) \in \mathbb{Q}[x] \mid f(x) = f(-x)\}.$$

$\mathbb{Q}[x^2]$ 中的元实际上就是只出现偶次幂的多项式. 现在考虑 $\mathbb{Q}[x^2]$ 的理想

$$I = \{f(x) \in \mathbb{Q}[x^2] \mid f(0) = 0\}.$$

I 是无幺环. 另外, I 作为 $\mathbb{Q}[x]$ 的子环, 并非 $\mathbb{Q}[x]$ 的理想. ■

2.6.2 无幺环的扩张定理

我们将在这一节证明如下重要结论.

定理 2.6.1 (**无幺环扩张定理**)　任何无幺环都可以扩张成一个幺环. 换言之, 无幺环可以嵌入到某个幺环中.

这个结论告诉我们, 其实没必要孤立研究一个无幺环, 而是可以把它作为一个幺环的子环来研究. 这就是为什么此前我们只讨论幺环及其子环 (比如理想) 的性质.

为了证明扩张定理, 我们做一些准备工作. 考虑集合

$$S = \mathbb{Z} \times R.$$

设 $(m, a), (n, b) \in S$. 我们定义 S 上的加法

$$(m, a) + (n, b) = (m + n, a + b),$$

以及乘法

$$(m,a)\cdot(n,b)=(mn,mb+na+ab).$$

显见该加法满足 (A0-A4), 其中零元是 $(0,0_R)$.

引理 2.6.1 S 在上述运算下构成幺环.

证明 我们只要证明 S 满足结合律和分配律, 并且有幺元即可. 设 $\alpha=(m,a)$, $\beta=(n,b)$, $\gamma=(q,c)$. 先验证结合律.

$$(\alpha\cdot\beta)\cdot\gamma=(mn,mb+na+ab)(q,c)=(mnq,mnc+qmb+qna+qab+mbc+nac+abc).$$

$$\alpha\cdot(\beta\cdot\gamma)\ =(m,a)(nq,nc+qb+bc)=(mnq,mnc+qmb+qna+qab+mbc+nac+abc).$$

再验证分配律

$$(\alpha+\beta)\cdot\gamma=(m+n,a+b)(q,c)=(mq+nq,mc+nc+qa+qb+ac+bc).$$

$$\begin{aligned}\alpha\cdot\gamma+\beta\cdot\gamma&=(mq,mc+qa+ac)+(nq,nc+qb+bc)\\&=(mq+nq,mc+nc+qa+qb+ac+bc).\end{aligned}$$

最后验证幺元存在性. 令 $1_S:=(1,0)$. 我们有

$$1_S\cdot(m,a)=(1,0)(m,a)=(m,a)=(m,a)(1,0)=(m,a)1_S.$$

至此, 我们完成了证明. ■

定理 2.6.1 **的证明**: 考虑 S 的子集

$$R'=\{(0,a)\in S\mid a\in R\}.$$

因为

$$(0,a)-(0,b)=(0,a-b),\quad (0,a)(0,b)=(0,ab),$$

所以 R' 是 S 的子环.

我们有如下环同态

$$\sigma:R\longrightarrow S,\quad a\to(0,a).$$

容易验证, 这是单同态, 并且诱导了同构 $R\cong R'$. 因此, R 可以视作 S 的子环. ■

本章习题

加 $*$ 号的习题表示有一定难度.

习题 2.1 设 $\mathbb{H}$ 是四元数体, $v\in\mathbb{H}$, $\bar v$ 是其共轭元, $\mathcal{N}(v)$ 是其范数, $Tr(v):=v+\bar v$ 称作 v 的迹 (Trace). 证明: 对任何 $u\in\mathbb{H}$, 有

(1) $\overline{v+u}=\bar v+\bar u$, $\overline{v\cdot u}=\bar u\cdot\bar v$ 及 $\bar{\bar v}=v$.

(2) $Tr(v+u)=Tr(v)+Tr(u)$ 及 $\mathcal{N}(v\cdot u)=\mathcal{N}(v)\cdot\mathcal{N}(u)$.

(3) $\mathcal{N}(v)=\mathcal{N}(\bar v)$, $\mathcal{N}(av)=a^2\mathcal{N}(v)$, 这里 $a\in\mathbb{R}$.

习题 2.2 设 $\mathbb{H}$ 是四元数体, $q,q'\in\mathbb{H}$ 是非零元, $\sigma_q,\sigma_{q'}$ 分别是它们诱导的内自同构. 证明: $\sigma_{qq'}=\sigma_q\sigma_{q'}$.

习题 2.3　给定下列四元数 α, β, 计算

$$\alpha+\beta, \quad \alpha-\bar{\beta}, \quad \alpha\cdot\beta, \quad \alpha\cdot\beta-\beta\cdot\alpha, \quad \alpha^2, \quad \beta^{-1}, \quad \beta\cdot\alpha\cdot\beta^{-1}.$$

(1) $\alpha=\mathbf{1}-2\mathbf{i}+3\mathbf{k}$, $\beta=2\mathbf{1}-\mathbf{i}+\mathbf{j}-2\mathbf{k}$.
(2) $\alpha=2\mathbf{1}+\mathbf{i}-3\mathbf{j}+\mathbf{k}$, $\beta=-3\mathbf{1}-2\mathbf{i}+\mathbf{j}+4\mathbf{k}$.
(3) $\alpha=-\mathbf{1}+2\mathbf{i}-3\mathbf{j}+4\mathbf{k}$, $\beta=\mathbf{1}+2\mathbf{i}+2\mathbf{j}+\mathbf{k}$.

习题 2.4 (*)　设 $\mathbb{H}$ 是四元数体, $u, v\in\mathbb{H}$.
(1) 证明: 存在元 $q\in\mathbb{H}$ 使得 $b=q\cdot a\cdot q^{-1}$ 的充分必要条件是 $Tr(a)=Tr(b)$ 且 $\mathcal{N}(a)=\mathcal{N}(b)$. (提示: 先归结到迹为零的情形, 再说明 q 的四个分量满足线性方程组.)
(2) 证明: 每个判别式小于零的实系数二次方程都有无限多个根.

习题 2.5　在四元数体 $\mathbb{H}$ 中, 试求方程 $x^2+2x+13=0$ 的至少 8 个根.

习题 2.6 (*)　设 $\mathbb{H}$ 是四元数体, $u, v, w, z\in\mathbb{H}$ 是非零的四元数, 满足

$$u\cdot v=-v\cdot u, \quad w\cdot z=-z\cdot w, \quad \mathcal{N}(u)=\mathcal{N}(v), \quad \mathcal{N}(w)=\mathcal{N}(z).$$

证明: 存在四元数 q, 使得 $q\cdot u\cdot q^{-1}=v$ 且 $q\cdot w\cdot q^{-1}=z$. (提示: 利用习题 2.4.)

习题 2.7 (*)　证明四元数体 $\mathbb{H}$ 的自同构仅有内自同构. (提示: 利用习题 2.6 和习题 1.17.)

习题 2.8　设 H 是除环, 证明:
(1) $a^{-1}\cdot b^{-1}=(b\cdot a)^{-1}$, $\forall a, b\in H$,
(2) $(a^{-1})^{-1}=a$, $-(-a)=a$, $\forall a\in H\setminus\{0\}$,
(3) $(-a)\cdot(-b)=a\cdot b$.

习题 2.9 (**华罗庚恒等式**)　设 H 是一个除环, $a, b\in H$ 是非零元, 且 $a\cdot b\neq 1$. 证明:

$$a-(a^{-1}+(b^{-1}-a)^{-1})^{-1}=a\cdot b\cdot a.$$

习题 2.10　设 H 是一个体, $a, b\in H$ 是非零元, 我们定义 a, b 的换位子 $[a, b]:=a\cdot b\cdot a^{-1}\cdot b^{-1}$. 证明:
(1) $[a, b]=1$ 当且仅当 $a\cdot b=b\cdot a$.
(2) $a\cdot[b, c]\cdot a^{-1}=[a, [b, c]]\cdot[c, b]^{-1}$.
(3) 如果 $[a, b]\neq 1$, 那么

$$a=(1-[(a-1)^{-1}, b^{-1}])\cdot([a^{-1}, b^{-1}]-[(a-1)^{-1}, b^{-1}])^{-1}.$$

习题 2.11　设 H 是一个除环, Σ 是换位子全体组成的集合. 证明:
(1) H 由 Σ 生成. (提示: 利用习题 2.10.)
(2) 如果 H 的中心 $C(H)$ 包含 Σ, 则 H 必是域.

习题 2.12　设 H 是除环, $a\in H$ 是非零元, 定义 $C(a)=\{q\in H|\, a\cdot q=q\cdot a\}$, 称之为 a 的中心化子. 证明:
(1) $C(a)$ 是 H 的子除环.
(2) $\bigcap\limits_{a\in H\setminus\{0\}} C(a)=C(H)$.

习题 2.13　设 H 是除环, $H^* := H \setminus \{0\}$, 考虑 H^* 上的关系

$$r \sim r' \overset{\text{def}}{\Longleftrightarrow} r' = q \cdot r \cdot q^{-1}, \quad \text{对某个 } q \in H^*.$$

(1) 证明: 这是一个等价关系.

(2) 假设

$$S_a = \{r |\, r = q \cdot a \cdot q^{-1}, \quad \text{对某个 } q \in H^*\}$$

是 $a \in H^*$ 在上述等价关系下对应的等价类. 考虑满射

$$f_a : H^* \longrightarrow S_a, \quad q \to q \cdot a \cdot q^{-1}.$$

证明: $f_a(q) = f_a(q')$ 当且仅当 $q^{-1} \cdot q' \in C(a)^*$ (见习题 2.12), 亦等价于 $q' \in qC(a)^*$, 这里

$$C(a)^* := C(a) \setminus \{0\}, \quad qC(a)^* := \{qx |\, x \in C(a)^*\}.$$

习题 2.14　假设除环 H 是有限集合.

(1*) 证明: 那么 $|H^*| = |S_a| \cdot |C(a)^*|$ (提示: 利用习题 2.13 (2) 的结论).

(2) 设中心 $C(H)$ 的元素个数为 $|C(H)| = q$, 证明: 存在正整数 $n, n_a > 0$, 使得

$$|H^*| = q^n - 1, \quad |C(a)^*| = q^{n_a} - 1.$$

(3) (**类数公式**) 设 H 是有限集合, $\{A_k\}_{k=1}^t$ 是所有不含中心元素的等价类 (两两不同), $|A_k| = q^{n_k} - 1$. 证明:

$$q^n - 1 = q - 1 + \sum_{k=1}^{t} \frac{q^n - 1}{q^{n_k} - 1}.$$

习题 2.15 (*)　考虑多项式

$$\phi_d(x) = \prod_{\substack{0 \le k \le d-1 \\ \gcd(k,\, d) = 1}} (x - \omega^k),$$

这里 ω 是本原的 k 次单位根, 即满足 $\omega^k = 1$ 且对任何小于 k 的正整数 k', 都有 $\omega^{k'} \neq 1$.

(1) 证明: $\phi_d(x)$ 是整系数多项式.

(2) 证明: 对任何大于 1 的正整数 q, 都有 $|\phi_d(q)| > q - 1$.

(3) 证明: $k|d$ 当且仅当 $(q^k - 1)|(q^d - 1)$.

(4) 证明: 当 $k|d$ 时, 我们有

$$\phi_d(q) \left| \frac{q^d - 1}{q^k - 1}. \right.$$

(5) 结合习题 2.14 与以上结论证明 Wedderburn 小定理.

第三章　群的基础知识

3.1　群的基本概念

设 G 是一个集合, G 上有一个代数运算"$\cdot$"

$$G \times G \longrightarrow G, \quad (a, b) \to a \cdot b.$$

为方便起见, 我们把这个运算称作"乘法".

定义 3.1.1　如果 G 的乘法满足公理 (M0)(M1)(M3)(M4), 我们就称 G 为群 (Group). 换言之, 群 G 上的乘法满足结合律, 有乘法幺元, 并且每个非零元都是乘法可逆的.

进一步, 如果群 G 还满足交换律, 即公理 (M2), 我们就称之为交换群或 Abel 群.

注 3.1.1　(1) 对于交换群, 出于使用习惯, 我们通常将乘法运算改称为"加法", 并记作 $+$. (2) 类似环中的记号, 我们也能定义乘法运算下的方幂 a^n, 这里 $a \in G$, $n \in \mathbb{Z}$. 对于交换群的加法, 则将方幂形式改写为倍数形式 na. ■

类似环的讨论, 我们也能定义子群的概念.

定义 3.1.2　设 G 是群, H 是 G 的非空子集, 如果 H 在 G 的乘法下封闭并且构成群, 则称之为 G 的子群 (Subgroup).

我们还能类似定义群同态的概念.

定义 3.1.3　设 $\sigma : G \to G'$ 是群 G, G' 之间的映射. 如果 σ 满足

$$\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b), \quad \forall a, b \in G,$$

则称之为群同态 (Group homomorphism).

一个有限群 G 的元素个数记作 $|G|$, 称为 G 的阶数.

3.2　群的例子

3.2.1　交换群

例 3.2.1　所有的环关于加法构成交换群. 比如

$$\mathbb{Z}, \quad \mathbb{Q}, \quad \mathbb{H}, \quad \mathbb{Z}_N, \quad N\mathbb{Z}, \quad R[x], \quad M_n(R), \cdots$$

此处不再一一例举. ■

例 3.2.2　剩余类环的直和

$$\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}$$

在加法下构成一个有限的交换群. ■

例 3.2.3　设 V 是 n 维向量空间, 则 V 是加法群. ■

例 3.2.4　设 $\omega = e^{\frac{2\pi\sqrt{-1}}{n}}$ 是 n 次单位根, 即满足 $\omega^n = 1$. 集合

$$U_n = \{1, \omega, \omega^2, \cdots, \omega^{n-1}\}$$

在通常乘法下构成交换群. ■

3.2.2 幺环的单位群

设 R 是幺环. R 中的乘法可逆元也叫做*单位*. R 中所有单位构成的集合记作 R^*. 容易验证, R^* 在 R 的乘法下构成群, 称作*单位群*.

例 3.2.5　除环 H 的单位群就是由所有非零元构成的集合. 比如

$$\mathbb{Q}^*, \quad \mathbb{R}^*, \quad \mathbb{Z}_p^*, \quad \mathbb{H}^*, \quad \mathbb{Q}(x)^*, \cdots$$

都是常见的乘法群. ■

例 3.2.6 (**既约剩余系**)　模 N 的剩余类环中的单位群

$$\mathbb{Z}_N^* = \{[m] \mid \gcd(m, N) = 1\}.$$

它也称作模 N 的既约剩余系. 比如

$$\mathbb{Z}_6^* = \{[1], [5]\}, \quad \mathbb{Z}_8^* = \{[1], [3], [5], [7]\}, \quad \mathbb{Z}_{12}^* = \{[1], [5], [7], [11]\}.$$

$\mathbb{Z}_N^*$ 的元素个数记作 $\varphi(N)$, 通常称为*欧拉函数*. 比如 $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(6) = 2$, $\varphi(8) = 4$, $\varphi(12) = 4$. ■

例 3.2.7　设 R 是交换幺环, $M_n(R)$ 是矩阵环. $M_n(R)$ 的单位群由全体可逆矩阵构成. 由命题 2.5.1, 我们可以将其写成

$$M_n(R)^* = \{A \in M_n(R) \mid \det A \text{ 是 } R \text{ 中的单位 }\}.$$

特别地, 我们取 $R = F$ 为数域, 那么 $M_n(F)$ 的单位群由所有的行列式非零的矩阵构成, 称为 n 阶*一般线性群*, 通常记作 $GL_n(F)$. ■

例 3.2.8 (**特殊线性群**)　设 F 是数域, $GL_n(F)$ 是一般线性群.

$$SL_n(F) = \{A \in GL_n(F) \mid \det A = 1\}$$

在矩阵乘法下构成一个群, 称作*特殊线性群*. 它显然是 $GL_n(F)$ 的子群. ■

3.2.3 图形的对称群

考虑平面上的一个图形 F. 设 G_F 为全体保持 F 不变的平面正交变换构成的集合. G_F 在复合运算下构成群, 称为图形 F 的对称群. G_F 的幺元就是恒等变换.

注 3.2.1　回顾: 平面正交变换是一系列旋转和镜面反射复合成的几何变换. 每个平面正交变换对应一个 2 阶正交矩阵

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \text{(旋转)} \qquad \text{或} \qquad \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} \text{(反射)}.$$

■

例 3.2.9 (正交群) 取 F 为平面上的单位圆盘, 则 G_F 就是全体正交变换构成的集合, 我们通常称之为 2 阶*正交群* (Orthogonal group), 也记作 $O(2)$. 实际上 $O(2)$ 的元素也可以看作 2 阶正交矩阵. 从这个角度看, 我们可以推广地定义 n 阶*正交群*

$$O(n) = \left\{P \in GL_n(\mathbb{R}) \mid PP^T = P^TP = I_n\right\}.$$

这是一个非交换群. ■

例 3.2.10 (特殊正交群) $O(n)$ 中有一个子群

$$SO(n) = \{P \in O(n) \mid \det P = 1\}.$$

我们称之为*特殊正交群* (Special orthogonal group). 当 $n = 2, 3$ 时, 它也称为旋转群 (Rotation group). ■

例 3.2.11 (二面体群) 设 F 是中心在原点 O 的正 n 边形. 设 $T \in G_F$ 是关于 F 的中心逆时针旋转 $\frac{2\pi}{n}$, S 是关于某对称轴的镜面反射. 我们要证明

$$G_F = \{T, T^2, \cdots, T^n, ST, ST^2, \cdots, ST^n\}$$

满足关系 $T^n = S^2 = I$ 及 $TST = S$, 此处 I 是恒等映射. 该群称作二面体群 (Dihedral group), 通常记为 D_n. D_n 是有限非交换群, 共有 $2n$ 个元素.

为方便起见, 我们不妨把顶点坐标设为

$$v_k = \left(\cos\frac{2\pi k}{n}, \sin\frac{2\pi k}{n}\right), \quad k = 1, 2, \cdots, n.$$

将 S 视作关于 x 轴的镜面反射. 这样,

$$T = \begin{pmatrix} \cos\frac{2\pi k}{n} & \sin\frac{2\pi k}{n} \\ -\sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix}, \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

由此可以直接验证 T, S 的各关系式. 注意到 $T^{-k} = T^{n-k}$, $S^{-1} = S$,

$$T^kS = T^kST^k \cdot T^{-k} = T^{k-1}ST^{k-1} \cdot T^{-k} = \cdots = TST \cdot T^{-k} = S \cdot T^{-k},$$

因此 D_n 中的元素都可以写成 T^k, ST^k 的形式 $(k = 1, 2, \cdots, n)$.

我们也可以从复数的角度去理解 T, S 及其关系式. 将顶点看成单位根$v_k = \omega^k$, 这里 $\omega = e^{\frac{2\pi\sqrt{-1}}{n}}$, $(k = 1, \cdots, n)$. 这样, T 相当于让诸 v_k 乘以 ω, S 相当于对 v_k 取共轭. 按照这一观点, 我们很容易验证 T, S 的关系式. ■

例 3.2.12 作为上例的具体计算, 我们考虑 D_4. 此时

$$D_4 = \left\{T, T^2, T^3, T^4, ST, ST^2, ST^3, ST^4\right\},$$

满足关系式 $T^4 = S^2 = I$, $TST = S$. T 表示绕 O 点旋转 90°,S 表示关于 x 轴翻转.

(1) T^2 即绕 O 点旋转 180°.

(2) T^3 即绕 O 点旋转 270°.

(3) $T^4 = I$ 即保持 F 不动 (相当于绕 O 点旋转 360°), $T^5 = T, T^6 = T^2, \cdots$

(4) $S^2 = I$ 即保持 F 不动 (关于 x 轴翻转两次).

(5) ST 是关于直线 $x = -y$ 作翻转.

(6) ST^2 是关于 y 轴作翻转.

(7) ST^3 是关于直线 $x = y$ 轴作翻转. ■

3.2.4 置换群

设 M 非空集合, 我们用 $S(M)$ 表示全体从 M 到 M 的可逆变换构成的集合. 容易验证, $S(M)$ 在复合运算下构成群, 其幺元就是恒等变换. 我们称之为 M 的全变换群.

今取

$$M = \{1, 2, \cdots, n\}.$$

M 上的可逆变换称为 n 元置换, $S(M)$ 称为 n 元置换群 (Permutation group) 或者 n 元对称群, 通常记为 S_n. 它的幺元通常记作 (1). 当 $n > 2$ 时, S_n 是非交换群.

设 $\sigma \in S_n$. 为书写方便, 我们通常记

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix},$$

其中 $a_i = \sigma(i), i = 1, 2, \cdots, n$.
由于 σ 是双射 (即一一对应), 所以 $a_1, \cdots, a_n$ 实际上是 $1, 2, \cdots, n$ 的排列, 故 S_n 共有 $n!$ 个元素.

例 3.2.13 以 $n = 4$ 为例, 取

$$\sigma = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 2\ 4\ 1\ 3 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 1\ 2\ 4 \end{pmatrix}.$$

由定义

$$\sigma\tau(i) = \sigma(\tau(i)), i = 1, 2, 3, 4,$$

于是

$$\sigma\tau = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 2\ 4\ 1\ 3 \end{pmatrix} \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 1\ 2\ 4 \end{pmatrix} = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 2\ 4\ 3 \end{pmatrix}.$$

此外, 我们有

$$\sigma^{-1} = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 1\ 4\ 2 \end{pmatrix} \qquad \tau^{-1} = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 2\ 3\ 1\ 4 \end{pmatrix}.$$ ■

定义 3.2.1 设 $\sigma \in S_n$. 如果 σ 将 $1, 2 \cdots, n$ 中的 m 个数 $a_1, \cdots, a_m$ 轮换, 即

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_3, \quad \cdots \quad \sigma(a_{m-1}) = a_m, \quad \sigma(a_m) = a_1,$$

且保持其余数不动, 则称 σ 为一个轮换 (Cycle), 简记作 $\sigma = (a_1 a_2 \cdots a_m)$. 当 $m = 2$ 时, 它也称作对换 (Transposition). 两个轮换 $\alpha = (\alpha_1 \cdots \alpha_m), \beta = (\beta_1 \cdots \beta_l)$ 称为不相交 (Disjoint), 如果 $\alpha_i \neq \beta_j, \forall i, j$.

注 3.2.2　很明显,

$$(\alpha_1\cdots\alpha_m)=(\alpha_2\cdots\alpha_m a_1)=(\alpha_3\cdots\alpha_m a_1a_2)=(\alpha_m a_1\cdots a_{m-1}).$$

此外, 一阶轮换在 S_n 都相当于幺元 (1). ■

例 3.2.14　以 $n=4$ 为例,

$$\sigma=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}=(1243),\qquad \tau=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}=(132),$$

以及

$$\sigma\tau=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=(34).\qquad \tau\sigma=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}=(24)$$ ■

注 3.2.3　对不相交的轮换 α,β, 我们有 $\alpha\beta=\beta\alpha$. ■

我们已知如下经典结论.

命题 3.2.1　*S_n 中置换必可唯一表示为一些不相交的轮换乘积 (不考虑相乘的顺序).*

例 3.2.15　以 $n=6$ 为例, 取

$$\sigma=\begin{pmatrix}1&2&3&4&5&6\\3&1&2&5&4&6\end{pmatrix},$$

则 $\sigma=(1\,3\,2)(4\,5)$ (通常将 (6) 省略),

$$\tau=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&3&2&1\end{pmatrix}=(1\,6)(2\,5)(3\,4).$$ ■

例 3.2.16　设 $\sigma,\tau\in S_n$. 我们希望求 $\tau\sigma\tau^{-1}$. 由命题 3.2.1, 不妨考虑

$$\sigma=(i_1i_2\cdots i_r)$$

是轮换的情形. 我们要证明

$$\tau\sigma\tau^{-1}=(\tau(i_1)\tau(i_2)\cdots\tau(i_r)).\tag{3-1}$$

任取 $j\in\{1,2,\cdots,n\}$. 分两种情形讨论.

情形(A): 假设 $j=\tau(i_k)$, 对某个下标 k 成立. 此时有

$$\tau\sigma\tau^{-1}(j)=\tau\sigma(i_k)=\tau(i_{k+1}).$$

情形(B): 假设 $j\neq\tau(i_k)$, $\forall k$. 因此 $\tau^{-1}(j)\neq i_k$, $\forall k$. 这就推出 $\sigma(\tau^{-1}(j))=\tau^{-1}(j)$. 这样, 我们有

$$\tau\sigma\tau^{-1}(j)=\tau\sigma(\tau^{-1}(j))=\tau(\tau^{-1}(j))=j.$$

这就证明了 (3-1). ■

例 3.2.17　设 $\sigma=(159),\rho=(264)\in S_9$, 求 $\tau\in S_9$, 使得 $\tau\sigma\tau^{-1}=\rho$.

由例 3.2.16, τ 满足 $\tau(1)=2$, $\tau(5)=6$, $\tau(9)=4$. 因此不妨取 $\tau=(1294)(56)$. 当然, τ 还有其他不同的取法, 比如取 $\tau=(1256738)(49)$. ■

我们还有如下经典结论.

命题 3.2.2　任何 $\sigma \in S_n$ 总能分解一些对换的乘积, 并且对换个数的奇偶性不依赖于分解. 特别地, 若 σ 分解成偶 (奇) 数个互不相交的对换, 则称其为偶 (奇) 置换.

例 3.2.18　$\sigma = (a_1 a_2 \cdots a_r)$ 可以分解成如下对换的乘积

$$\sigma = (a_1 a_2)(a_2 a_3) \cdots (a_{r-1} a_r).$$

对任意 $\tau \in S_n$, 由命题 3.2.1, τ 可以分解成不相交的轮换乘积. 再由上述讨论, 这些轮换又能进一步分解为对换乘积. 比如

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 6 & 2 & 5 & 4 & 1 \end{pmatrix} = (17)(2364).$$

可以有如下分解

$$\tau = (17)(23)(36)(64).$$

一般说来, 对换的分解表示不是唯一的, 比如

$$\tau = (17)(36)(25)(64)(45)(25).$$

请读者自己验证. ■

例 3.2.19　假设 $\sigma \in S_n$ 能分解成 k 个不相交轮换的乘积 (包括一阶轮换), 则 σ 的奇偶性与 $n-k$ 的奇偶性一致. 我们只需要验证 σ 是轮换的情形, 此时由例 3.2.18 的讨论.

仍以例 3.2.18 中的 τ 为例. $\tau = (17)(2364)(5)$ 是偶置换. 注意 $n = 7$, $k = 3$, 所以 $n - k = 4$ 是偶数. ■

推论 3.2.1　所有偶置换组成的集合在 S_n 的运算下构成其子群, 称作 n 阶交错群 (Alternating group).

例 3.2.20　S_3 的交错群 $A_3 = \{(1), (123), (132)\}$. ■

例 3.2.21 (**鲁菲尼定理**)　设 $\sigma \in S_n$, 我们将满足性质 $\sigma^d = (1)$ 的最小正整数 d 称作 σ 的阶, 记作 $\mathrm{ord}\sigma$.

首先来求 $\sigma = (a_1 a_2 \cdots a_r)$ 的阶. 此时容易验证 $\mathrm{ord}\sigma = r$.

其次考虑一般情形. 设 σ 分解成互不相交的轮换乘积 $\sigma = \alpha_1 \cdots \alpha_k$. 于是

$$\mathrm{ord}\sigma = \mathrm{l.c.m.}(\mathrm{ord}\alpha_1, \cdots, \mathrm{ord}\alpha_k),$$

这里 l.c.m. 表示最小公倍数.

比如$\sigma = (17)(2364)$ 的阶 $\mathrm{ord}\sigma = \mathrm{l.c.m.}(2, 4) = 4$. ■

例 3.2.22　证明: 如果 $\sigma \in S_n$ 的阶是奇数, 则 σ 必是偶置换.

设 $\sigma = \alpha_1 \cdots \alpha_k$ 是互不相交的轮换乘积. 由例 3.2.21 的讨论以及 $\mathrm{ord}\sigma$ 为奇数, 立知诸 $\mathrm{ord}\alpha_i$ 皆奇数. 因此由例 3.2.19 知, 每个 α_i 都是偶置换, 从而 σ 是偶置换. ■

例 3.2.23　设 $\sigma = (1357246) \in S_7$, 求 $\tau \in S_7$ 满足 $\tau^2 = \sigma$.

注意到 $\sigma^7 = (1)$, 因此 $\sigma^8 = \sigma$. 这样, 我们可以取 $\tau = \sigma^4 = (1234567)$. ■

3.3 群同态的例子

设 $\sigma : G \to G'$ 是群同态. 我们可以类似定义如下诸概念.

定义 3.3.1 *若 σ 为单射 (相应地, 满射), 则称 σ 为单同态 (相应地, 满同态). 若存在群同态 $\tau : G' \to G$, 使得*

$$\tau\sigma = \mathrm{Id}_G, \quad \sigma\tau = \mathrm{Id}_{G'},$$

则称 σ 为群同构, 通常记作 $G \overset{\sigma}{\cong} G'$. 此外, 我们记逆映射 $\tau = \sigma^{-1}$.

命题 3.3.1 *群同态 $\sigma : G \to G'$ 是同构当且仅当 σ 既单又满.*

证明 ($\Longrightarrow$) 显然.

($\Longleftarrow$) 设 $\tau : G' \to G$ 是 σ 的逆映射. 对任何 $u, v \in G'$, 设 $a = \tau(u)$, $b = \tau(v)$. 由定义有 $u = \sigma(a)$, $v = \sigma(b)$. 我们有

$$\tau(uv) = \tau(\sigma(a)\sigma(b)) = \tau(\sigma(ab)) = ab = \tau(u)\tau(v).$$

这表明 τ 是群同态. ■

例 3.3.1 (**平凡同态**) 设 G, G' 是群, $e' \in G'$ 是其幺元.

$$\sigma : G \longrightarrow G', \quad a \to e'$$

称为平凡同态. ■

例 3.3.2 任何环同态都可以作为加法群的同态. 比如

$$(\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_N, +), \quad n \to [n].$$ ■

例 3.3.3 设 U_n 是 n 次单位根构成的乘法群 (见例 3.2.4), 我们有同构映射

$$\sigma : (U_n, \cdot) \longrightarrow (\mathbb{Z}_n, +), \quad \omega^k \to [k].$$

尽管从集合上说, 两个群的元素和运算都不相同, 但是它们却有相同的代数结构. 因此从代数角度看, 我们没有必要区别对待. ■

例 3.3.4 (**符号映射**) $\mathrm{sgn} : S_n \longrightarrow U_2$ 定义为

$$\mathrm{sgn}(\sigma) = \begin{cases} [0] & \sigma\text{为偶置换} \\ [1] & \sigma\text{为奇置换.} \end{cases}$$

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma) \cdot \mathrm{sgn}(\tau) = \begin{cases} [0] & \sigma, \tau\text{同奇同偶} \\ [1] & \sigma, \tau\text{一奇一偶.} \end{cases}$$

$\mathrm{sgn}((1)) = [0]$, $\mathrm{sgn}((12)) = [1]$. 因此 sgn 是满同态. ■

例 3.3.5 (**迹映射**) 设 $(M_n(R), +)$ 是交换幺环 R 上的 n 阶矩阵加法群, 我们定义迹映射

$$\mathrm{tr} : M_n(R) \longrightarrow R, \quad \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix} \to \sum_{k=1}^{n} a_{kk}.$$

由高等代数的结论, 我们有 $\mathrm{tr}(I_n) = n$,

$$\mathrm{tr}(A + B) = \mathrm{tr}(A) + \mathrm{tr}(B).$$

因此 tr 是群同态. 它是满同态, 但不是单同态, 比如 $n = 2$ 时,

$$\mathrm{tr}\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \mathrm{tr}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 0.$$ ■

例 3.3.6 (行列式映射) 设 $GL_n(F)$ 是域 F 上的 n 阶一般线性群. 行列式映射

$$\det : GL_n(F) \longrightarrow F^*, \quad A \to \det A.$$

由命题 2.5.1 可知 det 是群的满同态. ■

例 3.3.7 (指数映射) 考虑正实数集在通常乘法下构成的群 $(\mathbb{R}^+, \cdot)$. 我们有指数映射

$$\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \cdot), \quad x \to e^x.$$

显然有

$$\exp(x + y) = e^{x+y} = \exp(x) \cdot \exp(y).$$

因此 exp 是同态. 进一步可验证, 它是同构 $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$. ■

例 3.3.8 设 G 是群, $a \in G$ 是给定元.

$$\Phi : \mathbb{Z} \longrightarrow G, \quad n \to a^n.$$

我们有

$$\Phi(n + m) = a^{n+m} = \Phi(n) \cdot \Phi(m).$$

因此它是群同态.

比如取 $G = 2\mathbb{Z}$, $a = 2$, 则有同态

$$\Phi : \mathbb{Z} \xrightarrow{\sim} 2\mathbb{Z}, \quad n \to 2n.$$

容易验证, 它是同构. 另一方面, $2\mathbb{Z}$ 是 $\mathbb{Z}$ 的子群. 这表明, 一个群有可能与其子群同构. ■

例 3.3.9 (莫比乌斯变换) 设 G 是扩充复平面 $\overline{\mathbb{C}}$ 上的全体莫比乌斯变换构成的集合. 任何 $\sigma \in G$ 可以写成

$$\sigma(z) = \frac{az + b}{cz + d}, \quad ad - bc = 1, \quad z \in \overline{\mathbb{C}}.$$

G 在复合映射下构成群. 我们可以验证如下映射是群的满同态

$$\Phi : SL_2(\mathbb{C}) \longrightarrow G, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \sigma(z) = \frac{az + b}{cz + d}.$$ ■

例 3.3.10 (自同构群) 设 G 是群. 我们把 G 到自身的同构称作群 G 的自同构. 全体自同构构成的集合记作 $\mathrm{Aut}(G)$. 容易验证 $\mathrm{Aut}(G)$ 在复合运算下构成群, 其幺元是恒同映射. 这个群称作 G 的*自同构群* (Automorphism group). ■

3.4 群的基本性质

在群的定义中, 公理 (M3)(M4) 可以被弱化, 这就是下面的结论.

命题 3.4.1 *设 G 是非空集合, G 上有满足结合律的乘法运算. 如果 G 在该运算下还满足如下条件:*

(M'3) *存在左幺元 e, 使得 $ea = a$, $\forall a \in G$,*

(M'4) *对任何元 $a \in G$, 都存在左逆元 $b \in G$, 即满足 $ba = e$,*

则 G 必是群. 特别地, 幺元 e 是唯一的, a 的逆元也是唯一的.

证明 任取 $a \in G$, 设 $b \in G$ 是左逆元. 由条件 (M'4), 存在 $c \in G$, 满足 $cb = e$. 于是有

$$ab = (ea)b = ((cb)a)b = (c(ba))b = (ce)b = c(eb) = cb = e.$$

这表明 b 也是 a 的右逆.

另一方面,

$$ae = a(ba) = (ab)a = ea = a.$$

因此 e 也是右幺元.

现在, 我们来验证幺元的唯一性. 设 e' 是另一幺元, 则由上讨论可知

$$e' = ee' = e.$$

最后再验证逆元的唯一性. 设 c, b 都是 a 的逆元, 则

$$c = ce = c(ab) = (ca)b = eb = b.$$

至此, 我们完成了证明. ■

注 3.4.1 按照习惯, 我们仍将 a 的逆元记为 a^{-1}. 我们有显然的关系式

$$(a^{-1})^{-1} = a, \quad (ab)^{-1} = b^{-1}a^{-1}.$$

■

推论 3.4.1 *对任意 $a, b \in G$, 方程 $ax = b$ 在 G 上有唯一解 $x = a^{-1}b$.*

命题 3.4.2 *设 G 是群, H 是 G 的子群, 则 H 的幺元就是 G 的幺元, H 中任一元的逆元就是它在 G 中的逆元.*

证明 设 $e \in G$ 是 G 的幺元, $e' \in H$ 是 H 的幺元. 由定义知, $e'e' = e'$. 设 $e'^{-1} \in G$ 是 e' 在 G 的逆元, 于是

$$e = e'e'^{-1} = (e'e')e'^{-1} = e'(e'e'^{-1}) = e'e = e'.$$

任取 $h \in H$. 设 $h' \in H$ 是 h 在 H 中的逆元, h^{-1} 是 h 在 G 中的逆元. 于是有

$$h^{-1} = eh^{-1} = (h'h)h^{-1} = h'(hh^{-1}) = h'e = h'.$$

这就完成了证明. ■

注 3.4.2　在环中, 幺环与其子环未必有相同的幺元. 比如例 2.3.8 中的幺环

$$R=\left\{\left(\begin{array}{cc} a & \\ & b \end{array}\right)\in M_2(F)\,\middle|\, a,b\in F\right\}$$

以及它的子环

$$L=\left\{\left(\begin{array}{cc} a & \\ & 0 \end{array}\right)\in M_2(F)\,\middle|\, a\in F\right\}.$$

它们的幺元分别是

$$1_R=\left(\begin{array}{cc} 1 & \\ & 1 \end{array}\right),\quad 1_L=\left(\begin{array}{cc} 1 & \\ & 0 \end{array}\right).$$

出现这种现象的关键原因就是公理 (M4), 即乘法逆元的存在性. ■

命题 3.4.3　*设 $\sigma: G\longrightarrow G'$ 群同态, $e\in G$ (相应地, $e'\in G'$) 是 G (相应地, G') 的幺元, 则*
(1) *σ 将幺元映为幺元, 即 $\sigma(e)=e'$.*
(2) *σ 将逆元映为像的逆元, 即 $\sigma(a^{-1})=(\sigma(a))^{-1}$.*

证明　(1) $\sigma(e)\cdot\sigma(e)=\sigma(e\cdot e)=\sigma(e)$, 因此 $\sigma(e)=e'$.
(2) $\sigma(a)\cdot\sigma(a^{-1})=\sigma(a\cdot a^{-1})=\sigma(e)=e'$, 因此 $\sigma(a^{-1})=(\sigma(a))^{-1}$. ■

命题 3.4.4　*群的同构关系是等价关系.*

(1) (自反性) $G\cong G$,

(2) (对称性) $G\cong G'\Rightarrow G'\cong G$,

(3) (传递性) $G\cong G', G'\cong G''\Rightarrow G\cong G''$.

例 3.4.1　我们已有加法群同构 $\mathbb{Z}\cong n\mathbb{Z}$ 以及 $\mathbb{Z}\cong m\mathbb{Z}$, 因此由对称性及传递性得到同构 $n\mathbb{Z}\cong m\mathbb{Z}$. ■

3.5 群的构造

3.5.1 构造方法 (I): 子群

前面我们已经定义了子群的概念, 并且介绍了一些经典的例子, 比如交错群 A_n 是置换群 S_n 的子群; 特殊线性群 $SL_n(\mathbb{R})$ 是一般线性群 $GL_n(\mathbb{R})$ 的子群; 特殊正交群 $SO(n)$ 是正交群 $O(n)$ 的子群, 等等.

为方便书写, 我们习惯上通常将群 G 及其子群 H 的包含关系记作 $H<G$.

命题 3.5.1 (**子群的判定条件**)　*$H<G$ 当且仅当 $a^{-1}b\in H$, 对任何 $a,b\in H$.*

证明　($\Longrightarrow$) 显然.
($\Longleftarrow$) 结合律显然. 任取 $a\in H$, 由条件得 $e=a^{-1}\cdot a\in H$, 这表明幺元存在. 进一步,

$$a^{-1}=a^{-1}\cdot e\in H.$$

这就证明了逆元的存在性.

最后验证运算封闭性. 设 $a,b\in H$, 由于 $a^{-1}\in H$, 故 $ab=(a^{-1})^{-1}b\in H$. 这样, 我们就证明了 $H<G$. ■

注 3.5.1 类似地, $H<G$ 也当且仅当 $ab^{-1}\in H$, $\forall a,b\in H$. ■

例 3.5.1 设 R 是环, S 是子环, 它们作为加法群显然有 $(S,+)<(R,+)$. 特别地, 理想作为加法群是环的加法子群. ■

例 3.5.2 G 有两个平凡子群 $\{e\}$ 和 G. ■

例 3.5.3 由前讨论, 我们已知 $SL_n(F)<GL_n(F)$, $SO(n)<O(n)$. ■

例 3.5.4 (**共轭子群**) 设 $H<G$, 给定元 $g\in G$, 我们可以定义 H 的*共轭子群* (Congruence subgroup)

$$gHg^{-1}:=\{ghg^{-1}\mid h\in H\}.$$

我们利用子群判定法来检验它. 对任取的 $a=gh_1g^{-1}$ 及 $b=gh_2g^{-1}\in H$,

$$a^{-1}b=(gh_1g^{-1})^{-1}\cdot(gh_2g^{-1})=g(h_1^{-1}h_2)g^{-1}\in gHg^{-1}.$$

因此它确实是 G 的子群.

(1) 一般说来, $H\neq gHg^{-1}$. 比如 $H=\{(1),(12)\}<S_n$, 对任意 $\tau\in S_n$, 利用例 3.2.16 的讨论可得

$$\tau H\tau^{-1}=\{(1),(\tau(1)\tau(2))\}.$$

(2) 我们可以定义群同构

$$\sigma_g:H\longrightarrow gHg^{-1},\quad h\to ghg^{-1}.$$

特别地, 如果 H 是有限子群, 那么其共轭子群也是有限群, 并且它们的元素个数相同.

(3) 如果 $gHg^{-1}=H$, 那么 $g^{-1}Hg=H$. 这是因为

$$g^{-1}Hg=g^{-1}(gHg^{-1})g=(g^{-1}g)H(g^{-1}g)^{-1}=H.$$

(4) 对任意 $h\in H$, $hHh^{-1}\subseteq H$. 特别地, $h^{-1}Hh\subseteq H$, 从而 $H\subseteq hHh^{-1}$, 这就推出 $hHh^{-1}=H$.

此外, 很明显, 交换群中的子群除了本身之外, 没有其他共轭子群. ■

例 3.5.5 (**正规子群**) 设 $H<G$, 满足

$$gHg^{-1}=H,\quad \forall g\in G,$$

我们就称 H 是 G 的*正规子群* (Normal subgroup), 记作 $H\lhd G$.

显然, 交换群的子群总是正规子群. 非交换的子群未必是正规的 (见例 3.5.4).

现在我们验证 $A_n\lhd S_n$. 对任意 $\tau\in S_n$, 由例 3.2.16 的讨论, $\tau A_n\tau^{-1}$ 中的元素都是偶置换, 因此 $\tau A_n\tau^{-1}\subseteq A_n$. 由于这两个子群的元素个数相等, 因此 $\tau A_n\tau^{-1}=A_n$.

我们来证明 $H\lhd G$ 当且仅当 $gHg^{-1}\subseteq H$ 对任何 $g\in G$ 成立.

($\Longrightarrow$) 是显然的.

($\Longleftarrow$) 因为 $g^{-1}Hg = (g^{-1})H(g^{-1})^{-1} \subseteq H$, 故 $H \subseteq gHg^{-1}$. 另一方面, $gHg^{-1} \subseteq H$. 因此 $gHg^{-1} = H$. ■

例 3.5.6 (**正规化子**, Normalizer)　对任何子群 $H < G$, 我们定义集合

$$N(H) = \{g \in G \mid gHg^{-1} = H\}.$$

先证明 $N(H) < G$. 任取 $g_1, g_2 \in N(H)$, 我们有

$$(g_1^{-1}g_2)H(g_1^{-1}g_2)^{-1} = g_1^{-1}(g_2Hg_2^{-1})g_1 = g_1^{-1}Hg_1 = H.$$

因此 $g_1^{-1}g_2 \in N(H)$. 由子群判别法, $N(H) < G$. 再由上例讨论, $H \lhd N(H)$. ■

推论 3.5.1　*任意多个子群的交仍是子群. 换言之, 设 $\{H_\alpha\}_{\alpha\in I}$ 是 G 的一族子群, 则 $\bigcap\limits_{\alpha\in I} H_\alpha$ 也是 G 的子群.*

设 S 是群 G 的非空子集, $\{H_\alpha\}_{\alpha\in I}$ 是所有包含 S 的子群. 由推论 3.5.1,

$$\langle S\rangle := \bigcap_{\alpha\in I} H_\alpha$$

仍是子群. 我们把它称为由 S 生成的子群, S 中的元称作 $\langle S\rangle$ 的生成元.

命题 3.5.2　*设 S, G 同上.*

(1) *$\langle S\rangle$ 是包含 S 的最小子群.*

(2) *令 $S^{-1} = \{a^{-1} | a \in S\}$, 则*

$$\langle S\rangle = \{x_1x_2\cdots x_m |\, x_i \in S \cup S^{-1}\}.$$

证明　(1) 设 $H < G$, 且 $S \subseteq H$, 则由定义知 $\langle S\rangle \subseteq H$. 另一方面, 显然有 $S \subseteq \langle S\rangle$. 因而 $\langle S\rangle$ 是包含 S 最小子群.

(2) 令

$$H = \{x_1x_2\cdots x_m |\, x_i \in S \cup S^{-1}\},$$

我们来验证 $H < G$. 设

$$\sigma = x_1x_2\cdots x_m, \quad \tau = y_1\cdots y_l \in H,$$

这里 $x_i, y_j \in S \cup S^{-1}$. 于是

$$\sigma^{-1}\tau = x_m^{-1}x_{m-1}^{-1}\cdots x_1^{-1}y_1y_2\cdots y_l \in H.$$

由子群判别法知 H 是子群.

由 $\langle S\rangle$ 定义，显然 $\langle S\rangle \subseteq H$. 另一方面, 对任意 $\sigma = x_1x_2\cdots x_m \in H$, 注意到 $x_i \in S \cup S^{-1} \subseteq \langle S\rangle$, 从而 $\sigma \in \langle S\rangle$, 这就推出 $H \subseteq \langle S\rangle$. 因此 $H = \langle S\rangle$. ■

例 3.5.7 (**循环子群**)　取 $S = \{a\}$, 由 a 生成的子群 $\langle a\rangle$ 称为*循环子群* (Cyclic subgroup). 由定义,

$$\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

环 R 中的主理想 $I=(a)$ 作为加法群显然是 $(R,+)$ 的加法子群. 比如整数加法群 $\mathbb{Z}=\langle 1\rangle$ 的有循环子群 $N\mathbb{Z}=\langle N\rangle$. 又比如, 模 N 的剩余类加法群 $\mathbb{Z}_N=\langle a\rangle$ 有循环子群 $\langle [d]\rangle$, 这里 $d\mid N$.

如果 $\langle a\rangle$ 是有限子群, 那么该子群中的元素个数称作 a 在 G 中的阶数, 记作 $\operatorname{ord} a$, 并称 a 是有限阶的. 如果 $\langle a\rangle$ 是无限子群, 则称 a 是无限阶的, 通常表示为 $\operatorname{ord} a=\infty$. ■

例 3.5.8　假设 G 是群, $a,b\in G$ 满足 $ab=ba$, 那么

$$\langle a,b\rangle=\{a^nb^m\mid n,m\in\mathbb{Z}\}.$$

请注意, 如果 $ab\neq ba$, 那么上述结论通常并不成立. 比如取 $G=S_3$, $\sigma=(12),\tau=(13)\in S_3$, 则 $\langle\sigma,\tau\rangle=S_3$, 其中 (23) 不能写为 $\sigma^n\tau^m$ 的形式 (为什么?). ■

例 3.5.9　证明: S_n 由如下集合

$$\Sigma=\{(12),(13),\cdots,(1n)\}$$

生成.

由于 S_n 中的元都能写成对换的乘积并且对换的逆元就是其本身, 所以我们只要证明 Σ 中的元素的乘积. 容易验证

$$(ij)=(1i)(1j)(1i).$$

这就得到了所需结论. ■

例 3.5.10 (**中心化子**, centralizer)　设 G 是群, $a\in G$. 我们可以构造子群

$$C(a)=\{g\in G\mid ga=ag\}.$$

它称为 a 的中心化子. 对 G 的任何非空子集 S, 同样可以定义 S 的中心化子

$$C(S)=\bigcap_{a\in S}C(a).$$

由推论 3.5.1, 它是一个子群.

特别地,

$$C(G)=\{g\in G\mid gx=xg,\ \forall x\in G\}$$

称作 G 的中心. 它是交换子群. 我们在除环的讨论中其实已经介绍过类似的概念. ■

例 3.5.11 (**换位子群**)　设 G 是群. 对任何 $a,b\in G$, 我们定义 $[a,b]=a^{-1}b^{-1}ab$. 它称作 a,b 的换位子 (Commutator). 由全体换位子生成的子群叫做换位子群 (Commutator subgroup), 记作 $[G,G]$. 比如 $[S_3,S_3]=A_3$ (请读者验证).

此外, 我们有

(1) $[a,b]^{-1}=b^{-1}a^{-1}ba=[b,a]$.

(2) 对任意 $g\in G$, 以及任意 $[a,b]\in[G,G]$, 有

$$g[a,b]g^{-1}=[gag^{-1},gbg^{-1}].$$

结合命题 3.5.2 以及上面讨论可知 $g[G,G]g^{-1}\subseteq[G,G]$, 故 $[G,G]$ 是正规子群. ■

例 3.5.12 (**内自同构群**)　设 G 是群, $\mathrm{Aut}(G)$ 是自同构群 (见例3.3.10). 我们考察其中一类特殊的自同构. 任取 $g \in G$, 定义映射

$$\sigma_g : G \longrightarrow G, \quad a \to gag^{-1}.$$

容易验证 $\sigma_g(ab) = \sigma_g(a)\sigma_g(b)$ 以及它是一一对应, 因而它是群同构. 我们把这类群同构称作 G 的*内自同构* (Inner automorphism). 全体内自同构构成的集合记作 $\mathrm{Inn}(G)$.

我们来验证 $\mathrm{Inn}(G)$ 是 $\mathrm{Aut}(G)$ 的子群. 任取 $g, g' \in G$, $\sigma_g, \sigma_{g'}$ 是相应的内自同构.

$$\sigma_g\sigma_{g'}^{-1}(x) = \sigma_g(g'^{-1}xg') = g(g'^{-1}xg')g^{-1} = (gg'^{-1})x(gg'^{-1})^{-1} = \sigma_{gg'^{-1}}, \quad \forall x \in G.$$

因此 $\sigma_g\sigma_{g'}^{-1} = \sigma_{gg'^{-1}} \in \mathrm{Inn}(G)$. 由子群判别法即得结论. 我们将 $\mathrm{Inn}(G)$ 称作*内自同构群* (Inner automorphism group). 它是 $\mathrm{Aut}(G)$ 的子群.

对任何 $\tau \in \mathrm{Aut}(G)$, 因为

$$\tau\sigma_g\tau^{-1}(x) = \tau\sigma_g(\tau^{-1}(x)) = \tau(g\tau^{-1}(x)g^{-1}) = \tau(g)x(\tau(g))^{-1} = \sigma_{\tau(g)}(x), \quad \forall x \in G,$$

故 $\tau\sigma_g\tau^{-1} = \sigma_{\tau(g)} \in \mathrm{Inn}(G)$. 这就推出 $\mathrm{Inn}G \lhd \mathrm{Aut}G$ 是正规子群. ■

我们也可以利用群同态来构造一些子群.

定义 3.5.1　*设 $\sigma : G \to G'$ 是群同态, e (相应的, e') 是 G (相应的, G') 的幺元.*

(1) *σ 的核* (Kernel) *是指如下子集合*

$$\mathrm{Ker}\,\sigma \stackrel{\triangle}{=} \{x \in G \mid \sigma(x) = e'\}.$$

(2) *σ 的像* (Image) *是指如下子集合*

$$\mathrm{Im}\sigma \stackrel{\triangle}{=} \{x' \in G' \mid \exists\, x \in G, \text{ 使得 } \sigma(x) = x'\}.$$

命题 3.5.3　*设 $\sigma : G \to G'$ 是群同态, 则*

(1) $\mathrm{Ker}\,\sigma \lhd G$,

(2) $\mathrm{Im}\sigma < G'$.

证明　(1) 先证 $\mathrm{Ker}\,\sigma < G$. 对任意 $x, y \in \mathrm{Ker}\,\sigma$,

$$\sigma(x^{-1}y) = \sigma(x)^{-1} \cdot \sigma(y) = e',$$

故 $x^{-1}y \in \mathrm{Ker}\,\sigma$, 因此 $\mathrm{Ker}\,\sigma < G$.

其次, 对任何 $a \in G$, 我们要证

$$a \cdot \mathrm{Ker}\,\sigma \cdot a^{-1} \subseteq \mathrm{Ker}\,\sigma.$$

对任何 $x \in \mathrm{Ker}\,\sigma$, 我们有

$$\sigma(axa^{-1}) = \sigma(a) \cdot \sigma(x) \cdot \sigma(a)^{-1} = \sigma(a) \cdot e' \cdot \sigma(a)^{-1} = \sigma(a) \cdot \sigma(a)^{-1} = e',$$

故 $axa^{-1} \in \mathrm{Ker}\,\sigma$. 因此 $a \cdot \mathrm{Ker}\,\sigma \cdot a^{-1} \subseteq \mathrm{Ker}\,\sigma$, $\forall a \in G$. 因这就推出 $\mathrm{Ker}\,\sigma \lhd G$.

(2) 类似可证. ■

例 3.5.13　我们举几个常见的例子.

(1)

$$\sigma : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_N, +), \quad n \to [n]$$

的核 $\mathrm{Ker}\,\sigma = N\mathbb{Z}$.

(2)

$$\tau : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad k \to kN$$

的像 $\mathrm{Im}\tau = N\mathbb{Z}$.

(3) 设 $a \in G$ 是给定元.

$$\rho : \mathbb{Z} \longrightarrow G, \quad n \to a^n.$$

它的核为 $N\mathbb{Z}$, 这里 $N = \mathrm{ord}\, a$; 它的像为 $\langle a \rangle < G$. 一般说来, $\mathrm{Im}\sigma$ 不是 G 的正规子群. ■

类似环同态的讨论, 我们有如下结论.

命题 3.5.4　*设 $\sigma : G \to G'$ 是群同态, 则*

(1) $\mathrm{Ker}\,\sigma = \{e\}$ *当且仅当* σ *单同态.*

(2) σ *是平凡同态 当且仅当* $\mathrm{Ker}\,\sigma = G$, *也当且仅当* $\mathrm{Im}\sigma = \{e'\}$.

(3) σ *是满同态当且仅当* $\mathrm{Im}\sigma = G'$.

证明　(1) ($\Leftarrow$) 显然. ($\Rightarrow$) 设 $\sigma(x) = \sigma(y)$, 则 $\sigma(xy^{-1}) = e'$, 故 $xy^{-1} = e$, 即 $x = y$.
(2) (3) 显然. ■

推论 3.5.2　*群同态 $\sigma : G \to G'$ 是同构的充分必要条件为* $\mathrm{Ker}\,\sigma = \{e\}$ *及* $\mathrm{Im}\sigma = G'$.

3.6 构造方法 (II): 循环群

前面已经触及了循环子群的概念. 这里我们在正式定义循环群的概念.

定义 3.6.1　*设 G 是群. 如果存在一个元素 $a \in G$ 使得 $G = \langle a \rangle$, 我们就称其为循环群.*

由定义知, 循环群

$$\langle a \rangle = \{a^n | n \in \mathbb{Z}\}.$$

它是结构最简单的一类群.

例 3.6.1　(1) $G = \{e\}$ 是平凡的循环群.
(2) $(\mathbb{Z}, +) = \langle 1 \rangle$ 是循环群.
(3) $(\mathbb{Z}_N, +) = \langle [1] \rangle$ 是循环群.
(4) n 次单位根群 $(U_n, \cdot) = \langle \omega \rangle$ 是循环群. ■

例 3.6.2 (**原根**)　设 $\mathbb{F}_p$ 是模素数 p 的剩余类域, $\mathbb{F}_p^* = \mathbb{F} - \{[0]\}$ 是乘法群. 根据经典数论的结果, $\mathbb{F}_p^*$ 是循环群. *它的生成元叫做原根.* ■

引理 3.6.1　设 $G=\langle a\rangle$ 是循环群.

(1) 若 G 是 N 阶有限群, 则 $a^n=a^m$ 当且仅当 $N\mid n-m$. 特别地, $a^n=e$ 当且仅当 $N\mid n$.

(2) 若 G 是无限循环群, 则对任何 $n\neq m$, 都有 $a^n\neq a^m$.

证明　我们分两种情形讨论:
(A) 存在正整数 d 满足 $a^d=e$;
(B) 对任何正整数 d, $a^d\neq e$.

先考虑情形 (A). 设 $d>0$ 是最小的正整数, 满足 $a^d=e$. 对任何 $n\in\mathbb{Z}$, 考虑带余除法, $n=qd+r$, $0\leq r<d$. 我们有

$$a^r=a^{n-qd}=a^n\cdot(a^d)^{-q}=a^n.$$

因此每个元都能写成 a^r $(0\leq r<d)$. 这就推出

$$G\subseteq\{e,a,\cdots,a^{d-1}\}$$

是有限群. 又因为 $\{e,a,\cdots,a^{d-1}\}\subseteq G$, 所以 $G=\{e,a,\cdots,a^{d-1}\}$.

由 d 的最小性, $a^n=e$ 当且仅当上述 $r=0$, 即 $d\mid n$. 进一步,

$$a^n=a^m\Longleftrightarrow e=a^{n-m}\Longleftrightarrow d\mid n-m.$$

特别地, 这表明 $\{e,a,\cdots,a^{d-1}\}$ 中的元素两两不同. 因为 $|G|=N$, 故 $N=d$.

再考虑情形(B). 如果 $a^n=a^m$ $(n>m)$, 则 $e=a^{n-m}$, 与假设矛盾! 故 $a^n\neq a^m$. 这推出 G 是无限循环群.

综上可知, (A) 对应有限循环群的情形, (B) 对应无限循环群的情形. ■

定理 3.6.1　设 $G=\langle a\rangle$ 是循环群, 则

(1) G 要么同构于 $\mathbb{Z}$, 要么同构于 $\mathbb{Z}_N$.

(2) G 的子群必是形如 $\langle a^d\rangle$ 的循环子群. 特别地, 如果 $|G|=N$, 那么我们可以取 $d\mid N$.

证明　(1) 先考虑 $G=\langle a\rangle$ 是无限循环群的情形. 我们诱导群同态

$$\sigma:\mathbb{Z}\longrightarrow G,\quad n\to a^n.$$

由 a 的选取, σ 显然是满同态. 现证 σ 是单射. 假设 $\sigma(n)=\sigma(m)$, 即 $a^n=a^m$. 由引理 3.6.1, $n=m$. 因此它是单射.

其次考虑 $G=\langle a\rangle$ 是有限循环群的情形, 设 $|G|=N$. 定义映射

$$\sigma:\mathbb{Z}_N\longrightarrow G,\quad [n]\to a^n.$$

先说明合理性. 若 $[n]=[n']$, 则 $N\mid n-n'$, 从而

$$a^n=a^{n'}a^{n-n'}=a^{n'}(a^N)^{\frac{n-n'}{N}}=a^{n'}.$$

再验证它是同态.

$$\sigma([n]+[m])=\sigma([n+m])=a^{n+m}=a^na^m=\sigma(n)\sigma(m).$$

由定义知 σ 是满的.

最后证 σ 是单射. 设 $\sigma([n]) = \sigma([m])$, 即 $a^n = a^m$, 因而 $a^{n-m} = e$. 因此由引理 3.6.1, $N \mid n-m$, 即 $[n] = [m]$.

(2) 设 $H < G$. 取 d 是满足 $a^d \in H$ 的最小正整数. 对任意 $a^m \in H$, 考虑带余数除法 $m = dq + r$, 于是

$$a^r = a^{m-dq} = a^m \cdot (a^d)^{-q} \in H.$$

由 d 的最小性推知 $r = 0$, 即 $d \mid m$. 反之, 对任何 d 的倍数 dk, 都有 $a^{dk} = (a^d)^k \in H$. 因此 $H = \langle a^d \rangle$.

如果 G 是 N 阶有限群, 则由引理 3.6.1, $a^N = e$ 蕴含着 $d \mid N$. ■

例 3.6.3 整数加法群的子群都是形如 $N\mathbb{Z}$ $(N \geq 0)$ 的循环子群. ■

例 3.6.4 $\mathbb{Z}_N$ 的任何子群都是形如 $\langle [d] \rangle$ 的循环子群 (可以取 $d \mid N$) . ■

推论 3.6.1 *设 $G = \langle a \rangle$ 是 N 阶循环群, 则*

$$\operatorname{ord} a^n = \frac{N}{\gcd(N,n)},$$

即 $\langle a^n \rangle = \langle a^{\gcd(n,N)} \rangle$ 是 $\frac{N}{\gcd(N,n)}$ 阶循环子群. 特别地, 循环子群的阶数必整除 G 的阶数.

上述结论的最后一部分实际上是拉格朗日定理的特殊情形 (见定理 3.6.2).

例 3.6.5 设 $G = \langle a \rangle$ 是 N 阶循环群. 我们有

(1) $\langle a^n, a^m \rangle = \langle a^{\gcd(n,m)} \rangle$.

(2) 若 $n \mid N$, $m \mid N$, 则 $\langle a^n \rangle \cap \langle a^m \rangle = \langle a^{\operatorname{lcm}(n,m)} \rangle$. ■

3.6.1 构造方法 (III): 正规子群与商群

设 $\sigma : G \to G'$ 是群同态. 我们前面已证 $\operatorname{Ker}\sigma$ 是 G 的正规子群. 反过来, 是否每个子群 $H < G$ 都可以看作某个群同态的核呢? 很显然, H 首先必须是 G 的正规子群. 接下来, 我们希望能仿照商环的做法, 来类似地定义商群的概念, 以及 G 到商群的同态, 使得其核恰好是 H.

设 G 群, $H < G$. 我们首先给出 G 上的关系

$$a \sim_H b \Longleftrightarrow a^{-1}b \in H.$$

容易验证

引理 3.6.2 *$\sim_H$ 是 G 上的等价关系.*

我们可以定义 $\sim_H$ 的等价类

$$aH = \{b \in G |\ b \sim_H a\}.$$

它称为 H 的*左陪集* (Left coset). 由定义,

$$aH = \{ah \mid h \in H\}.$$

类似地, 我们也可以定义另一等价关系

$$a \sim'_H b \Longleftrightarrow ba^{-1} \in H,$$

以及右陪集 (Right coset)

$$Ha = \{b \in G |\ b \sim'_H a\} = \{ha \mid h \in H\}.$$

注 3.6.1　这里罗列一些陪集的简单性质.

(1) $a \in aH$, $a \in Ha$.

(2) 由上述等价关系的定义可知, $aH = bH$ 当且仅当 $a^{-1}b \in H$; $Ha = Hb$ 当且仅当 $ba^{-1} \in H$. 特别地, $H = aH$ 当且仅当 $H = Ha$, 亦当且仅当 $a \in H$.

(3) 我们有集合上的一一对应

$$\phi : H \longrightarrow aH, \quad h \to ah.$$

假设 $\phi(h_1) = \phi(h_2)$, 则 $ah_1 = ah_2$, 故 $h_1 = h_2$, 这表明 ϕ 是单的. 另一方面, 对任何 $x = ah \in aH$, 则 $\phi(h) = x$, 因此 ϕ 是满的. 同理, 也有一一对应 $\psi : H \to Ha$.

特别地, 任何两个左 (右) 陪集间都存在一一对应.

(4) 如果 $|H| < \infty$, 则 $|H| = |Ha| = |aH|$.

(5) 一般而言, aH 不是 G 的子群, 且 $aH \neq Ha$.

(6) 由定义, 任何两个不同的左 (右) 陪集必不相交; G 可以表示成一些互不相交的左(右)陪集的并, 即 $G = \dot{\bigcup\limits_{a \in G}} aH$ (去掉重复出现的陪集) 或 $G = \dot{\bigcup\limits_{a \in H}} Ha$. ■

定义 3.6.2　若 G 可表为 r 个互不相交左 (右) 陪集之并$(r < \infty)$, 则 $r \overset{\triangle}{=} [G : H]$ 称为 H 在 G 中的指标 (Index).

注 3.6.2　我们来说明上述定义的指标不依赖于左陪集或右陪集, 即左陪集个数总是等于右陪集个数. 不妨假设共有 r 个不同的左陪集 (其余各类情形可类似讨论)

$$a_1H, \cdots, a_rH.$$

我们来说明, $Ha_1^{-1}, \cdots, Ha_r^{-1}$ 恰好不重复地跑遍所有右陪集.

若 $Ha_i^{-1} = Ha_j^{-1}$ $(i \neq j)$, 则 $a_i^{-1}a_j \in H$, 因而 $a_j^{-1}a_i = (a_i^{-1}a_j)^{-1} \in H$, 即 $a_iH = a_jH$, 与假设矛盾! 对任何 $b \in G$, 存在 i, 使得 $b^{-1} \in a_iH$, 即 $a_i^{-1}b^{-1} \in H$. 因此 $ba_i = (a_i^{-1}b^{-1})^{-1} \in H$, 即 $b \in Ha_i^{-1}$. ■

例 3.6.6　设 R 是环, I 是理想. $(I, +) < (R, +)$ 作为加法子群的陪集就是

$$a + I := \{a + r \mid r \in I\} := I + a.$$

比如取 $R = \mathbb{Z}$ 及 $I = n\mathbb{Z}$, 共有 n 个陪集

$$r + n\mathbb{Z} = \{r + nk |\ k \in \mathbb{Z}\}, \quad r = 0, 1, \cdots, n-1.$$

因此指标 $[\mathbb{Z}, n\mathbb{Z}] = n$.

这个例子表明, 即使群和子群都是无限群, 它也可能有有限指标. ■

例 3.6.7 设 $G = S_n$, $H = A_n$, 其陪集仅有两个: A_n 及 $(12)A_n = A_n(12)$. 陪集 $(12)A_n$ 恰好就是所有奇置换全体. 此时, $[S_n, A_n] = 2$. ■

例 3.6.8 设 $G = S_3$, $H = \langle(12)\rangle$. 我们共有三个左陪集: H, $(13)H = \{(13), (123)\}$, 以及 $(23)H' = \{(23), (132)\}$. 因此, $[G : H] = 3$. 我们也有三个右陪集: H, $H(13) = \{(13), (132)\}$, 以及 $H(23) = \{(23), (123)\}$. 直接验证得

$$S_n = H \cup (13)H \cup (23)H = H \cup H(13) \cup H(23).$$

容易看到, $(13)H \neq H(13)$, $(23)H \neq H(23)$. ■

定理 3.6.2 (Lagrange) 设 G 有限群, $H < G$, 则

$$|G| = |H| \cdot [G : H].$$

特别地, $|H|$ 整除 $|G|$.

证明 G 是 $[G : H]$个左陪集的并，每个陪集元素个数 $|H|$, 因此 $|G| = |H| \cdot [G : H]$. ■

注 3.6.3 G 的所有不同右陪集个数也是 $[G : H]$. ■

推论 3.6.2 设 $|G| = N$, $a \in G$, 则 $\operatorname{ord} a \mid N$. 特别地, $a^N = e$.

证明 $\operatorname{ord} a = |\langle a\rangle|$, 由 Lagrange 定理, $\operatorname{ord} a \mid N$. ■

推论 3.6.3 素数阶的有限群必是循环群.

证明 设 G 的阶数为素数 p. 取 $a \in G$, 并且 $a \neq e$. 由推论 3.6.2, $\operatorname{ord} a \mid p$. 这就推出 $\operatorname{ord} a = p$, 亦即 $G = \langle a\rangle$. ■

推论 3.6.4 (**欧拉-费马定理**) 对任何 $[a] \in \mathbb{Z}_N^*$, 我们有

$$[a]^{\varphi(N)} = [1],$$

这里 $\mathbb{Z}_N^*$ 是环 $\mathbb{Z}_N$ 的单位群, 即模 N 的既约剩余系 (见例 3.2.6), $\varphi(N)$ 是欧拉函数.

特别地, 若 N 是素数, 则

$$[a]^{N-1} = [1].$$

命题 3.6.1 设 $K < H < G$, 并且 $[G : H] < \infty$, $[H : K] < \infty$, 则

$$[G : K] = [G : H] \cdot [H : K] < \infty.$$

证明 设 $r = [G : H]$, $s = [H : K]$. 设 H 在 G 中所有不同的左陪集为

$$a_1H, \cdots, a_rH,$$

K 在 H 中所有不同的左陪集为

$$b_1K, \cdots, b_sK.$$

我们先说明: 若 $(i,j)\neq(h,k)$, 则 $a_ib_jK\neq a_hb_kK$. 若不然,

$$b_k^{-1}a_h^{-1}a_ib_j=(a_hb_k)^{-1}(a_ib_j)\in K\subseteq H. \tag{3-2}$$

因为 $b_j,b_k\in H$, 所以 $a_h^{-1}a_i\in H$, 即 $a_iH=a_hH$, 从而由假设条件知 $h=i$. 再次由 3-2 推出 $b_k^{-1}b_j\in K$, 故 $b_kL=b_jK$, 从而 $k=j$.

其次说明: K 在 G 中的任何左陪集必可写为 a_ib_jK. 设 $a\in G$. 存在下标 i, 使得 $a_iH=aH$. 因此 $a_i^{-1}a\in H$. 同样地, 存在下标 j, 使得 $a_i^{-1}aK=b_jK$, 即

$$(a_ib_j)^{-1}a=b_j^{-1}a_i^{-1}a\in K.$$

这等价于 $a_ib_jK=aK$.

综上讨论即知诸 a_ib_jK 不重复地跑遍 K 在 G 中所有的左陪集, 因而 $[G:K]=rs$. ■

命题 3.6.2 (正规子群判别法) 设 $H<G$, 则以下条件彼此等价:

(1) $H\lhd G$,

(2) $gHg^{-1}\subseteq H$, $\forall g\in G$,

(3) $H\subseteq gHg^{-1}$, $\forall g\in G$,

(4) $gH\subseteq Hg$, $\forall g\in G$,

(5) $gH\supseteq Hg$, $\forall g\in G$,

(6) $gH=Hg$, $\forall g\in G$.

证明 (1) $\Longleftrightarrow$ (2) 前面已证. 类似可证(1) $\Longleftrightarrow$ (3).

(2) $\Longrightarrow$ (4) $gH=gHg^{-1}\cdot g\subseteq Hg$.

(4) $\Longrightarrow$ (2) $gHg^{-1}\subseteq H\cdot g\cdot g^{-1}=H$.

类似可证 (3) $\Longleftrightarrow$ (5).

(6) 来自于 (4)(5), 反之 (6) 显然蕴含 (4)(5). ■

注 3.6.4 $aH=Ha$ 并不表示 $ah=ha$, $h\in H$. 比如 $G=S_3$, $H=A_3$. 虽然 $(12)A_3=A_3(12)$, 但是 $(12)(123)\neq(123)(12)$. ■

例 3.6.9 设 $H<G$ 的指数 $[G:H]=2$, 证明: $H\lhd G$.

任取 $a\notin H$, 我们只要证 $aH=Ha$ 即可. 由假设条件, H 只有两个不同的左陪集 H,aH. 同样地, 它也只有两个右陪集 H,Ha. 注意到 $G=H\cup aH=H\cup Ha$, 并且 $H\cap aH=H\cap Ha=\emptyset$, 所以 $aH=Ha$. ■

例 3.6.10 设 H_1,H_2 是群 G 的正规子群, 证明: $H_1\cap H_2$ 也是 G 的正规子群.

任取 $h\in H_1\cap H_2$, $g\in G$. 因为 H_1,H_2 是正规的, 所以 $ghg^{-1}\in H_i$, $i=1,2$, 即 $ghg^{-1}\in H_1\cap H_2$. 由 h 的任意性得 $g(H_1\cap H_2)g^{-1}\subseteq H_1\cap H_2$. 再由 g 的任意性及命题 3.6.2 即得结论. ■

例 3.6.11　回顾例 3.5.6 中定义的正规化子 $N(H)$. 它也可以等价地定义为

$$N(H) = \{g \in G |\ gH = Hg\}.$$

因此 $H \lhd N(H)$. 现在我们来证明: 若 $[G : N(H)] < \infty$, 则 H 恰有 $[G : N(H)]$ 个互不相同的共轭子群.

$gHg^{-1} = g'Hg'^{-1}$ 当且仅当 $H = g^{-1}g'H(g^{-1}g')^{-1}$, 故亦等价于 $g^{-1}g' \in N(H)$. 后一条件又等价于 $g'N(H) = gN(H)$. 由此立得结论. ■

例 3.6.12　设 G 是有限群, $H < G$ 且 $H \neq G$, 证明: $G \neq \bigcup\limits_{g\in G} gHg^{-1}$.

由例 3.6.11, H 恰有 $r = [G : N(H)]$ 个互不相同的共轭子群 ($r \geq 2$)

$$g_1Hg_1^{-1}, \cdots, g_rHg_r^{-1}.$$

注意到每个共轭子群都包含幺元 e, 并且 $|g_iHg_i^{-1}| = |H|$. 因此

$$\Big|\bigcup_{g\in G} gHg^{-1}\Big| \leq 1 + \sum_{i=1}^{r}\big(|g_iHg_i^{-1}| - 1\big) = r|H| + 1 - r = \frac{|G|}{[N(H) : H]} + 1 - r < |G|.$$

这就证明了结论. ■

一个有趣的问题是: 群 G 中除了平凡子群外, 是否还有其他正规子群? 对某些群来说, 答案是否定的. 我们把不包含非平凡正规子群的群称作*单群* (Simple group). 我们证明如下重要结果.

定理 3.6.3 (**伽罗华定理**)　*A_n ($n \geq 5$) 是单群.*

证明　设 $H \lhd A_n$ ($n \geq 5$).

首先, 我们说明任何偶置换都能写成 3-阶轮换的乘积. 注意, 偶置换能分解成偶数个对换的乘积. 因此我们只需要证明两个对换的乘积可以分解成 3-阶轮换的乘积. 这可以由如下关系式直接得到:

$$(ij)(ik) = (ikj), \quad (ij)(lk) = (jki)(klj).$$

利用上述结论, 我们只需要证明 H 包含全体 3-阶轮换即可.

其次证明, 如果 H 包含一个 3-阶轮换, 那么它包含所有 3-阶轮换. 换言之, 设 $(i_1i_2i_3) \in H$, 对任何 3-阶轮换 $(j_1j_2j_3)$, 要找到 $\varphi \in A_n$, 使得

$$\varphi(i_1i_2i_3)\varphi^{-1} = (j_1j_2j_3).$$

今取置换 π 使得 $\pi(i_k) = j_k$ ($k = 1, 2, 3$). 若 $\pi \in A_n$, 则取 $\varphi = \pi$. 若 $\pi \neq A_n$, 我们找 $\{i_1, i_2, i_3\}$ 之外的两个数 l, m (注意 $n \geq 5$), 并取 $\varphi = \pi(lm)$.

现在我们用反证法. 假设 H 不含任何 3-阶轮换. 对任何置换 σ, 我们把满足 $\sigma(i) = i$ 的 i 称为 σ 的不动点. 今取非幺元 $\tau \in H$, 使得 τ 的不动点个数达到极大, 记作 r. 由假设条件, $r \leq n - 4$.

我们要证明, 存在 $\psi \in A_n$, 使得 $\tau^{-1}\psi\tau\psi^{-1}$ 的不动点个数大于 r. 这样, 我们就导出矛盾. 另外请注意, $\tau^{-1}\psi\tau\psi^{-1} = \tau^{-1}(\psi\tau\psi^{-1}) \in H$.

将 τ 分解成不相交的轮换乘积. 分两种情形讨论:
(A) 所有轮换都是对换, 比如

$$\tau = (12)(34)\cdots,$$

(B) 存在一个轮换非对换, 比如

$$\tau = (123\cdots)\cdots$$

无论哪种情形, 我们都取 $\psi = (345)$.

对情形 (A), $\tau^{-1}\psi\tau\psi^{-1}$ 保持 $1,2$ 不动, 并且仍保持除了 5 之外其他不动点不动 (若 5 也是不动点的话). 对情形 (B), 至少存在另两个数, 比如 $4,5$, 它们不是 τ 的不动点. 于是 $\tau^{-1}\psi\tau\psi^{-1}$ 保持 1 不动. 它当然也保持 τ 的不动点不动. 无论哪种情形, 都得到矛盾! ■

正规子群类似于环论中的理想. 因此我们很自然地希望建立类似商环的概念. 设 G 是群, A, B 是 G 的非空子集. 我们首先引入子集乘积以及逆的概念:

$$A \cdot B = \{ab \mid a \in A, b \in B\}$$
$$A^{-1} = \{a^{-1} \mid a \in A\}.$$

例 3.6.13 设 G 是单群, $\sigma : G \to G'$ 是非平凡群同态, 因为 $\operatorname{Ker}\sigma$ 是 G 的正规子群, 且 $\operatorname{Ker}\sigma \neq G$, 故 $\operatorname{Ker}\sigma = \{1\}$, 即 σ 为单同态. ■

现在我们要开始建立商群的概念. 首先做一些准备工作.

例 3.6.14 设 $H < G$, $a \in G$.

(1) 若取 $A = \{a\}$, $B = H$, 则 $A \cdot B = aH$ 就是左陪集.

(2) $H^{-1} \cdot H = H \cdot H^{-1} = H \cdot H = H$.

(3) $(A \cdot B) \cdot C = A \cdot (B \cdot C)$.

(4) $(A \cdot B)^{-1} = B^{-1}A^{-1}$. ■

一个基本问题是: 对子群 $H < G$, $(aH) \cdot (bH)$ 是否仍为 H 的左陪集? 很明显, 若它仍是 H 的左陪集, 则等于 abH. 对右陪集, 我们也可以提出类似的问题. 下面的结论给出了回答.

命题 3.6.3 设 $H < G$, 则条件彼此等价:

(1) $(aH) \cdot (bH) = (ab)H$, $\forall a, b \in G$.

(2) $(Ha) \cdot (Hb) = H(ab)$, $\forall a, b \in G$.

(3) $H \lhd G$.

证明 (1) $\Longrightarrow$ (3) 对任何 $g \in G$, 我们有

$$H \cdot g = H \cdot (g \cdot e) \subseteq H \cdot (gH) = (eH) \cdot (gH) = (eg)H = gH.$$

因此由命题 3.6.2 知 H 是 G 的正规子群.

(3) $\Longrightarrow$ (1) 对任何 $a, b \in G$, 由命题 3.6.2,

$$(aH)\cdot(bH) = ((aH)\cdot b)\cdot H = (a(Hb))\cdot H = (a(bH))\cdot H = ((ab)H)H = (ab)(H\cdot H) = (ab)H.$$

类似可证 (2)$\Longleftrightarrow$ (3). ■

定理 3.6.4 *设 G 是群, H 是 G 的正规子群, 记 G/H 为 H 的所有不同陪集全体. 那么 G/H 在子集合的乘法运算下构成群, 称作 G 对 H 的商群* (Quotient group). *特别地, G/H 的幺元就是 H.*

证明 结合律是显然的. 命题3.6.3 给出了运算的封闭性. 因为 $H\cdot aH = aH$, $(a^{-1}H)\cdot(aH) = H$, $\forall a \in G$, 所以由命题 3.4.1, G/H 构成群. ■

注 3.6.5 为了方便书写, 在不产生歧义的情形下, 我们今后把商群中的元素 aH 仍写成 $[a]$ 或 $\bar{a}$. ■

推论 3.6.5 *如果 $H \lhd G$, 并且 $[G:H] < \infty$, 那么 G/H 是有限群且 $|G/H| = [G:H]$.*

推论 3.6.6 *设 $H \lhd G$, $a \in G$, 则 $(aH)^{-1} = a^{-1}H$.*

证明 $(aH)^{-1} = H^{-1}\cdot a^{-1} = Ha^{-1}$. ■

例 3.6.15 设 I 是环 R 的理想, 则商环 R/I 作为加法群就是 $(R,+)$ 对子群 $(I,+)$ 的商群. 比如 $(\mathbb{Z}_N,+) = \mathbb{Z}/N\mathbb{Z}$. ■

例 3.6.16 设 $H < G$, $[G:H] = 2$, 则 $G/H \cong \mathbb{Z}_2$. 比如 $S_n/A_n \cong \mathbb{Z}_2$. ■

例 3.6.17 设 $G = \langle a\rangle$ 是 N 阶子群, $H = \langle a^d\rangle$ $(d \mid N)$, 则 $G/H \cong \mathbb{Z}_d$. 具体言之, $G/H = \{H, aH, \cdots, a^{d-1}H\}$, 并且 $(aH)^d = a^dH = H$.

比如 $\mathbb{Z}_N/\langle[d]\rangle = \mathbb{Z}_d$, 这里 $d \mid N$. ■

例 3.6.18 (**群的阿贝尔化**) 设 G 是群, $[G,G]$ 是换位子群 (见例 3.5.11). 前已证, $[G,G]$ 是正规子群. 我们来验证商群 $G/[G,G]$ 是交换群. 这是因为对任何 $[r],[s] \in G/[G,G]$, 因为 $r^{-1}s^{-1}rs \in [G,G]$, 所以

$$[r]^{-1}[s]^{-1}[r][s] = [r^{-1}s^{-1}rs] = [0] \in G/[G,G],$$

即 $[r][s] = [s][r]$. 我们把这个商群称作 G 的阿贝尔化. 它相当于把原来的群乘法变成了可交换的.

今取 $G = S_n$, 我们验证 $[G,G] = A_n$, 因而 $G/[G,G] \cong \mathbb{Z}_2$. 首先, 因为 $[G,G]$ 中的换位子显然都是偶置换, 所以 $[G,G] \in A_n$. 反过来, 由伽罗华定理的证明知, A_n 中的元素都可以分解成 3-阶轮换的乘积. 注意到每个 3-阶轮换 (ijk) 都可以分解为

$$(ijk) = (ik)^{-1}(jk)^{-1}(ik)(jk).$$

因此, $A_n = [G,G]$. ■

例 3.6.19 (外自同构群) 设 G 是群, $\mathrm{Aut}G$ 是自同构群, $\mathrm{Inn}G$ 是内自同构群, 我们把商群

$$\mathrm{Out}G := \mathrm{Aut}G/\mathrm{Inn}G.$$

称为 G 的外自同构群 (Outer automorphism group). 一个经典的计算结果是:

$$\mathrm{Out}(S_n) = \begin{cases} \{1\}, & n \neq 6, \\ \mathbb{Z}_2, & n = 6. \end{cases} \quad \mathrm{Out}(A_n) = \begin{cases} \mathbb{Z}_2, & n \neq 6, \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2, & n = 6. \end{cases}$$ ■

设 $H \lhd G$. 我们定义映射

$$\pi : G \longrightarrow G/H, \quad a \to aH.$$

因为

$$\pi(ab) = (ab)H = (aH) \cdot (bH) = \pi(a)\pi(b),$$

所以 π 是同态映射. 我们称之为自然同态.

命题 3.6.4 设 $H \lhd G$, 则自然同态 $\pi : G \longrightarrow G/H$ 是满同态, 且 $\mathrm{Ker}\,\pi = H$. 特别地, 任何正规子群都是某个群同态的核.

证明 首先证 $\mathrm{Im}\pi = G/H$. 设 $aH \in G/H$, 则 $\pi(a) = aH$. 由 aH 的任意性即得 $\mathrm{Im}\pi = G/H$.

其次证 $\mathrm{Ker}\,\pi = H$. 对任意 $x \in H$, 我们有 $\pi(x) = xH = H$. 因而 $H \subseteq \mathrm{Ker}\,\pi$. 反过来, 对任何 $x \in \mathrm{Ker}\,\pi$,$H = \pi(x) = xH$, 因而 $x \in H$. 这就推出 $\mathrm{Ker}\,\pi \subseteq H$. 综上可知, $\mathrm{Ker}\,\pi = H$. ■

接下来, 我们要仿照环论的结果, 引入群同态基本定理. 为此先做一些准备工作.

引理 3.6.3 设 $\sigma : G \to G'$ 是满同态, $H < G$, $H' < G'$, 则

(1) $\sigma(H) < G'$, $\mathrm{Ker}\,\sigma \lhd \sigma^{-1}(H) < G$. 进一步, 如果 $H \lhd G$ (相应地, $H' \lhd G'$), 则 $\sigma(H) \lhd G'$ (相应地, $\sigma^{-1}(H') \lhd G$).

(2) $\sigma(\sigma^{-1}(H')) = H'$.

(3) $H \subseteq \sigma^{-1}(\sigma(H))$. 进一步, 若 $\mathrm{Ker}\,\sigma \subseteq H$, 则 $H = \sigma^{-1}(\sigma(H))$.

证明 设 e (相应地, e') 是 G (相应地, G') 的幺元, $N = \mathrm{Ker}\,\sigma$.

(1) 任取 $r, s \in \sigma(H)$. 设 $a, b \in H$ 满足 $r = \sigma(a)$, $s = \sigma(b)$,

$$rs^{-1} = \sigma(a)\sigma(b)^{-1} = \sigma(ab^{-1}) \in \sigma(H),$$

故 $\sigma(H) < G'$.

任取 $a, b \in \sigma^{-1}(H')$, 则有

$$\sigma(ab^{-1}) = \sigma(a)\sigma(b)^{-1} \in H',$$

即 $ab^{-1} \in \sigma^{-1}(H')$. 由 a, b 的任意性, $\sigma^{-1}(H') < G$. 注意到 $\sigma(n) = e' \in H'$, $\forall n \in N$, 所以 $n \in \sigma^{-1}(H')$. 由 n 的任意性即知 $N < \sigma^{-1}(H')$. 注意 $N \lhd G$, 故 $N \lhd \sigma^{-1}(H')$.

今设 $H \lhd G$. 对任何 $r \in G'$, $s \in \sigma(H)$, 取 $g \in G, h \in H$ 满足 $r = \sigma(g)$, $s = \sigma(h)$. 于是 $rsr^{-1} = \sigma(ghg^{-1}) \in \sigma(H)$. 由 r, s 的任意性, $\sigma(H) \lhd G'$.

设 $H' \lhd G'$. 任取 $g \in G$, $x \in \sigma^{-1}(H')$. 因为

$$\sigma(gxg^{-1}) = \sigma(g)\sigma(x)\sigma(g)^{-1} \in H',$$

故 $gxg^{-1} \in \sigma^{-1}(H')$. 由 g, x 的任意性即得 $\sigma^{-1}(H') \lhd G$.

(2) 对任何 $r \in H'$, 设 $a \in G$ 满足 $r = \sigma(a)$. 因而 $a \in \sigma^{-1}(H')$, 故

$$r = \sigma(a) \in \sigma(\sigma^{-1}(H')).$$

由 r 的任意性, $H' \subseteq \sigma(\sigma^{-1}(H'))$.

反过来, 任取 $x \in \sigma^{-1}(H')$, 有 $\sigma(x) \in H'$. 由 x 的任意性, $\sigma(\sigma^{-1}(H')) \subseteq H'$.

(3) 前半部分显然. 今假设 $\mathrm{Ker}\,\sigma \subseteq H$. 对任何 $x \in \sigma^{-1}(\sigma(H))$, 有 $\sigma(x) \in \sigma(H)$, 即存在 $h \in H$, 满足 $\sigma(x) = \sigma(h)$, 亦即 $x \in h\mathrm{Ker}\,\sigma$. 由假设条件即得 $x \in hH \subseteq H$. 由 x 的任意性, $\sigma^{-1}(\sigma(H)) \subseteq H$. ■

定理 3.6.5 (同态基本定理) 设 $\sigma : G \to G'$ 是满同态, 则

(1) 我们有同构

$$\bar{\sigma} : G/\mathrm{Ker}\,\sigma \cong G', \quad a(\mathrm{Ker}\,\sigma) \to \sigma(a).$$

(2) 设

$$A = \{G \text{ 中所有包含 } \mathrm{Ker}\,\sigma \text{ 的子群}\},$$
$$B = \{G' \text{ 中所有子群}\}.$$

那么 A, B 之间存在一一对应

$$\Phi : A \longrightarrow B, \quad H \to \sigma(H).$$

(3) 设

$$A' = \{G \text{ 中所有包含 } \mathrm{Ker}\,\sigma \text{ 的正规子群}\},$$
$$B' = \{G' \text{ 中所有正规子群}\}.$$

那么 A', B' 之间存在一一对应

$$\Phi' : A' \longrightarrow B', \quad K \to \sigma(K),$$

这里的 Φ' 就是 Φ 在 A' 上的限制.

证明 设 e (相应的, e') 是 G (相应的, G') 的幺元, $N = \mathrm{Ker}\,\sigma$.

(1) 我们首先验证 $\bar{\sigma}$ 的定义合理. 设 $aN = bN$. 我们有 $a^{-1}b \in N$, 故 $\sigma(a^{-1}b) = e'$, 即 $\sigma(a) = \sigma(b)$. 因为

$$\bar{\sigma}(aN \cdot bN) = \bar{\sigma}((ab)N) = \sigma(ab) = \sigma(a)\sigma(b) = \bar{\sigma}(aN)\bar{\sigma}(bN),$$

所以 $\bar{\sigma}$ 是同态.

今验证 $\bar{\sigma}$ 是单同态, 即 $\mathrm{Ker}\,\bar{\sigma} = \{N\}$. 显见 $\bar{\sigma}(N) = \sigma(e) = e'$. 因此 $N \in \mathrm{Ker}\,\bar{\sigma}$. 反过来, 设 $aN \in \mathrm{Ker}\,\bar{\sigma}$, 则

$$e' = \bar{\sigma}(aN) = \sigma(a),$$

故 $a \in N$, 即 $aN = N$. 因此, $\mathrm{Ker}\,\bar{\sigma} = \{N\}$.

最后验证 $\bar{\sigma}$ 是满同态. $\forall y \in G'$, 因 σ 是满的, 故存在 $x \in G$, 使得 $y = \sigma(x)$. 因此 $\bar{\sigma}(xN) = \sigma(x) = y$.

(2) 设 $N < H < G$. 由引理 3.6.3, $\sigma(H) < G'$. 这就给出了映射 $\Phi : A \to B$. 其次验证 Φ 是满射, 即对任意 $H' < G'$, 由引理 3.6.3, $N \lhd \sigma^{-1}(H') < G$ 且 $\sigma(\sigma^{-1}(H')) = H'$.

最后验证, Φ 是单射. 设 $H_1, H_2 \in A$ 满足 $\sigma(H_1) = \sigma(H_2)$. 由引理 3.6.3 以及 H_i 的选取,

$$H_1 = \sigma^{-1}(\sigma(H_1)) = \sigma^{-1}(\sigma(H_2)) = H_2.$$

综上, Φ 是一一对应. 特别地,

$$\Phi^{-1} : B \longrightarrow A, \quad H' \to \sigma^{-1}(H).$$

(3) 设 $K \in A'$, 引理 3.6.3 推出 $\sigma(K) \lhd G'$. 这样, Φ 限制在 A' 上就得到 Φ'. 因而 Φ' 是单的. 现在证明 Φ' 是满的. 任取 $H' \lhd G'$, 由引理 3.6.3, $\sigma^{-1}(H') \lhd G$, 所以 Φ' 是满的. ■

例 3.6.20 (1) 回顾置换群的符号映射

$$\mathrm{sgn} : S_n \longrightarrow U_2, \quad \tau \to sgn(\tau).$$

前面已证 $\mathrm{Ker}\,\mathrm{sgn} = A_n$, sgn 是满的. 因此由同态基本定理, $S_n/A_n \cong U_2$.

(2) 回顾行列式映射

$$\det : GL_n(F) \longrightarrow F^*, \quad A \to \det A.$$

$\mathrm{Ker}\det = SL_n$, det 是满的. 由同态基本定理得 $GL_n(F)/SL_n(F) \cong F^*$.

(3) 设 $G =< a >$ 是循环群, $|G| = d$. 回顾指数映射

$$\sigma : \mathbb{Z} \longrightarrow G, n \to a^n.$$

σ 是满同态, $\mathrm{Ker}\,\sigma = \{k | a^k = e\} = d\mathbb{Z}$, 故 $\mathbb{Z}/d\mathbb{Z} \cong G$. ■

例 3.6.21 设 $C(G)$ 是 G 的中心, $\mathrm{Inn}G$ (定义见例 3.5.12) 是内自同构群. 我们有群的满同态

$$\sigma : G \longrightarrow \mathrm{Inn}G, \quad g \to \sigma_g.$$

此时, $\mathrm{Ker}\,\sigma = C(G)$, 因而由同态基本定理得 $G/C(G) \cong \mathrm{Inn}G$. ■

推论 3.6.7 设 $\sigma : G \to G'$ 是群同态, 则 $G/\mathrm{Ker}\,\sigma \cong \mathrm{Im}\sigma$.

推论 3.6.8 设 $N < H < G$, 并且 N 是 G 的正规子群, 则

$$H/N = \{hN \mid h \in H\}$$

是 G/N 的子群. 进一步, 若 $H \lhd G$, 则 $H/N \lhd G/N$.

反过来, G/N 中的每个 (正规) 子群都可以写成 H/N, 这里 H 是 G 的 (正规) 子群.

推论 3.6.9 设 $N \lhd G$, $\pi : G \to G/N$ 是自然同态, $H < G$, 则

(1) $N \lhd HN < G$, 并且 HN 是包含 N 和 H 的最小子群;

(2) π 在 H 上的限制给出满同态 $\pi|_H : H \to HN/N$;

(3) (**同构基本定理**) $\pi|_H$ 诱导了同构 $\bar{\pi}_H : H/(H \cap N) \cong HN/N$.

证明 (1) 任取 $r, s \in HN$, 则可将它们写作 $r = h_1 n_1$, $s = h_2 n_2$.

$$r^{-1}s = (n_1^{-1}h_1^{-1})(h_2 n_2) = (n_1^{-1}(h_1^{-1}h_2))n_2 \in (N(h_1^{-1}h_2))n_2.$$

由于 N 是正规的, 故 $N(h_1^{-1}h_2) \subseteq (h_1^{-1}h_2)N$, 因而

$$r^{-1}s \in (h_1^{-1}h_2)(Nn_2) \subseteq (h_1^{-1}h_2)N \subseteq HN.$$

由 r, s 的任意性即知 $HN < G$. 其余结论是显然的.

(2) 我们只需要证 $\pi(H) = HN/N$. 对任何 $h \in H$, 显然有 $\pi(h) = hN \in HN/N$. 因此 $\pi(H) \subseteq HN/N$. 反过来, HN/N 中的元素都可写为 hN (这里 $h \in H$), 因而 $HN/N \subseteq \pi(H)$.

(3) 我们只需要证 $\mathrm{Ker}\,\pi|_H = H \cap N$, 这样就能由同态基本定理得到想要的同构. 设 $x \in H \cap N$, 则 $\pi|_H(x) = xN = N$, 故 $x \in \mathrm{Ker}\,\pi|_H$. 由 x 的任意性知 $H \cap N \subseteq \mathrm{Ker}\,\pi|_H$. 反之, 设 $y \in \mathrm{Ker}\,\pi|_H (\subseteq H)$, 即 $N = \pi(y) = yN$. 这表明 $y \in N \cap H$. 这就推出 $\mathrm{Ker}\,\pi|_H \subseteq H \cap N$. ■

推论 3.6.10 *在推论 3.6.9 的条件下, 假设 G 是有限群, 则*

$$\frac{|H| \cdot |N|}{|H \cap N|} = |HN|.$$

推论 3.6.11 (**同构基本定理**) *设 $N < H$ 都是 G 的正规子群, 则存在群同构*

$$(G/N)/(H/N) \cong G/H.$$

证明 我们定义映射

$$\sigma : G/N \longrightarrow G/H, \quad gN \to gH.$$

首先说明映射的合理性. 设 $gN = g'N$, 则 $g^{-1}g' \in N \subseteq H$, 故 $gH = g'H$.

其次验证 σ 是同态.

$$\sigma(aN \cdot bN) = \sigma((ab)N) = (ab)H = (aH)(bH) = \sigma(aN)\sigma(bN).$$

显见 σ 是满的.

接下来, 我们验证 $\mathrm{Ker}\,\sigma = H/N$. 任取 $h \in H$, $\sigma(hN) = hH = H$, 即 $hN \in \mathrm{Ker}\,\sigma$. 由 h 的任意性得 $H/N \subseteq \mathrm{Ker}\,\sigma$. 反过来, 设 $gN \in \mathrm{Ker}\,\sigma$, 即 $H = \sigma(gN) = gH$. 因而 $g \in H$, $gN \in H/N$. 这样, $\ker\sigma \subseteq H/N$.

现在, 利用同态基本定理即得所需同构. ■

3.6.2 构造方法 (IV): 群的直积

设 G_1, G_2 群, e_i 是 G_i 的幺元 $(i = 1, 2)$. 我们构造集合

$$G := G_1 \times G_2 = \{(g_1, g_2) | g_1 \in G_1, g_2 \in G_2\}.$$

设 $(g_1, g_2) \in G, (h_1, h_2) \in G$, 定义 G 上的运算

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 h_1, g_2 h_2) \in G_1 \times G_2.$$

命题 3.6.5　$G = G_1 \times G_2$ 在上述运算下构成群,

(1) 其幺元为 $e = (e_1, e_2)$.

(2) $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$, 此处 $g_1 \in G_1$, $g_2 \in G_2$.

$G = G_1 \times G_2$ 称为 G_1 和 G_2 的外直积 (External direct product).

命题 3.6.6　设 G_1, G_2 群.

(1) $G_1 \times G_2$ 是有限群当且仅当 G_1, G_2 都是有限群. 此时 $|G_1 \times G_2| = |G_1| \cdot |G_2|$.

(2) $G_1 \times G_2$ 是交换群当且仅当 G_1, G_2 都是交换群. 此时也记作 $G_1 \oplus G_2$, 改称为 G_1, G_2 的直和 (Direct sum).

(3) $G_1 \times G_2 \cong G_2 \times G_1$, $(g_1, g_2) \to (g_2, g_1)$.

(4) $G_1 \times G_2$ 有两个正规子群

$$H_1 = \{(g_1, e_2) | g_1 \in G_1\}, \quad H_2 = \{(e_1, g_2) | g_2 \in G_2\},$$

并且 $H_1 \cong G_1$, $H_2 \cong G_2$.

(5) 我们有满同态

$$\begin{aligned} \pi_1 : G_1 \times G_2 &\longrightarrow G_1, & \pi_2 : G_1 \times G_2 &\longrightarrow G_2, \\ (x, y) &\to x, & (x, y) &\to y. \end{aligned}$$

因而有同构 $G_1 \times G_2/H_2 \cong G_1$, $G_1 \times G_2/H_1 \cong G_2$.

例 3.6.22　$\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{([0],[0]), ([1],[0]), ([0],[1]), ([1],[1])\}$. 考察 A_4 中子群

$$H = \{(1), (12)(34), (13)(24), (14)(23)\}.$$

我们可以验证如下同构

$$\begin{aligned} \pi : \mathbb{Z}_2 \oplus \mathbb{Z}_2 &\longrightarrow H \\ ([1],[0]) &\to (12)(34) \\ ([0],[1]) &\to (13)(24) \\ ([1],[1]) &\to (14)(23) \\ ([0],[0]) &\to (1) \end{aligned}$$

■

类似地, 我们可以定义 r 个群 $G_1, \cdots, G_r$ 的直积

$$G_1 \times \cdots \times G_r.$$

若 $G_1, G_2, \cdots, G_r$ 是交换群, 则 G 也是交换群. 此时改记为 $G = G_1 \oplus G_2 \oplus \cdots \oplus G_r$, 称作直和. 我们也有类似命题 3.6.6 的结论. 这里不再赘述.

例 3.6.23　环的直和 $R_1 \oplus \cdots \oplus R_r$ 作为加法群就是诸 $(R_i, +)$ 的直和. ■

类似环直和的讨论, 我们有如下经典例子.

例 3.6.24 (**中国剩余定理**) 设 $m_1, m_2, \cdots, m_r$ 是两两互质的正整数, $m_i > 1$, $M = \prod_{i=1}^{r} m_i$, 则

$$\mathbb{Z}_M \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}.$$

比如我们可以直接验证如下同构

$$\sigma : \mathbb{Z}_2 \oplus \mathbb{Z}_3 \longrightarrow \mathbb{Z}_6, (\bar{a}, \bar{b}) \to \overline{3a + 4b}. \quad \sigma\text{同构}.$$

读者可以参考环论情形的一般证明, 即先诱导同态

$$\sigma : \mathbb{Z} \longrightarrow \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}, \quad n \to ([n]_{m_1}, \cdots, [n]_{m_r}).$$

然后求得核 $\mathrm{Ker}\,\sigma = M\mathbb{Z}$. 由群同态基本定理得 $\mathbb{Z}_M \cong \mathrm{Im}\sigma$. 因为 $|\mathrm{Im}\sigma| = |\mathbb{Z}_M| = M$, 且

$$|\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}| = m_1 \cdots m_r = M,$$

故 $\mathrm{Im}\sigma = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}$. ■

推论 3.6.12 设 n 是正整数, $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ 是标准分解式, $p_1 < \cdots < p_s$ 是素数, 则

$$\mathbb{Z}_n \cong \bigoplus_{i=1}^{s} \mathbb{Z}_{p_i^{\alpha_i}}.$$

定理 3.6.6 (Abel **定理**) 若 G 是有限交换群, 那么 $G \cong \bigoplus\limits_{i=1}^{r} \mathbb{Z}_{m_i}$, 这里 m_i 是素数方幂. 此时 $|G| = m_1 m_2 \cdots m_r$.

注 3.6.6 请注意, 上述结论中的 m_i, m_j 未必互质. ■

定义 3.6.3 设 G 是群, $H \triangleleft G, K \triangleleft G$, 满足

(1) $G = HK$,

(2) $H \cap K = \{e\}$,

则称 G 是 H 和 K 内直积 (Internal direct product). 若 G 是交换群, 则上述 $G = H + K$ 也称之为内直和.

例 3.6.25 设 $G = \mathbb{Z}_6$, $H = \langle [2] \rangle$, $K = \langle [3] \rangle$. 可以验证, $H \cap K = \{[0]\}$, $H + K = \mathbb{Z}_6$. 所以 G 是 H 和 K 内直和. ■

例 3.6.26 设 $G = (\mathbb{Z}_7^*, \cdot) = \{[1], [2], \cdots, [6]\} = \langle [3] \rangle$. $H = \langle [2] \rangle = \{[1], [2], [4]\}$, $K = \langle [6] \rangle = \{[1], [6]\}$. 可以验证, $H \cap K = \{[0]\}$,

$$H \cdot K = G.$$

所以 G 是 H 和 K 内直积. ■

定理 3.6.7 设 G 是 H 和 K 内直积, 则存在同构

$$\sigma : H \times K \longrightarrow H \cdot K (= G), \quad (h, k) \to hk.$$

证明 首先验证 σ 是同态. 注意到

$$\sigma((h_1,k_1)(h_2,k_2)) = \sigma((h_1h_2,k_1k_2)) = h_1h_2k_1k_2,$$
$$\sigma((h_1,k_1))\sigma((h_2,k_2)) = h_1k_1h_2k_2.$$

因此我们只需要证 $h_1h_2k_1k_2 = h_1k_1h_2k_2$, 即 $k_1^{-1}h_2k_1h_2^{-1} = e$. 利用 H 的正规性, 可得

$$k_1^{-1}h_2k_1h_2^{-1} = (k_1^{-1}h_2k_1)h_2^{-1} \in Hh_2^{-1} \subseteq H.$$

同理 $k_1^{-1}h_2k_1h_2^{-1} \in K$. 因此 $k_1^{-1}h_2k_1h_2^{-1} \in H \cap K = \{e\}$, 所以 $k_1^{-1}h_2k_1h_2^{-1} = e$.

再证 σ 是单的. 设 $(h,k) \in \operatorname{Ker}\sigma$, 则 $hk = e$, 即 $h = k^{-1}$.
注意到

$$h = k^{-1} \in H \cap K = \{e\},$$

所以 $(h,k) = (e,e)$, 即 $\operatorname{Ker}\sigma = \{(e,e)\}$.

最后证 σ 是满的.
$\forall x \in G$, 由于 $G = HK$. 故 $\exists h \in H, k \in K, x = hk$. 因此 $x = \sigma((h,k))$. ■

推论 3.6.13 *设 $G = HK$ 为 G 的内直积.*

(1) *若 G 有限群, 则 $|G| = |H| \cdot |K|$.*

(2) *对任何 $g \in G$, 存在唯一的 $h \in H$ 及 $k \in K$ 满足 $g = hk$.*

(3) *对任何 $h \in H$, $k \in K$, $hk = kh$.*

(4) *考虑 $H \times K$ 的正规子群*

$$H' = \{(h,e) |\ h \in H\}, \quad K' = \{(e,k) |\ k \in K\},$$

则 $H' \cong H, K' \cong K$, $H \times K \cong H' \times K' \cong G$.

(5) $G/H \cong K, G/K \cong H$.

证明 我们只证 (5), 其余结论是显然的. 考虑群同态 $\phi_1 : G \xrightarrow{\sim} H \times K$ 及 $\phi_2 : H \times K \longrightarrow K, (h,k) \to k$, 我们得到复合群同态 $\phi_2\phi_1 : G \longrightarrow K$. 我们只需要证明 $\operatorname{Ker}(\phi_2\phi_1) = H$, 这样就能用同态基本定理得到 $G/H \cong K$.

设 $g \in \operatorname{Ker}(\phi_2\phi_1)$. 由于 $G = HK$ 是内直积, 故存在 $h \in H$ 及 $k \in K$, 满足 $g = hk$. 因 $\phi_1(g) = (h,k)$, 所以

$$e = \phi_2\phi_1(g) = \phi_2((h,k)) = k,$$

即 $g = h \in H$.
反之, 对任何$h \in H$,

$$\phi_2\phi_1(h) = \phi_2((h,e)) = e.$$

综上可知 $\operatorname{Ker}(\phi_2\phi_1) = H$. 同理可证 $G/K \cong H$. ■

内直和的概念也可以推广到一般情形. 设 $H_1, H_2, \cdots, H_r$ 是 G 的正规子群, 满足

(1) $G = H_1H_2\cdots H_r$,

(2) $(H_1\cdots H_i)\cap H_{i+1} = \{e\}$, $i = 1, 2, \cdots, r-1$,

则称 G 是 $H_1, \cdots, H_r$ 的内直积. 如果 G 是交换群, 则也称为内直和.

注 3.6.7 (1) 此时类似可证 $H_1 \times H_2 \times \cdots \times H_r \cong H_1 \cdots H_r$.
(2) 内直和的定义类似于向量空间的直和分解. 请注意, 条件 (2) 千万不能换成

$$H_i \cap H_j = \{e\}, \quad \forall i, j, \quad i \neq j.$$

但是条件 (2) 可以换成: 任何 $g \in G$, 可以有唯一分解

$$g = h_1 \cdots h_r, \quad h_i \in H_i, \quad i = 1, 2, \cdots, r.$$

(3) 在很多情况下, 我们也笼统地称之为直积. ■

推论 3.6.14 设 G_1, G_2 是群, $(a, b) \in G_1 \times G_2$, 则$\mathrm{ord}(a, b) = [\mathrm{ord}a, \mathrm{ord}b]$, 这里 $[,]$ 是最小公倍数.

证明 令 $m = \mathrm{ord}a$, $n = \mathrm{ord}b$, $s = \mathrm{ord}(a, b)$.

$$(e, e) = (a, b)^s = (a^s, b^s)$$

蕴含着 $m \mid s$, $n \mid s$, 因而 $[m, n] \mid s$. 另一方面, $(a, b)^{[m,n]} = (a^{[m,n]}, b^{[m,n]}) = (e, e)$, 故 $s \mid [m, n]$. 因此 $s = [m, n]$. ■

推论 3.6.15 设 G 是群, $a, b \in G$ 是有限阶的元素, 满足 $ab = ba$, 则

$$|\langle (a, b)\rangle| = [|\langle a\rangle|, |\langle b\rangle|].$$

例 3.6.27 求 $\mathbb{Z}_2 \oplus \mathbb{Z}_6$ 中 2 阶元素.

设 $(a, b) \in \mathbb{Z}_2 \oplus \mathbb{Z}_6$, 满足 $\mathrm{ord}(a, b) = 2$. 因而 $2 = [ord(a), ord(b)]$. 这就推出如下几种可能:

(1) $\mathrm{ord}(a) = 1$, $\mathrm{ord}b = 2$. 此时直接验证知 $a = [0]$, $b = [3]$.

(2) $\mathrm{ord}(a) = 2$, $\mathrm{ord}b = 1$. 此时 $a = [1]$, $b = [0]$.

(3) $\mathrm{ord}(a) = \mathrm{ord}b = 2$. 此时 $a = [1]$, $b = [3]$.

因此 $\mathbb{Z}_2 \oplus \mathbb{Z}_6$ 共有三个 2 阶元素. ■

例 3.6.28 设 $G_1 = \langle a\rangle$, $G_2 = \langle b\rangle$ 是有限循环群. 我们有

$$G_1 \times G_2 = \langle (a, e_2), (e_1, b)\rangle = \{(a, e_2)^n \cdot (e_1, b)^m | n, m \in \mathbb{Z}\}.$$

一般来说, $G_1 \times G_2 \neq \langle (a, b)\rangle$. $\langle (a, b)\rangle$ 只是 $G_1 \times G_2$ 的循环子群.

$G_1 \times G_2 = \langle (a, b)\rangle$ 等价于 $|G_1 \times G_2| = |\langle (a, b)\rangle|$, 即

$$\mathrm{ord}((a, b)) = \mathrm{ord}(a)\mathrm{ord}(b),$$

亦即

$$[ord(a), ord(b)] = \mathrm{ord}(a) \cdot \mathrm{ord}(b).$$

这表明 $G_1 \times G_2 = \langle (a, b)\rangle$ 当且仅当 $\gcd(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$. ■

3.7 群作用

3.7.1 基本概念与例子

设 G 是群, $e \in G$ 是幺元, X 是非空集合, $S(X)$ 是 X 的全变换群 (即 X 到自身的所有一一对应构成的群).

定义 3.7.1 *如果存在一个映射*

$$f : G \times X \to X, \quad (g, x) \to f(g, x)$$

满足如下条件, 则称 G 作用在 X 上.

(1) $f(e, x) = x, \forall x \in X,$

(2) $f(gg', x) = f(g, f(g', x)), \forall x \in X, \forall g, g' \in G.$

有时为方便书写, 也简记 $gx := f(g, x)$ 或者 $g(x) := f(g, x)$. 这样, 群作用的两个条件就可写为

$$ex = x, \quad (gg')x = g(g'x), \quad \forall x \in X, \forall g, g' \in G.$$

对任何 $g \in G$, 上述群作用给出了一个 X 到自身的映射

$$\sigma_g : X \longrightarrow X, \quad x \to gx.$$

同样地, g^{-1} 也给出映射

$$\sigma_{g^{-1}} : X \longrightarrow X, \quad x \to g^{-1}x.$$

可以验证

$$\sigma_{g^{-1}}\sigma_g(x) = g^{-1}(gx) = (g^{-1}g)(x) = ex = x, \quad \forall x \in X.$$

因此 $\sigma_{g^{-1}}\sigma_g = \mathrm{Id}_X$. 同理 $\sigma_g\sigma_{g^{-1}} = \mathrm{Id}_X$. 这表明 $\sigma_g \in S(X)$, 即它是 X 到自身的一一对应, 其逆映射就是 $\sigma_{g^{-1}}$. 进一步, 我们可以用同态的语言等价地描述群作用.

命题 3.7.1 *以下条件彼此等价:*

(1) *群 G 作用在集合 X 上.*

(2) *存在群同态 $\psi : G \to S(X)$.*

条件成立时, $\psi(g)(x) = gx, \forall g \in G, \forall x \in X.$

证明 (1) $\Longrightarrow$ (2) 由前面讨论, 我们定义 $\psi : G \to S(X)$, 满足 $\psi(g) = \sigma_g$ (定义见上). 因为

$$\psi(e)(x) = \sigma_e(x) = ex = x$$

以及

$$\psi(gg')(x) = \sigma_{gg'}(x) = (gg')x = g(g'x) = \sigma_g(\sigma_{g'}(x)) = (\psi(g)\psi(g'))(x), \quad \forall x \in X, \quad \forall g, g' \in G,$$

所以 ψ 是群同态.

(2) $\Longrightarrow$ (1) 定义 $gx := \psi(g)(x)$, $\forall g \in G$, $\forall x \in X$. 我们有 $ex = \psi(e)(x) = \mathrm{Id}_X(x) = x$, 以及

$$(gg')x = \psi(gg')(x) = (\psi(g)\psi(g'))(x) = \psi(g)(\psi(g')(x)) = g(g'x).$$

因而 ψ 诱导了一个群作用. ■

上述结论表明, 群作用的定义条件实际上对应了群同态的定义条件.

推论 3.7.1 *设 $H < G$, 且 G 在 X 上有一群作用, 则它也诱导了 H 在 X 上的作用. 设 $\varphi : G' \to G$ 是群同态, 则可诱导 G' 在 X 上的群作用, $g'x := \varphi(g')x$, $\forall g' \in G'$.*

下面我们例举各种经典的群作用.

例 3.7.1 (**平凡作用**) 我们定义

$$gx = x, \quad \forall g \in G, \quad \forall x \in X.$$

这显然是群作用. 但是它对 X 的作用是平凡的. ■

例 3.7.2 设 $G = \{1, -1\}$ 是二元乘法群, $X = G'$ 是任一群. 我们定义

$$1x := x, \quad (-1)x := x^{-1}.$$

容易验证, 这是个群作用. ■

例 3.7.3 (**置换群作用**) 设 $X = \{1, 2, \cdots, n\}$, $G = S_n$. 对任何

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \in S_n$$

给出作用 $\sigma(i) := a_i$. ■

例 3.7.4 (**线性变换**) 设 $G = GL_n(F)$ 是数域 F 上的一般线性群, $X = V$ 是 F 上的 n 维线性空间. G 中的元素对应的线性变换 $\sigma : V \to V$ 自然诱导了作用 $\sigma(x)$, $\forall x \in X$. 换言之, 我们有自然的嵌入同态

$$\psi : G \hookrightarrow S(X).$$

由命题 3.7.1, 即得上述群作用.

考虑特殊线性群 $SL_n(F) < GL_n(F)$. 由推论 3.7.1, 它也自然作用在 X 上. 从几何上看, 它描述了所有保定向的线性变换. 类似地, 还能定义正交群 $O_n(F)$ 与特殊正交群 $SO_n(F)$ 的在该空间上的作用. 我们也能定义二面体群及其子群在正多边形上的作用等等, 这里不再详细展开.■

例 3.7.5 (**莫比乌斯变换**) 设 G 是扩充复平面 $\overline{\mathbb{C}}$ 上的全体莫比乌斯变换构成的群. $X = \overline{\mathbb{C}}$. G 自然诱导了 X 上的作用. ■

例 3.7.6 (**左平移**) 设 G 是群, $X = G$. 对任意 $g \in G$, 我们定义

$$g(x) = gx, \quad \forall x \in X,$$

即将 g 左乘到每个元素上. 容易验证这是一个群作用, 我们称之为*左平移* (Left translation) 或者*左乘* (Left multiplication).

由命题 3.7.1, 左平移诱导了群同态

$$\psi : G \to S(X).$$

对任何非幺元 $g \in G$, 因为 $gx \neq x$, $\forall x \in G$, 所以 g 在 G 上的作用不可能是平凡的. 这表明 $\operatorname{Ker}\psi = \{e\}$, 即$\psi$ 是单同态. ■

例 3.7.6 的讨论, 让我们得到如下经典定理.

定理 3.7.1 (凯莱定理) 任何群都同构于某个集合上的变换群 (即全变换群的子群). 换言之, 任何群都能嵌入到某个集合的全变换群中. 特别地, 任何有限群必同构于某个置换群的子群.

注 3.7.1 上述结论表明, 我们研究群和研究群作用是等效的. 特别是有限群, 它们都能看成置换群的子群, 从而可以用置换群作用来描述. 这两种观点各有千秋, 在不同的研究中起着不同的作用. 在伽罗瓦创建他的理论时, 群的公理化概念还没有清晰地形成. 实际上, 当时他对群的理解相当于置换群作用的概念–称为图表, 即把元素写成置换形式. ■

例 3.7.7 (右平移) 设 G 是群, $X = G$. 对任意 $g \in G$, 我们定义

$$g(x) = xg^{-1}, \quad \forall x \in X,$$

即将 g^{-1} 右乘到每个元素上. 这是一个群作用, 我们称之为右平移 (Right translation).

请注意, 如果定义 $g(x) = xg$, 那么这一般不是群作用, 因为它不满足群作用的条件 (2). ■

例 3.7.8 (共轭变换) 设 G 是群, $X = G$. 我们定义另一种和平移完全不同的群作用 (请读者自己验证)

$$g(x) = gxg^{-1}, \quad \forall g \in G, \quad \forall x \in X.$$

由命题 3.7.1, 它给了群同态

$$\psi : G \to S(X),$$

其核 $\operatorname{Ker}\psi = C(G)$ (请读者自己验证). ■

例 3.7.9 (齐性空间) 设 $H < G$, X 是 H 的全体左陪集构成的集合. 我们定义群作用

$$g(xH) = (gx)H, \quad g \in G, xH \in X.$$

它诱导的同态 $\psi : G \to S(X)$ 之核为 $\operatorname{Ker}\psi = \cap_{x\in G}\, xHx^{-1}$. X 通常称为齐性空间. 若 H 是正规子群, X 就是商群 G/H, $\operatorname{Ker}\psi = H$. 有时为书写方便, 我们仍将齐性空间记作 G/H.

类似地, 设 X' 是右陪集构成的集合. 我们也有群作用

$$g(Hx) := H(xg^{-1}).$$

请读者自己验证. ■

例 3.7.10 (稳定子集) 设 G 作用在 X 上, Y 是 X 的子集. 如果 Y 满足以下条件, 就称为在 G 作用下稳定:

$$gY := \{gy | y \in Y\} \subseteq Y.$$

G 在 X 上的作用可以限制到 Y 上.

比如 G 在自身的共轭变换可限制到正规子群上, 因为正规子群是共轭变换下的稳定子集. ■

例 3.7.11 (如实作用) 设 G 在 X 有作用. 如果诱导同态 $\psi : G \to S(X)$ 是单同态, 我们就说该作用是*如实的* (Effective). 比如

(1) 左平移和右平移都是如实的.

(2) 一般 (特殊, 正交, 特殊正交) 线性变换是忠实的.

(3) 共轭变换如实当且仅当群的中心是平凡的.

(4) 齐性空间上的作用如实当且仅当 H 不包含 G 的任何非平凡正规子群 (例 3.7.9).

(5) 有限集合上的置换群作用是忠实的. ■

定义 3.7.2 *设 G 分别作用在两个集合 X, X' 上. 如果存在一一对应 $\varphi : X \to X'$, 满足交换图*

$$\begin{array}{ccccc} (g,x) & & G\times X & \xrightarrow{id\times\varphi} & G\times X' & & (g,x') \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ gx & & X & \xrightarrow{\varphi} & X' & & gx' \end{array}$$

亦即

$$\varphi(g(x)) = g(\varphi(x)), \quad \forall g \in G, \quad \forall x \in X, \tag{3-3}$$

我们就称这两个群作用是等价的.

从抽象的角度看, 两个等价的群作用可以视作是等效的, 因而不必再区分它们.

例 3.7.12 左平移和右平移等价. 事实上, 我们可以定义一一映射

$$\varphi : G \longrightarrow G, \quad x \to x^{-1}.$$

容易验证, 它满足式 (3-3). 类似地, 我们也可以说明左陪集的齐性空间作用和右陪集齐性空间的作用等价. ■

例 3.7.13 (有限群表示) 设 G 是有限群, $X = V$ 是复数域 $\mathbb{C}$ 上的 n 维向量空间, $GL(V)$ 是对应的一般线性群. 设 $\psi : G \to GL(V)$ 是群同态. 我们把 ψ 称为 G 在 V 内的*一个线性表示* (Representation). 从群作用角度看, 相当于 G 给出了在 V 上的一个作用.

有限群的线性表示是数学中非常重要的研究对象. 群的表示理论包含了异常丰富且深刻的内容. 它将结构复杂的群投射到我们比较熟悉的一般线性群上, 从而可以利用后者较为成熟的技巧和工具来研究群的特性. 比如, 我们可以利用矩阵的迹的概念来刻画群, 即定义

$$\chi_\psi(g) = \mathrm{tr}(\psi(g)), \quad g \in G.$$

它称为表示 ψ *的特征标* (Character). 有限群的特征标理论包含了许多有趣的结论. 它可以追溯到高斯关于特征和的研究. 有兴趣的读者可以参看塞尔的《有限群的线性表示》. ■

3.7.2 轨道

设群 G 作用在集合 X 上. 利用群作用, 我们可以定义 X 上的等价关系.

$$x \sim_G y \Longleftrightarrow y = gx, \text{对某个 } g \in G \text{ 成立.}$$

我们验证它是等价关系:

(1) 自反性: $x = ex$.

(2) 对称性: 设 $y = gx$, 则 $x = (g^{-1}g)x = g^{-1}(gx) = g^{-1}y$.

(3) 传递性: 设 $y = gx$, $z = g'y$, 则 $z = g'(gx) = (g'g)x$.

X 在上述等价关系下的等价类叫做G-轨道或简称轨道 (Orbit). 包含 $x \in X$ 的轨道就是

$$Gx = \{gx | g \in G\},$$

也称作 x 的 G-轨道. 根据等价类的性质, 我们有

$$X = \bigcup_{x \in X} Gx,$$

此处 x 跑遍不同的等价类. 显然, 每个轨道都是稳定子集.

例 3.7.14 有些教材上, 也将 x 所在轨道记作 O_x. ■

定义 3.7.3 设 G 作用在 X 上.

(1) 设 $x \in X$, 若 $Gx = \{x\}$, 则称 x 是不动元素.

(2) 若存在 $y \in X$, 使得 $X = Gy$, 则称 G 的作用是传递的 (Act transitively). 换言之, 传递作用相当于仅有一个轨道的作用.

例 3.7.15 (**陪集**) 考虑群 G 在自身的左平移. 它是传递作用. 设 $H < G$, 我们有诱导的群作用. 对任何 $x \in G$, x 在 H 的左平移作用下的轨道就是右陪集 Hx.

类似地, x 在 H 的右平移作用下的轨道就是左陪集 xH. ■

例 3.7.16 (**双陪集**) 设 H, K 是 G 的子群, X 是 K 的左陪集全体. G 在齐性空间 X 上的作用可以限制到 H 上. 此时, 对任何 $xK \in X$, 它在 H 作用下的轨道是 HxK, 称为双陪集. ■

例 3.7.17 (**共轭类**) 考虑群 G 在自身的共轭变换. $x \in G$ 的轨道

$$Gx = \{gxg^{-1} | g \in G\}$$

称作 x 的共轭类. x 是不动元素当且仅当 $x \in C(G)$. 比如取 $G = S_n$, $x = (12)$, 则轨道 Gx 就是所有对换构成的集合. ■

例 3.7.18 设 $T \subseteq X$ 是 G 作用下的稳定子集, 则 $T = \cup_{x \in T} Gx$. ■

例 3.7.19 设 $G = GL_n(F)$, $X = V$ 是域 F 上的 n 维向量空间. $G0 = \{0\}$ 是一个轨道, 即 0 是不动元素. 对任何非零元 $x, y \in X$, 显然存在可逆线性变换, 使得 x 变成 y. 因此 X 是两个轨道的并 $X = \{0\} \cup (X \setminus \{0\})$. ■

命题 3.7.2 (稳定子群) 设群 G 作用在集合 X 上, $x \in X$. 那么

(1)

$$\operatorname{Stab} x := \{g \in G | gx = x\}$$

是 G 的子群, 称为元素 x 的稳定子群 (Stabilizer).

(2) 如果 $y = gx$, $g \in G$, 那么 $\operatorname{Stab} y = g \cdot \operatorname{Stab} x \cdot g^{-1}$.

证明 (1) 设 $g, g' \in \operatorname{Stab} x$, 则

$$(g^{-1}g')(x) = g^{-1}(x) = g^{-1}(gx) = (g^{-1}g)x = ex = x.$$

因此 $\operatorname{Stab} x < G$.

(2) 设 $y = gx$, $a \in \operatorname{Stab} x$, 则

$$(gag^{-1})y = (ga)(g^{-1}y) = (ga)(x) = g(ax) = gx = y.$$

因此 $gag^{-1} \in \operatorname{Stab} y$, 这推出 $g \cdot \operatorname{stab} x \cdot g^{-1} \subseteq \operatorname{Stab} y$. 同理可证另一方向的包含关系. ■

例 3.7.20 考虑 G 在自身的共轭作用. 设 $x \in G$, 则 $\operatorname{Stab} x = C(x)$, 即 x 的中心化子. ■

定理 3.7.2 设群 G 作用在集合 X 上, $H_x = \operatorname{Stab} x$, 则

(1) 存在一一对应

$$\varphi : G/H_x \longrightarrow Gx, \quad gH_x \to Gx.$$

(2) G 在 Gx 上的作用与 G 在齐性空间 G/H_x 上的作用等价, 它由 φ 给出.

证明 (1) 注意

$$gH_x = g'H_x \Longleftrightarrow g^{-1}g' \in H_x \Longleftrightarrow (g^{-1}g')x = x \Longleftrightarrow g'x = gx.$$

这就推出合理性和单射性. 满射性则是显然的.

(2) 对任何左陪集 aH 及 $g \in G$, 我们有

$$\varphi(g(aH)) = \varphi(gaH) = (ga)x = g(ax) = g\varphi(aH).$$

这就推出两个作用等价. ■

推论 3.7.2 设 G 是有限群, G 作用在 X 上, 则

$$|Gx| = [G : \operatorname{Stab} x].$$

特别地, 轨道 Gx 的元素个数必是 $|G|$ 的因子.

推论 3.7.3 设 G 是有限群, 则

$$|G| = |C(G)| + \sum_{Gx} [G : C(x)],$$

这里 Gx 不重复地跑遍所有不含中心元素的共轭类.

证明 考虑 G 在自身的共轭作用. 由前面讨论, 对任何 $x \in G$, x 的共轭类中元素个数$|Gx| = [G : C(x)]$. $x \in C(G)$ 当且仅当 $Gx = \{x\}$, 即仅含一个元素. 再由

$$G = C(G) \cup \left(\bigcup_{x \in G \setminus C(G)} Gx \right)$$

即得结论. ■

3.7.3 补充材料: 西罗定理

如果一个有限群 G 的阶数是素数 p 的方幂, 我们就称之为 p-群. 利用群作用的技巧, 我们可以得到许多关于 p-群的漂亮结论. 限于篇幅, 我们只作简单的介绍.

定理 3.7.3 设 G 是 p-群, 作用在有限集合 X 上, $|X| = n$. 设 t 是 X 中不动元素的个数. 那么

$$t \equiv n \pmod{p}.$$

特别地, 若 $\gcd(n, p) = 1$, 则 X 必有不动元素.

如果考虑群的共轭作用, 我们有如下经典推论.

推论 3.7.4 p-群必有非平凡中心.

定理 3.7.4 (西罗第一定理) 设 G 是 n 阶有限群, p 是素数, $p^k \mid n$, $k \geq 0$, 则 G 必含阶为 p^k 的子群.

设 $|G| = p^\ell \cdot m$, $\gcd(p.m) = 1$, 由西罗第一定理, 存在 p^ℓ 阶子群, 我们称之为 G 的西罗 p-子群(Sylow p-subgroup).

定理 3.7.5 (西罗第二定理) 设 G 是 $p^\ell \cdot m$ 阶有限群, p 是素数, $\gcd(p, m) = 1$, 则

(1) G 的任何两个西罗 p-子群彼此共轭.

(2) 设 k 是西罗 p-子群的个数, 则 $k \mid m$ 且 $k \equiv 1 \pmod{p}$.

(3) 任何 p^k 阶子群必含于某个西罗 p-子群中.

本章习题

加 $*$ 号的习题表示有一定难度.

习题 3.1 设 G 是单群, 证明: 要么 G 是素数阶循环群, 要么 $G = [G, G]$.

习题 3.2 设 $G = \langle a \rangle$ 是 n 阶循环群. 证明: $\mathrm{Aut}G \cong \mathbb{Z}_n^*$.

第二部分

提高篇

第四章　域扩张

4.1　基本概念

我们先回顾一些概念. 设 F, E 是两个域. 如果 $F \subseteq E$, 那么就称 E 是 F 上的扩域 (也叫做 F 上的域扩张), 记作 E/F. F 是 E 的子域 (也称为 E 的基域). 如果一个域 K 满足

$$F \subseteq K \subseteq E,$$

我们就说 K 是 E/F 的中间域.

注 4.1.1　请读者注意, 切勿将 E/F 与商环的记号混淆. ■

例 4.1.1　(1) 任何 F 都可以选定它的素域

$$P = \{(n1)(m1)^{-1} | m1 \neq 0\}$$

作为一个基域, 这就有 P 的域扩张 F/P. 回顾一下, 当 $\mathrm{char}F = 0$ 时, $P \cong \mathbb{Q}$; 当 $\mathrm{char}F = p$ (p 是素数) 时, $P \cong \mathbb{F}_p$ 是模 p 的剩余类域.

(2) 考虑域扩张 $\mathbb{C}/\mathbb{Q}$, 我们有中间域 $\mathbb{R}$, 还有中间域

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}.$$

更一般的, 对任意代数数 θ, $\mathbb{Q}(\theta)$ 是 $\mathbb{C}/\mathbb{Q}$ 的中间域.

(3) 设 F 是域, $F(x)$ 是 F 上的有理函数域. 因而我们有 F 上的域扩张 $F(x)/F$. ■

例 4.1.2　考虑域扩张 E/F. 设 $S \subseteq E$ 是非空子集.

(1) 考虑由 $F \cup S$ 生成的子域 $F(S)$, 即 E 中包含 F 和 S 的所有子域的交. 它是 E/F 的中间域, 称作 F 上添加 S 得到的子域, 或叫做 S 在 F 上生成的子域.

(2) 设 $S = \{\alpha_1, \cdots, \alpha_n\} \subseteq E$ 是有限集, 我们也将 $F(S)$ 改记为 $F(\alpha_1, \cdots, \alpha_n)$, 它是环 $F[\alpha_1, \cdots, \alpha_n]$ 的分式域. 回顾命题 2.3.7, $F[\alpha_1, \cdots, \alpha_n]$ 实际上是如下环同态的像.

$$\sigma : F[x_1, \cdots, x_n] \longrightarrow E, \quad f(x_1, \cdots, x_n) \to f(\alpha_1, \cdots, \alpha_n).$$

(3) 设域扩张 E/F 是由 F 上添加一个元 α 得到, 即 $E = F(\alpha)$, 则称 E 是 F 的单扩张 (Simple extension). 比如 $\mathbb{Q}(\sqrt{d})$ 是 $\mathbb{Q}$ 的单扩张. ■

对任何域扩张 E/F, E 可以看成域 F 上的线性空间 (未必是有限维的). 我们把该线性空间的维数记作 $[E : F]$, 称为扩张 E/F 的次数. 若 $[E : F] < \infty$, 则称 E/F 是有限扩张; 否则称为无限扩张. 对有限扩张 E/F, E 作为 F 上的线性空间的一组基也称做扩张 E/F 的基.

设 E/F 是域扩张, $\alpha \in E$. 如果存在多项式 $f(x) \in F[x]$, 满足 $f(\alpha) = 0$, 我们就称 α 在 F 上是代数的 (Algebraic); 否则就称之为超越的 (Transcendental). 如果 E 中每个元都是 F 上的代数元, 就称 E/F 是代数扩张 (Algebraic extension).

例 4.1.3　扩张 $\mathbb{C}/\mathbb{Q}$ 中的代数元就是我们在例 1.3.3 中定义的代数数. ■

4.2 各种类型的域扩张

4.2.1 单扩张

命题 4.2.1 设 E/F 是域扩张, $\alpha \in E$, 则

(1) α 是 F 上的代数元, 则

$$F[\alpha] = F(\alpha) \cong F[x]/(h(x)),$$

这里 $h(x) \in F[x]$ 是 α 的极小多项式. 进一步, 如果 $g(x) \in F[x]$ 也满足 $g(\alpha) = 0$, 则 $h(x) \mid g(x)$. $F(\alpha)/F$ 称为单代数扩张.

(2) 若 α 在 F 上是超越的, 则 $F[\alpha] \cong F[x]$, 因而 $F(\alpha) \cong F(x)$. 此时 $F(\alpha)/F$ 称为单超越扩张.

证明 由命题 2.3.7, 我们有满同态

$$\sigma : F[x] \longrightarrow F[\alpha], \quad f(x) \to f(\alpha).$$

它的核 $\operatorname{Ker}\sigma = (h(x))$. 由同态基本定理, $F[x]/(h(x)) \cong F[\alpha]$.

(1) 如果 α 在 F 上是代数的, 则 $h(x)$ 是非零不可约多项式. 因此 $F[\alpha] \cong F[x]/(h(x))$ 是域, 故 $F(\alpha) = F[\alpha]$. 如果 $g \in F[x]$ 满足 $g(\alpha) = 0$, 则 $g \in (h(x))$, 即 $h(x) \mid g(x)$.

(2) 如果 α 是超越的, 则 $h(x) = 0$, 故 $F[x] \cong F[\alpha]$. ■

设 $\alpha \in E$ 是 F 上的代数元, $h(x) \in F[x]$ 是 α 的极小多项式, 我们称 $\deg h$ 为 α 的次数.

命题 4.2.2 (**根的存在性**) 设 F 是域, $f(x) \in F[x]$ 是不可约多项式, 则存在单代数扩张 E/F, 使得 $f(x)$ 在 E 内有根.

证明 设 $E = F[x]/(f(x))$. 由于 $f(x)$ 不可约, 所以 E 是域. 我们有单同态

$$F \hookrightarrow E = F[x]/(f(x)), \quad a \to [a].$$

因此 F 可以看成 E 的子域.

设 $\alpha = [x] \in E$, 则 $E = F[\alpha]$,

$$f(\alpha) = [f(x)] = [0] \in E.$$

这就完成了证明. ■

注 4.2.1 取 $F = \mathbb{C}$, $f(x) \in \mathbb{C}[x]$. 命题 4.2.2 表面看似乎给出了高斯代数学基本定理, 实则不然. 因为这一命题并不保证其所给的扩域 E 就是 $\mathbb{C}$. ■

例 4.2.1 设 p 是模 4 余 3 的素数. 由例 2.3.37, 有限域 $E := \mathbb{F}_p[x]/(x^2+1)$ 是 $\mathbb{F}_p$ 的单扩张. 具体言之, $E = F[\alpha]$, 这里 $\alpha = [x]$ 满足 $\alpha^2 + [1] = 0$. ■

命题 4.2.3 设 E/F 是域扩张, $\alpha \in E$, 则以下条件彼此等价:

(1) $F(\alpha)/F$ 是代数扩张,

(2) α 在 F 上是代数的.

(3) $F(\alpha)/F$ 是有限扩张.

条件成立时, $[F(\alpha):F]$ 等于 α 的次数.

证明 (1) $\Longrightarrow$ (2) 显然.

(2) $\Longrightarrow$ (3) 设 α 是 F 上的 n 次代数元, 其极小多项式为 $h(x)\in F[x]$. 对任何多项式 $f(x)\in F[x]$, 由带余数除法,

$$f(x)=h(x)q(x)+r(x),\quad \deg r<\deg h.$$

因而 $f(\alpha)=r(\alpha)$. 这表明, $F[\alpha]=F(\alpha)$ 中的元素都可以表为

$$c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1},\quad c_i\in F.$$

另一方面, 由于极小多项式是 n 次的, 所以 $1,\alpha,\cdots,\alpha^{n-1}$ 在域 F 上线性无关. 这就推出 $1,\alpha,\cdots,\alpha^{n-1}$ 是 E/F 的基. 特别地, $[F(\alpha):F]=n$.

(3) $\Longrightarrow$ (1) 设 $[F(\alpha):F]=n$. 对任何 $\beta\in F(\alpha)$, 因为 $1,\beta,\cdots,\beta^n$ 在 F 上线性相关, 即

$$c_0+c_1\beta+\cdots+c_n\beta^n=0,\quad c_i\in F,$$

且 c_i 不全为零. 这就推出 β 在 F 上是代数的. ■

例 4.2.2 设 θ 是 n 次代数数, 则 $[\mathbb{Q}(\theta):\mathbb{Q}]=n$. 特别地, $[\mathbb{Q}(\sqrt{d}):\mathbb{Q}]=2$. ■

4.2.2 有限扩张

定理 4.2.1 (望远镜定理) 设 E/F 是域扩张, K 是中间域, 则 E/F 是有限扩张当且仅当 E/K 和 K/F 都是有限扩张. 当条件成立时, 我们有

$$[E:F]=[E:K]\cdot[K:F].$$

证明 ($\Longrightarrow$) 已知 $n:=[E:F]<\infty$, 即 E 是域 F 上的有限维线性空间. 因而 K 是 E 的子空间, 故 $[K:F]\le[E:F]<\infty$. 设 $\alpha_1,\cdots,\alpha_n$ 是线性空间 E 在域 F 上的基. 如果将 E 看成域 K 上的线性空间, 那么显然 $\alpha_1,\cdots,\alpha_n$ 在域 K 上生成 E, 故 $[E:K]\le[E:F]<\infty$.

($\Longleftarrow$) 已知 $m:=[E:K]<\infty$, $r:=[K:F]<\infty$, 并设 $\beta_1,\cdots,\beta_m$ 是 E/K 的基, $\gamma_1,\cdots,\gamma_r$ 是 K/F 的基.

对任何 $\alpha\in E$, 存在 $a_i\in K$ $(i=1,\cdots,m)$ 满足

$$\alpha=\sum_{i=1}^{m}a_i\beta_i.$$

对每个 $a_i\in E$, 我们有

$$a_i=\sum_{j=1}^{r}b_{ij}\gamma_j,\quad b_{ij}\in F.$$

因此

$$\alpha=\sum_{i,j}b_{ij}\beta_i\gamma_j,\quad b_{ij}\in F.$$

这表明诸 $\beta_i\gamma_j$ 在域 F 上线性生成 E. 因此

$$[E:F] \leq mr = [E:K]\cdot[K:F] < \infty.$$

现在证明诸 $\beta_i\gamma_j$ 线性无关. 设

$$\sum_{i,j} b_{ij}\beta_i\gamma_j = 0, \quad b_{ij} \in F.$$

令

$$a_i = \sum_{j=1}^{r} b_{ij}\gamma_j \in E, \quad i = 1, \cdots, m.$$

故有 $\sum\limits_{i=1}^{m} a_i\beta_i = 0$. 由于 β_i 是 E/K 的基, 所以 $a_i = 0$ $(i = 1, \cdots, m)$. 又因为 γ_j 是 K/F 的基, 所以 $b_{ij} = 0$. 这就推出所有 $\beta_i\gamma_j$ 在域 F 上线性无关. 因此它们是一组基, 从而迫使 $n = mr$. ■

注 4.2.2 用通俗的话来讲, 望远镜定理可以断言: 有限扩张的有限扩张仍是有限的. ■

推论 4.2.1 *设 E/F 是有限扩张, $\alpha \in E$, 那么 α 在 F 上必是代数的, 且其次数是 $[E:F]$ 的因子. 特别地, E/F 是代数扩张.*

证明 取中间域 $K = F(\alpha)$. 由望远镜定理, $[K:F]$ 是 $[E:F]$ 的因子, 故 K/F 是有限扩张. 再由命题 4.2.3 知 α 在 F 上是代数的. ■

推论 4.2.2 (**单代数扩张升链**) *设 E/F 是域扩张. 以下条件彼此等价:*

(1) *E/F 是有限扩张,*

(2) *存在中间域的有限升链*

$$F = F_0 \subset F_1 \subset \cdots \subset F_r = E,$$

使得 F_{i+1}/F_i 是单代数扩张.

证明 ($\Longrightarrow$) 对次数 $n := [E:F]$ 施归纳法. $n = 1$ 时, 显然有 $E = F$. 今假设 $< n$ 的情形已证. 任取 $\alpha_1 \in E$, 但要求 $\alpha_1 \notin F$. 设 $F_1 = F(\alpha_1)$. 因此 $F_1(\alpha_1)/F$ 是单代数扩张且 $[F_1:F] > 1$. 这样, 由望远镜定理知 $[E:F_1] < n = [E:F]$. 由归纳假设, E/F_1 有单代数扩张升链 $F_1 \subset F_2 \subset \cdots \subset F_r = E$, 故得 E/F 的单代数扩张升链

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r = E.$$

($\Longleftarrow$) 因为每个扩张 F_{i+1}/F_i 都是有限扩张, 故由望远镜定理立得结论. ■

4.2.3 代数扩张

前面已经给出了如下概念的包含关系

$$\text{单代数扩张} \subseteq \text{有限扩张} \subseteq \text{代数扩张}.$$

一般来说, 有限扩张不是单代数扩张. 但是加上某些条件后, 这两类扩张可以相同. 我们后面再解释这一点. 类似地, 代数扩张也未必是有限扩张 (见下面的例子 4.2.3).

我们证明如下重要结论.

定理 4.2.2　设 K 是域扩张 E/F 的中间域. 如果 E/K 和 K/F 都是代数扩张, 那么 E/F 必是代数扩张.

证明　设 $\alpha \in E$. 由推论 4.2.1, 我们只需要找到 E/F 的一个中间域 L, 使得 $\alpha \in L$, 并且 L/F 是有限扩张即可 (因为这蕴含着 α 是 F 上的代数元). 再由推论 4.2.2, 我们的目标可以转为构造单代数扩张升链

$$F = F_0 \subset F_1 \subset \cdots \subset F_r \subset F_{r+1} = L.$$

首先, 因 E/K 是代数扩张, 故 α 是 K 上的代数元, 即存在极小多项式

$$h(x) = x^r + a_1 x^{r-1} + \cdots + a_{r-1}x + a_r \in K[x], \quad a_i \in K,$$

满足 $h(\alpha) = 0$. 今构造中间域

$$F = F_0, \quad F_k = F(a_1, \cdots, a_k), \quad L = F_r(\alpha), \quad k = 1, \cdots, r.$$

显然有

$$F_0 \subset F_1 \subset \cdots \subset F_r \subset L. \tag{4-1}$$

注意到 K/F 是代数扩张, 因而诸 a_i 皆 F 上的代数元, 因而 $a_i \in F_i$ 也是 F_{i-1} 的代数元, 即 F_i/F_{i-1} 是单代数扩张. 此外, 由 α 的极小多项式选取, L/F_r 显然也是单代数扩张. 因而升链 (4-1) 是单代数扩张升链. ■

推论 4.2.3 (**代数闭包**)　设 E/F 是域扩张. K 是 F 上所有代数元全体构成的集合, 则 K 是 E/F 的中间域, 称为 F 在 E 中的代数闭包 (Algebraic closure).

证明　任取 $\alpha, \beta \in K$. 此时有单代数扩张升链

$$F \subset F(\alpha) \subset F(\alpha, \beta).$$

由定理 4.2.2, $F(\alpha, \beta)/F$ 仍是代数扩张. 特别地,

$$\alpha \pm \beta,\ \alpha \cdot \beta,\ \frac{\alpha}{\beta} \in F(\alpha, \beta)$$

都是 F 上的代数元, 因而都落在 K 中. 这就证明 K 是子域. ■

例 4.2.3 (**代数数域**)　考虑 $\mathbb{Q}$ 在扩张 $\mathbb{C}/\mathbb{Q}$ 中的代数闭包 $\overline{\mathbb{Q}}$. 它称为代数数域 (Algebraic number field). $\overline{Q}$ 中的元素就是代数数.

我们这里来具体验证一对代数数的加法. 比如取 $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$, 则 $\alpha + \beta$ 的极小多项式为 $h(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$.

可以看到 $\overline{\mathbb{Q}}/\mathbb{Q}$ 不可能是有限扩张. 若不然, 由推论 4.2.1, 任何代数数的次数都不超过 $[\overline{\mathbb{Q}} : \mathbb{Q}]$, 这是不可能的. ■

4.2.4　分裂域扩张 (I): 存在性

设 F 是给定的域, $f(x) \in F[x]$ 是给定的 $n(\geq 1)$ 次多项式.

定理 4.2.3 (**分裂域**)　存在有限域扩张 E/F, 满足如下条件:

(1) $f(x)$ 在 E 内完全分解成一次因式乘积

$$f(x) = c(x-\alpha_1)\cdots(x-\alpha_n), \quad \alpha_i \in E, \quad i = 1, \cdots, n.$$

(2) $E = F(\alpha_1, \cdots, \alpha_n)$.

特别地, $[E:F] \leq n!$. E/F 称为 $f(x)$ 在 F 上的分裂域 (Splitting field).

证明 对 $n = \deg f(x)$ 施归纳法. $n = 1$ 时, $f(x) = c(x-a)$, $a \in F$, 即取 $E = F$. 今假设 $< n$ 的情形已证.

首先, 我们构造单代数扩张 K/F, 使得 $f(x)$ 在 K 中至少有一个根. 设 $p(x) \in F[x]$ 是 $f(x)$ 的不可约因式. 类似前面的讨论, $K := F[x]/(p(x))$ 就是我们要找的单代数扩张, $\alpha_1 := [x] \in K$ 满足 $p(\alpha_1) = 0$ (在 K 里). 因此, $f(\alpha_1) = 0$. 这表明, f 在 K 里至少能分解出一个一次因式 $(x-\alpha_1)$.

不妨设

$$f(x) = c(x-\alpha_1)\cdots(x-\alpha_r)f_1(x), \quad \alpha_1, \cdots, \alpha_r \in K, \quad f_1(x) \in K[x], \quad \deg f_1 < n.$$

若 f_1 是常数, 则结论已得证. 因此不妨假设 $f_1(x)$ 非常值的首一多项式. 由归纳假设, 存在 $f_1(x)$ 在 K 上的分裂域 E/K, 即满足

$$f_1(x) = (x-\alpha_{r+1})\cdots(x-\alpha_n),$$

并且 $E = K(\alpha_{r+1}, \cdots, \alpha_n)$.

注意到

$$K = F(\alpha_1) = F(\alpha_1, \cdots, \alpha_r),$$

我们就得到

$$E = F(\alpha_1, \cdots, \alpha_r)(\alpha_{r+1}, \cdots, \alpha_n) = F(\alpha_1, \cdots, \alpha_r, \alpha_{r+1}, \cdots, \alpha_n).$$

此外, 由归纳假设以及望远镜定理立知

$$[E:F] = [K:F]\cdot[E:K] \leq n\cdot(n-1)! = n!.$$

综上可知结论对任何 n 成立. ■

后面我们还要证明这种分裂域在某种同构意义下是唯一的. 下面先举几个分裂域的例子.

例 4.2.4 取 $F = \mathbb{R}$,

(1) $f(x) = x^2 + 1$, 则 f 在 F 上的分裂域 E 就是 $\mathbb{C}$, $[E:F] = 2$.

(2) $f(x) = x^2 + x + 1$, 则 f 的分裂域 $E = \mathbb{R}\left(-\frac{1}{2} + \frac{\sqrt{-3}}{2}\right)$, $[E:F] = 2$. ■

例 4.2.5 设 p 是模 4 余 3 的素数, $F = \mathbb{F}_p$ 是模 p 的剩余类域, $f(x) = x^2 + 1$. 前面已证 $E = F[x]/(x^2+1)$ 是 F 的域扩张. 显然, $E = F(\alpha)$, $f(x) = (x-\alpha)(x+\alpha)$, 这里 $\alpha = [x] \in E$. 因此 E/F 就是 $f(x)$ 在 F 上的分裂域. ■

例 4.2.6　设 $F=\mathbb{Q}$, $f(x)=(x^2-2)(x^2-3)$. $E=\mathbb{Q}(\sqrt{2},\sqrt{3})$ 是 f 在 F 上的分裂域. 设 $K=\mathbb{Q}(\sqrt{2})$ 是其中间域. 显见, K/F 是 x^2-2 在 F 上的分裂域. $F\subseteq K\subseteq E$ 是单代数扩张升链. 由望远镜定理, $[E:F]=4$.

我们来验证, $E=K[x]/(x^2-3)$. 这相当于验证 $x^2-3\in K[x]$ 也是不可约的, 即 $x^2-3=0$ 在 K 中无根. 若不然, 设 $a+b\sqrt{2}$ 是一根, 则

$$0=(a+b\sqrt{2})^2-3,$$

即

$$(a^2+2b^2-3)+2ab\sqrt{2}=0.$$

这迫使 $ab=0$. 无论 $a=0$ 或 $b=0$, 都将导致矛盾!

最后, 我们来证明 $E=\mathbb{Q}(\sqrt{2}+\sqrt{3})$. 由例 4.2.3, $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4$. 又因为 $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subseteq E$, 且 $[E:\mathbb{Q}]=4$. 由望远镜定理, $[E:\mathbb{Q}(\sqrt{2}+\sqrt{3})]=1$, 由此即得结论. ■

例 4.2.7 (p **次单位根**)　设 $F=\mathbb{Q}$, $f(x)=x^p-1$, 这里 p 是素数.

$$E=\mathbb{Q}(\omega)=\mathbb{Q}[x]/(x^{p-1}+\cdots+x+1)$$

是 f 在 F 上的分裂域, 这里 ω 是 p 次单位根. 在 E 中, $f(x)=(x-1)(x-\omega)\cdots(x-\omega^{p-1})$. 请注意, 对素数 p, 多项式 $x^{p-1}+\cdots+x+1\in Q[x]$ 已知是不可约的. 此时 $[E:F]=p-1$. ■

4.2.5　分裂域扩张 (II): 唯一性

下面我们来证明分裂域的唯一性. 为此先做一些准备工作.

命题 4.2.4　设 $\sigma:F\to F'$ 是域同构, 则

(1) σ 可以唯一延拓为多项式环同构

$$\bar{\sigma}:F[x]\longrightarrow F'[y],$$

使得 $\bar{\sigma}(x)=y$. 进一步, 若 $h(x)\in F[x]$ 是不可约多项式, 则

$$h^\sigma(y):=\bar{\sigma}(h(x))\in F'[y]$$

也是不可约多项式.

(2) 设 α (相应地, β) 是不可约多项式 $h(x)\in F[x]$ (相应地, $h^\sigma(y)\in F'[y]$) 的根, 则 σ 可以唯一延拓为域同构 $\sigma':F(\alpha)\to F'(\beta)$, 使得 $\sigma'(\alpha)=\beta$.

证明　(1) 任取

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x].$$

我们定义

$$f^\sigma(y):=\sigma(a_n)y^n+\sigma_{n-1}(a_{n-1})y^{n-1}+\cdots+\sigma(a_1)y+\sigma(a_0)\in F'[y].$$

容易验证,

$$\bar{\sigma}:F[x]\to F'[y],\quad f(x)\to f^\sigma(y),$$

给出了环同构, 并且 $\bar{\sigma}_{|}F=\sigma$. 这一延拓的唯一性显然由 $\bar{\sigma}(x)=y$ 唯一确定.

(2) 利用上述延拓的多项式环同构,即得如下环同构

$$\sigma' : F[x]/(h(x)) \longrightarrow F'(y)/(h^\sigma(y)),$$

即 $\sigma' : F(\alpha) \to F'(\beta)$, 满足 $\sigma'(\alpha) = \beta$. ■

定义 4.2.1 设 E_1/F 和 E_2/F 都是 F 的域扩张, $\sigma : E_1 \to E_2$ 是域同态, 使得限制映射 $\sigma|_F$ 是 F 到自身的恒同映射, 则 σ 叫做 F-同态. 进一步, 若 σ 是同构, 则称之为 F-同构.

E/F 的全部 F-自同构组成一个群, 称为 E/F 的伽罗华群, 记作 $\mathrm{Gal}(E/F)$. 它在伽罗华理论中扮演了重要的角色. 我们将在后面详细介绍它.

推论 4.2.4 设 $\sigma : E_1/F \to E_2/F$ 是 F-同构, $\alpha \in E_1$, 那么

(1) α 在 F 上代数当且仅当 $\sigma(\alpha)$ 在 F 上代数, 并且它们有相同的极小多项式.

(2) 如果 $\alpha, \beta \in E_1$ 都是某个不可约多项式 $h(x) \in F[x]$ 的根, 则存在单代数扩张 $F(\alpha)$ 和 $F(\beta)$ 之间的 F-同构 $\eta : F(\alpha) \to F(\beta)$, 使得 $\eta(\alpha) = \beta$.

证明 (1) 设 α 是代数的, 极小多项式为

$$h(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x].$$

注意到 $\sigma|_F$ 是恒同映射, 所以

$$\begin{aligned} h(\sigma(\alpha)) &= \sigma(\alpha)^n + a_{n-1} \cdot \sigma(\alpha)^{n-1} + \cdots + a_1 \cdot \sigma(\alpha) + a_0 \\ &= \sigma(\alpha)^n + \sigma(a_{n-1}) \cdot \sigma(\alpha)^{n-1} + \cdots + \sigma(a_1) \cdot \sigma(\alpha) + \sigma(a_0) \\ &= \sigma(h(\alpha)) \\ &= 0. \end{aligned}$$

因此 $\sigma(\alpha)$ 也是 $h(x)$ 的根, 从而是代数的. 设 $h^\sigma(x) \in F[x]$ 是 $\sigma(\alpha)$ 的极小多项式, 这就推出 $h^\sigma \mid h$. 将同样的讨论应用到 σ^{-1} 上可知, $\sigma(\alpha)$ 若是代数元, 则 α 亦然, 并且 $h \mid h^\sigma$, 从而 $h = h^\sigma$.

(2) 将命题 4.2.4 应用到恒同映射 $\sigma|_F : F \to F$ 上即得. ■

定理 4.2.4 (**分裂域同构定理**) 设 $\sigma : F \to F'$ 是域同构, $f(x) \in F[x]$ 是正次数多项式, $f^\sigma(y) \in F'[y]$ 是相应的多项式 (定义见命题 4.2.4). 设 E (相应地, E') 是 f (相应地, f^σ) 在 F (相应地, F') 上的分裂域, 则 σ 可以延拓成域同构 $\bar{\sigma} : E \to E'$.

特别地, $f(x)$ 在 F 上的分裂域 E 在 F-同构意义上是唯一的.

证明 我们对 $[E : F]$ 施归纳法. 当 $[E : F] = 1$ 时, 即 $E = F$, 我们有

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_r), \quad \alpha_i \in F, \quad i = 1, \cdots, r.$$

于是

$$f^\sigma(y) = \sigma(c)(y - \sigma(\alpha_1)) \cdots (y - \sigma(\alpha_r)).$$

这表明 $E' = F'(\sigma(\alpha_1), \cdots, \sigma(\alpha_r)) = F'$. 因此结论显然成立.

今假设 $[E:F]<n$ 的情形已证. 当 $[E:F]=n$ 时, 我们取 $f(x)$ 的一个不可约因式 $h(x)$. 由命题 4.2.4 (1), $h^\sigma(y)$ 也是 $f^\sigma(y)$ 的不可约因式. 设 $\alpha\in E$ (相应地, $\beta\in E'$) 是 $h(x)$ (相应地, $h^\sigma(y)$) 的一个根. 由命题 4.2.4 (2), 存在域同构

$$\sigma':F(\alpha)\longrightarrow F'(\beta),\quad \alpha\to\beta.$$

注意到 $E/F(\alpha)$ (相应地, $E'/F'(\beta)$) 仍是 $f(x)$ (相应地, $f^\sigma(x)$) 的分裂域. 另一方面, $[E:F(\alpha)]<n$, 故由归纳假设, σ' 可以进一步延拓为域同构 $\sigma'':E\to E'$. 综上可知结论成立.

今取 $\sigma:F\to F$ 为恒同映射. 此时, $f=f^\sigma$, 因此分裂域在 F-同构下唯一. ■

注 4.2.3　分裂域的 F-同构一般不是唯一的. 利用上述定理的归纳讨论, 我们还可以证明这种同构的个数 $k\le[E:F]$. 特别地, 若 $f(x)$ 在 E 中的根互不相同, 那么 $k=[E:F]$. ■

推论 4.2.5　*设域扩张 L/F 包含中间域 E/F, 它是多项式 $f(x)\in F[x]$ 的分裂域, 那么*

(1) *若 E'/F 是另一中间域, 并且它也是 $f(x)\in F[x]$ 的分裂域, 则 $E'=E$.*

(2) *设 $\sigma\in\mathrm{Gal}(L/F)$, 则 $\sigma(E)=E$.*

证明　(1) 设 $f(x)\in F[x]$ 在 E,E' 中分别分解为

$$f(x)=c(x-\alpha_1)\cdots(x-\alpha_n)\in E,$$
$$f(x)=c'(x-\alpha_1')\cdots(x-\alpha_n')\in E',$$

由于它们也都是 $f(x)$ 在 L 中的分解, 所以根据 $L[x]$ 中多项式的唯一分解性可知, $\{\alpha_i\}_{1\le i\le n}$ 和 $\{\alpha_i'\}_{1\le i\le n}$ 只相差一个置换. 因而 $E=E'$.

(2) $\sigma(E)$ 是 f^σ 的分裂域, 而 $f^\sigma=f$ (因为 σ 是 F-自同构). 由 (1) 立知 $\sigma(E)=E$. ■

例 4.2.8　回顾例 4.2.7, $F=\mathbb{Q}$, $f(x)=x^p-1$ (p 是素数) 在 F 上的分裂域是 $E=\mathbb{Q}(\omega)$, 这里 ω 是 p 次单位根. 设 $\sigma\in\mathrm{Gal}(E/F)$. 容易看到, σ 由 $\sigma(\omega)$ 的取值唯一确定. 因为

$$(\sigma(\omega))^p=\sigma(\omega^p)=\sigma(1)=1,$$

所以 $\sigma(\omega)=\omega^k$, $k=1,\cdots,p-1$. 因此 $\mathrm{Gal}(E/F)$ 恰有 $[E:F]=p-1$ 个元. 更精确地说, $\mathrm{Gal}(E/F)\cong\mathbb{F}_p^*$. ■

例 4.2.9　设 $F=\mathbb{Q}$, $f(x)=x^p-2$ (p 是奇素数) 在 F 上的分裂域是 $E=\mathbb{Q}(\omega,\sqrt[p]{2})$, 这里 ω 是 p 次单位根, $\sqrt[p]{2}$ 是 $x^p-2=0$ 的正实根. 考虑中间域 $K=Q(\sqrt[p]{2})\cong\mathbb{Q}[x]/(f)$. $E=K(\omega\sqrt[p]{2})$ 也是 K 的单代数扩张. 因此我们有单代数扩张升链 $F\subseteq K\subseteq E$. 由望远镜定理可知 $[E:F]=[E:K]\cdot[K:F]=p(p-1)$.

可以验证, $\mathrm{Gal}(E/F)$ 中的 F-自同构恰好是以下类型: $\sigma_{ij}:E\to E$, 满足

$$\sigma_{ij}(\omega)=\omega^i,\quad \sigma_{ij}(\sqrt[p]{2})=\omega^j\cdot\sqrt[p]{2},\quad i=1,\cdots,p-1,\quad j=0,1,\cdots,p-1.$$

因此 $\mathrm{Gal}(E/F)$ 的元素个数是 $[E:F]=p(p-1)$. ■

4.2.6 正规扩张

定义 4.2.2 设 E/F 是代数扩张, 如果 E/F 满足如下性质, 我们就称它是正规扩张 (Normal extension): 设 $p(x) \in F[x]$ 是不可约多项式, 若它在 E 内至少有一个根, 则它在 E 内可以完全分解成一次因式的乘积.

我们要证如下主要结论.

定理 4.2.5 设 E/F 是域扩张, 则以下条件彼此等价:

(1) E/F 是有限正规扩张,

(2) E 是某多项式 $f(x) \in F[x]$ 的分裂域扩张.

证明 ($\Longrightarrow$) 已知 E/F 是有限正规的. 由有限性即知

$$E = F(\alpha_1, \cdots, \alpha_r),$$

这里 $\alpha_1, \cdots, \alpha_n$ 是 F 上的代数元. 设 $f_i(x) \in F[x]$ 是 α_i 的极小多项式, 并令

$$f(x) := f_1(x) \cdots f_r(x).$$

由于 E/F 是正规的, 所以每个 $f_i(x)$ 可以在 E 内分解为一次因式乘积, 故 $f(x)$ 亦然, 即

$$f(x) = (x - \beta_1) \cdots (x - \beta_n), \quad \beta_i \in E.$$

因此 $F(\beta_1, \cdots, \beta_n) \subseteq E$. 反之, 因为 α_i 是 f 的根, 因而它必是某个 β_j. 这就给出了包含关系 $E \subseteq F(\beta_1, \cdots, \beta_n)$. 因而

$$E = F(\beta_1, \cdots, \beta_n)$$

是 $f(x)$ 的分裂域.

($\Longleftarrow$) 已知 E/F 是 $f(x) \in F[x]$ 的分裂域. 设 $p(x) \in F[x]$ 是不可约多项式, 并且在 E 内有至少一个根 α.

设 L/E 是 $p(x)$ 在 E 上的分裂域. 因此 L/F 是 $g(x) = f(x)p(x)$ 的分裂域. 设 β 是 $p(x)$ 在 L 中的任意根. 由推论 4.2.4 (2), 可构造 F-同构 $\tau : F(\alpha) \to F(\beta)$, 满足 $\tau(\alpha) = \beta$. 再由分裂域同构定理, τ 可以延拓成 L 的 F-自同构 τ'.

由推论 4.2.5 (2), $\tau'(E) = E$. 因而 $\beta = \tau(\alpha) \in E$. 这表明 $p(x)$ 在 E 内完全分解成一次因式. 这就证明了 E/F 是正规的. ■

4.2.7 可分扩张

设 F 是域,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$$

是正次数多项式, E 是 f 的分裂域. 我们写

$$f(x) = c(x - \alpha_1)^{e_1} \cdots (x - \alpha_r)^{e_r}, \quad e_i \geq 1, \quad \alpha_i \neq \alpha_j,\ i > j.$$

α_i 称为 $f(x)$ 的 e_i 重根. 当 $e_i = 1$ 时, α_i 称为单根 (Simple root); 否则称为重根 (Multiple root).

我们定义 f 的形式导数 (Formal derivative)

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1.$$

引理 4.2.1 设 $f, g \in F[x]$, 我们有

(1) $(\alpha f + \beta g)' = \alpha f' + \beta g'$, $\alpha, \beta \in F$,

(2) $(f \cdot g)' = f' \cdot g + f \cdot g'$,

(3) $x' = 1$,

证明 与数域上多项式函数的导数情形类似. ■

引理 4.2.2 设 $x = \alpha$ 是 $f(x)$ 在分裂域 E 内的 k-重根 ($k \geq 1$).

(1) 当特征 $\mathrm{ch}(F) = 0$ 或 $\mathrm{ch}(F) \nmid k$ 时, $x = \alpha$ 是 $f'(x)$ 的 $k-1$ 重根;

(2) 当特征 $\mathrm{ch}(F) \mid k$ 时, $x = \alpha$ 是 $f'(x)$ 的至少 k 重根.

特别地, 若 $x = \alpha$ 是 $f(x)$ 的单根, 则 $f'(\alpha) \neq 0$.

证明 考虑 f 在 E 内的分解

$$f(x) = (x-\alpha)^k \cdot g(x), \quad g(\alpha) \neq 0.$$

因此

$$f'(x) = (x-\alpha)^{k-1} q(x),$$

这里 $q(x) = kg(x) + (x-\alpha)g'(x)$.

注意 $q(\alpha) = kg(\alpha)$. 如果特征 $\mathrm{ch}(F) = 0$ 或 $\mathrm{ch}(F) \nmid k$ 时, 那么 $q(\alpha) \neq 0$, 即 $(x-\alpha) \nmid q(x)$, 所以 $x = \alpha$ 是 $f'(x)$ 的 $k-1$ 重根.

若 $\mathrm{ch}(F) \mid k$, 则 $q(\alpha) = 0$, 即 $(x-\alpha) \mid q(x)$, 故 $x = \alpha$ 是 $f'(x)$ 的至少 k 重根. ■

定理 4.2.6 (重根判别法) 设 E/F 是 $f(x) \in F[x]$ 在 F 上的分裂域.

(1) f 在 E 内无重根当且仅当 $\gcd(f(x), f'(x)) = 1$.

(2) 若 $f(x)$ 不可约, 则它在 E 内无重根的充要条件为 $f'(x)$ 是非零多项式. 特别地, 当 $\mathrm{ch}(F) = 0$ 时, $F[x]$ 中的任何不可约多项式均无重根.

证明 (1) ($\Longrightarrow$) 已知 $f(x)$ 在 E 内无重根, 则由引理 4.2.2, $f(x)$ 与 $f'(x)$ 无公共根. 设 $d(x) = \gcd(f, f')$. 若 $d(x) \neq 1$, 则 $d(x)$ 的根是 f, f' 的公共根, 矛盾! 因此, $d = 1$.

($\Longleftarrow$) 设 α 是 $f(x)$ 的任一根. 若 $k > 1$, 则由引理 4.2.2, α 是 $f'(x)$ 的至少 $k-1 (\geq 1)$ 重根, 因而 $d(x) = \gcd(f, f')$ 是正次数首一多项式, 矛盾! 故 $k = 1$, 即 α 是单根.

(2) $f(x)$ 有重根当且仅当 $d(x) = \gcd(f, f')$ 是正次数多项式. 由于 $f(x)$ 不可约, 故 $d(x) = f(x)$, 从而 $f(x) \mid f'(x)$. 若 $f'(x) \neq 0$, 则 $\deg f' < \deg f$, 故不可能 $p \mid f'$, 矛盾! 因此, $f'(x) = 0$. ■

定义 4.2.3 (1) 设 $p(x)\in F[x]$ 是不可约多项式, E 是 $p(x)$ 的分裂域. 若 p 在 E 中只有单根, 就称 p 在 F 上可分 (Separable).
(2) 设 $f(x)\in F[x]$ 是非常值多项式. 如果 f 在 $F[x]$ 内的任何不可约因式都是可分的, 则称 f 在 F 可分; 否则 f 称为 F 上不可分的.

定义 4.2.4 设 E/F 是代数扩张, $\alpha\in E$.

(1) 如果 α 的极小多项式是 F 上可分多项式, 则称 α 是可分元素; 否则称为不可分元素.

(2) 如果 E 的每个元素在 F 上可分, 则称 E/F 是可分扩张; 否则称之为不可分扩张.

基域的特征对于扩张的可分性有影响. 下面我们来分析一下.

推论 4.2.6 若 $\mathrm{ch}(F)=0$, 则任何代数扩张 E/F 都是可分扩张.

证明 由定理 4.2.6 (2), F 上的任何不可约多项式都是可分的. 由此立得结论. ■

下面讨论正特征的域. 我们先回顾一些基本事实. 设 $\mathrm{ch}(F)=p>0$. 对任何 $\alpha,\beta\in F$, 我们有 $(\alpha+\beta)^p=\alpha^p+\beta^p$. 更一般地, 我们有

$$(\alpha_1+\cdots+\alpha_r)^{p^e}=\alpha_1^{p^e}+\cdots+\alpha_r^{p^e}.$$

命题 4.2.5 (**不可分多项式**) 设 $\mathrm{ch}(F)=p>0$, $f(x)\in F[x]$ 是不可分的不可约多项式, E/F 是 $f(x)$ 的分裂域, 则

$$f(x)=\prod_{i=1}^{r}(x-\beta_i)^{p^e},\quad \beta_i\in E,$$

这里 e 是某正整数, 诸根 β_i 互不相同. 特别地, 不可分的不可约多项式的每个根都相同重数, 该重数是 p 的方幂.

证明 设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0.$$

由定理 4.2.6, 此时 $f'(x)=0$, 即 $ka_k=0$, $k=0,1,\cdots,n$. 这意味着, 当 $p\nmid k$ 时, $a_k=0$. 因此,

$$f(x)=a_{mp}x^{mp}+a_{(m-1)p}x^{(m-1)p}+\cdots+a_px^p+a_0.$$

令

$$g(x)=a_{mp}x^m+a_{(m-1)p}x^{(m-1)}+\cdots+a_px+a_0,$$

则 $f(x)=g(x^p)$, $g(x)$ 在 F 上仍然不可约.

同样地, 若 g 不可分, 则 $g(x)=h(x^p)$. 依次类推, 最终得

$$f(x)=u(x^{p^e}),$$

这里 $u(x)\in F[x]$ 是可分的不可约多项式. $u(x)$ 可分解为

$$u(x)=(x-\alpha_1)\cdots(x-\alpha_r),\quad \alpha_i\neq\alpha_j.$$

因此

$$f(x) = (x^{p^e} - \alpha_1)\cdots(x^{p^e} - \alpha_r).$$

令 β_i 是 $x^{p^e} - \alpha_i = 0$ 的根, 则

$$x^{p^e} - \alpha_i = x^{p^e} - \beta_i^{p^e} = (x - \beta_i)^{p^e}.$$

将上式代入 $f(x)$ 的分解式即得结论. ■

例 4.2.10 (不可分多项式的例子) 设 $F = \mathbb{F}_p(t)$ 是模 p 剩余类域上 (关于 t) 的有理函数域. 我们先承认 $f(x) = x^p - t \in F[x]$ 是不可约的. 注意 $f'(x) = px^{p-1} = 0$, 因而 $f(x)$ 是不可分的.

现在我们证明 $f(x)$ 不可约. 不妨假设 f 可约, $f(x) = h(x)\cdot g(x)$, g, h 非常值. 设 E 是 f 的分裂域, $\alpha \in E$ 是 f 的根. 因此

$$h \cdot g = x^p - t = x^p - \alpha^p = (x - \alpha)^p.$$

这表明 $h(x) = (x - \alpha)^r \in F[x]$, $0 < r < p$, 故 $\alpha^r \in F$. 由于 $(r, p) = 1$, 故存在整数 u, v 使得 $ru + pv = 1$. 因此

$$\alpha = \alpha^{ur+pv} = (\alpha^r)^u \cdot (\alpha^p)^v = (\alpha^r)^u \cdot t^v \in F,$$

即 $\alpha = a(t)/b(t)$, 从而 $tb(t)^p = a(t)^p$. 注意到 $\mathbb{F}_p$ 的元素均满足费马小定理 $k^p = k$ $(\forall k \in \mathbb{F}_p)$. 因此 $a(t)^p = a(t^p)$, $b(t)^p = b(t^p)$, 故 $tb(t^p) = a(t^p)$, 两边次数不一致, 矛盾! 这就证明 $f(x)$ 不可约. ■

例 4.2.11 (有限域) 设 $\mathbb{F}_p$ 是模素数 p 的剩余类域, $n \geq 1$, $q = p^n$, $f(x) = x^q - x \in \mathbb{F}_p[x]$, E 是 $f(x)$ 的分裂域.

我们首先证明 $f(x)$ 在 $\mathbb{F}_p$ 上是可分的. 这是因为

$$f'(x) = qx^{q-1} - 1 = -1 \neq 0,$$

所以由重根判别法知 $f(x)$ 无重根. 因此 $f(x)$ 恰有 q 个不同的根, 设为 $\alpha_1, \cdots, \alpha_q$.

其次证明 $K = \{\alpha_1, \cdots, \alpha_q\}$ 是 E 的子域. 对任何 $\alpha, \beta \in K$, 我们有

$$(\alpha - \beta)^q = \alpha^q - \beta^q = \alpha - \beta,$$

$$(\alpha \cdot \beta^{-1})^q = \alpha^q \cdot \beta^{-q} = \alpha \cdot \beta^{-1},\ \beta \neq 0.$$

因此 K 是 E 的子域. 注意到 $E = \mathbb{F}_p(\alpha_1, \cdots, \alpha_q)$, 所以显然有 $K = E$.

E 是仅有 $q = p^n$ 个元素的有限域, 也叫做伽罗瓦域通常记作 $\mathbb{F}_q$ 或 $\mathrm{GF}(p^n)$.

$\mathbb{F}_q$ 有一个 $\mathbb{F}_p$-自同态

$$F : \mathbb{F}_q \longrightarrow \mathbb{F}_q, \quad a \to a^p.$$

容易验证, 它是自同构, 称为 Frobenius 自同构. ■

根据上面的讨论, 我们可以证明如下经典结论.

定理 4.2.7 (有限域分类定理) 任何有限域必同构于某个伽罗瓦域 $\mathbb{F}_q$, 这里 $q = p^n$, $n \geq 1$, p 是素数.

证明 设 E 是特征 p 的有限域, 因而包含素域 $\mathbb{F}_p$. 由有限性, E 是域 $\mathbb{F}_p$ 上的有限维线性空间, 不妨设 $u_1,\cdots,u_n$ 是一组基. 因而对任何 $a\in E$, 有唯一的表达式

$$a=a_1u_1+\cdots+a_nu_n,\quad a_i\in\mathbb{F}_p.$$

每项系数的取值只能是 $[0],\cdots,[p-1]$ 之一, 因而 a 共有 $q=p^n$ 种取法. 这表明 $|E|=q$. $E^*=E-\{0\}$ 是 $q-1$ 阶群, 因而由拉格朗日定理, $a^{q-1}=1,\forall a\in E^*$. 这表明 E 的元素都是方程 $x^q-x=0$ 的根, 因而该方程至少有 $q=p^n$ 个根. 另一方面, 该方程最多只有 p^n 个根 (推论 2.3.6). 因而 E 中的元素恰好跑遍 $x^q-x=0$ 的所有根. 由此知, E 是 x^q-x 的分裂域. 由分裂域的唯一性, E 是唯一的 q 阶域, 即 $E=\mathbb{F}_q$. ■

注 4.2.4 $\mathbb{F}_q^*=\mathbb{F}_q-\{0\}$ 是 $q-1$ 阶循环群. 限于篇幅, 我们不再证明该结论. ■

接下来, 我们要利用可分性来探讨有限扩张 E/F 何时是单扩张.

定理 4.2.8 *设 F 是有限域, E/F 是有限扩张, 则 E/F 是单代数扩张.*

证明 设 $n=[E:F]$. E 作为域 F 上的有限维线性空间, 有基 $u_1,\cdots,u_n$. 因而对任一 $a\in E$, 都可唯一地写为

$$a=a_1u_1+\cdots+a_nu_n,\quad a_i\in F.$$

因为每个 a_i 的取值可能性有 $|F|$ 个, 所以 $|E|=|F|^n$, 即 E 仍为有限域.

根据注记 4.2.4, E^* 是循环群. 今取生成元 $\alpha\in E^*$, 因而有 $E=F(\alpha)$. ■

更一般地, 我们有

定理 4.2.9 *设 E/F 是有限扩张, $E=F(\alpha_1,\cdots,\alpha_r)$, 并且 $\alpha_2,\cdots,\alpha_r$ 在 F 上可分, 则 E/F 是单代数扩张.*

特别地, 有限可分扩张必是单代数扩张.

证明 由定理 4.2.8 的结论, 我们下面只需要讨论 F 是无限域的情形. 不妨对 r 施归纳法.

先证 $r=2$ 的情形. 设 $E=F(\alpha,\beta)$, β 是可分的. 设 $f(x),g(x)$ 分别是 α,β 的极小多项式, E'/E 是 $f(x)g(x)$ 在 E 上的分裂域. $\alpha_1=\alpha,\cdots,\alpha_\ell$ 和 $\beta_1=\beta,\cdots,\beta_s$ 分别是 $f(x),g(x)$ 在 E' 中的全部根.

注意到 F 是无限域, 故可找 $c\in F$, 使得

$$\alpha_i+c\beta_j\neq\alpha_k+c\beta_1,\quad\forall i,j,k.$$

令 $\theta=\alpha_1+c\beta_1$, 则由 c 的选取可知, $f(\theta-cx)$ 与 $g(x)$ 仅有一个公共根 β_1, 即有公因子 $x-\beta_1$. 注意到 $x-\beta_1$ 是 $g(x)$ 的单因式 (来自 β 的可分性), 故 $\gcd(f(\theta-cx),g(x))=(x-\beta_1)$.

设 $K=F(\theta)$. 注意到 $f(\theta-cx),g(x)\in K[x]$, 因而存在 $u(x),v(x)\in K[x]$, 使得

$$u(x)f(\theta-cx)+v(x)g(x)=x-\beta_1.$$

这就推出 $\beta_1\in K$, 因而 $\alpha_1=\theta-c\beta_1\in K$, 故有 $E=F(\alpha,\beta)\subseteq K=F(\theta)$. 反过来, 显然有 $K\subseteq E$, 从而

$$F(\theta)=K=E=F(\alpha,\beta).$$

今假设 $< r$ 的情形已证. 由归纳假设, 存在 $\alpha \in E$, 使得 $F(\alpha_1, \cdots, \alpha_{r-1}) = F(\theta)$. 因此

$$E = F(\alpha_1, \cdots, \alpha_{r-1})(\alpha_r) = F(\alpha, \alpha_r).$$

再由前面讨论, 存在 $\theta \in E$, 使得 $F(\alpha, \alpha_r) = F(\theta)$. 这就证明了 E/F 是单扩张. ■

E/F 如果能写成 $E = F(\alpha)$, 我们就称 $\alpha \in E$ 是 E/F 的本原元素. 上面的结论告诉我们, 有限扩张必含本原元素.

本章习题

加 $*$ 号的习题表示有一定难度.

习题 4.1

第五章　伽罗瓦理论初步

5.1　伽罗瓦扩张

设 E/F 是域扩张. E 的所有 F-自同构全体构成的群叫做 E/F 的*伽罗瓦群*, 记作 $\mathrm{Gal}(E/F)$.

设 G 是域 E 的任一自同构群. 我们定义集合

$$\mathrm{Inv}(G)=\{a\in E|\sigma(a)=a,\ \forall\sigma\in G\}.$$

对任何 $a,b\in\mathrm{Inv}(G)$, 因为

$$\sigma(a-b)=\sigma(a)-\sigma(b)=a-b,$$
$$\sigma(ab^{-1})=\sigma(a)\sigma(b)^{-1}=ab^{-1},\ b\neq 0,$$

故 $a-b, ab^{-1}\in\mathrm{Inv}(G)$. 这就推出 $\mathrm{Inv}(G)$ 是 E 的子域. 它称作 G 的*不动域*. $\mathrm{Inv}(G)$ 的元素称作 G 的*不动元*.

我们有显然的包含关系

$$F\subseteq\mathrm{Inv}(\mathrm{Gal}(E/F)).$$

例 5.1.1　二次扩域 $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ 的伽罗瓦群

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})=\mathbb{Z}_2.$$

具体验证可以参看例 1.6.6. ■

例 5.1.2　三次扩域 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 的伽罗瓦群是平凡群. 这是因为, 对任何 $\sigma\in\mathrm{Gal}(E/F)$,

$$(\sigma(\sqrt[3]{2}))^3=\sigma((\sqrt[3]{2})^3)=\sigma(2)=2,$$

从而$\sigma(\sqrt[3]{2})$ 只能是实根 $\sqrt[3]{2}$. ■

定义 5.1.1　*如果域扩张 E/F 的伽罗瓦群的不动域等于 F, 则 E/F 称为伽罗瓦扩张.*

引理 5.1.1 (Artin)　*设 G 是域 E 的一个有限自同构群, 则*

$$[E:\mathrm{Inv}(G)]\leq|G|.$$

证明　设 $G=\{\sigma_1=Id_E,\ \sigma_2,\ \cdots,\ \sigma_n\}$. 任取 E 中的 $n+1$ 个非零元素 $u_1,\cdots,u_{n+1}$.

考虑域 E 上的向量

$$v_i=(\sigma_1(u_i),\cdots,\sigma_n(u_i)),\quad i=1,\cdots,n+1.$$

显然 $v_1,\cdots,v_{n+1}$ 在 E 上线性相关, 因而存在 $r<n+1$, 使得 $v_1,\cdots,v_r$ 线性无关, $v_1,\cdots,v_{r+1}$ 线性相关. 因此

$$v_{r+1}=a_1v_1+\cdots+a_rv_r,\quad a_i\in E,$$

故

$$\sigma_i(u_{r+1}) = a_1\sigma_i(u_1) + \cdots + a_r\sigma_i(u_r), \quad i = 1, \cdots, n. \tag{5-1}$$

将任何 $\sigma \in G$ 作用于上式得

$$\sigma\sigma_i(u_{r+1}) = \sigma(a_1)\sigma\sigma_i(u_1) + \cdots + \sigma(a_r)\sigma\sigma_i(u_r), \quad i = 1, \cdots, n.$$

注意到 $\sigma\sigma_1, \cdots, \sigma\sigma_n$ 只不过是 $\sigma_1, \cdots, \sigma_n$ 置换, 所以 σ 的作用只是引起了诸 v_i 的分量间的同一置换. 因此适当重新调整这些分量的位置, 我们就得

$$v_{r+1} = \sigma(a_1)v_1 + \cdots + \sigma(a_r)v_r.$$

由于 $v_1, \cdots, v_r$ 线性无关, 故上述表达式唯一, 从而迫使 $\sigma(a_i) = a_i$, 对任何 $\sigma \in G$, $1 \leq i \leq r$ 成立. 这样, $a_i \in \mathrm{Inv}(G)$.

因此, $v_1, \cdots, v_{r+1}$ 作为域 $\mathrm{Inv}(G)$ 上的向量是线性相关的. 考虑式 (5-1) 在 $i = 1$ 的情形, 即知 $u_{r+1} = \sum\limits_{i=1}^{r} \sigma(a_i)u_i$. 因而 $u_1, \cdots, v_n$ 在 F 上线性相关, 故 $[E : \mathrm{Inv}(G)] \leq |G|$. ■

引理 5.1.2 设 $\sigma_1, \cdots, \sigma_r$ 是域 E 的 r 个不同的自同构, $S = \{\sigma_1, \cdots, \sigma_r\}$, $\langle S\rangle$ 是由 S 生成的自同构子群, 则

(1) $\sigma_1, \cdots, \sigma_r$ 在 E 上线性无关, 即对任何一组不全为零的元素 $a_1, \cdots, a_r \in E$, 都存在 $x \in E$, 使得 $\sum\limits_{i=1}^{r} a_i\sigma_i(x) \neq 0$.

(2) $r \leq [E : \mathrm{Inv}(\langle S\rangle)]$.

证明 (1) 反证法, 假设诸 σ_i 线性相关. 因而存在 $s < r$, 使得 $\sigma_1, \cdots, \sigma_s$ 线性无关, 但 $\sigma_1, \cdots, \sigma_{s+1}$ 线性相关, 即 σ_{s+1} 可唯一表达成

$$\sigma_{s+1}(x) = \sum_{i=1}^{s} a_i\sigma_i(x), \quad a_i \in E, \quad \forall x \in E.$$

对任何非零元 $a \in E$, 用 ax 代替 x, 我们有

$$\sigma_{s+1}(x) = \sum_{i=1}^{s} \frac{a_i\sigma_i(a)}{\sigma_{s+1}(a)}\sigma_i(x).$$

由表达的唯一性可得,

$$a_i = \frac{a_i\sigma_i(a)}{\sigma_{s+1}(a)}.$$

由于 $\sigma_{s+1} \neq 0$, 故存在 $a_i \neq 0$. 这就推出 $\sigma_i(a) = \sigma_{s+1}(a)$. 由 a 的任意性, $\sigma_i = \sigma_{s+1}$, 矛盾! 故 $\sigma_1, \cdots, \sigma_r$ 线性无关.

(2) 假设 $n = [E : F]$ 是有限数. $F := \mathrm{Inv}(\langle S\rangle)$. 因为任意 $\sigma \in S$, 都保持 F 中的元素不动, 所以对任何 $\alpha, \beta \in E$, $\gamma \in F$, 有

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta), \quad \sigma(\gamma\alpha)\sigma(\gamma) = \sigma(\alpha) = \gamma\sigma(\alpha).$$

这表明 σ 是线性空间 E/F (在域 F 上) 的线性变换. 因此任何线性组合 $a_1\sigma_1 + \cdots + a_r\sigma_r$ 都是 E/F 的线性变换. 由 (1), 该变换为零当且仅当诸 $a_i = 0$.

设 $u_1,\cdots,u_n$ 是 E/F 的一组基. 考虑向量 $v_i=(\sigma_i(u_1),\sigma_i(u_2),\cdots,\sigma_i(u_n))$. 我们证明 $v_1,\cdots,v_r$ 在 E 上线性无关, 因而 $r\le n$.

假设存在 $a_1,\cdots,a_r\in E$, 使得 $\sum\limits_{i=1}^{r}a_iv_i=0$. 从分量上看, $\sum\limits_{i=1}^{r}a_i\sigma_i(u_k)=0$, $k=1,2,\cdots,n$. 这推出 $\sum\limits_{i=1}^{r}a_i\sigma_i$ 是零变换, 故每个 $a_i=0$. ■

推论 5.1.1 设 E/F 是有限扩张, 则 E/F 的 F-自同构个数不超过 $[E:F]$, 即

$$|\mathrm{Gal}(E/F)|\le[E:F].$$

证明 任取 r 个 F-自同构组成的集合 S. 由引理 5.1.2,

$$r\le[E:\mathrm{Inv}(\langle S\rangle)]\le[E:F].$$

这就表明 F-自同构的个数不超过 $[E:F]$. ■

定理 5.1.1 (**有限伽罗瓦扩张**) 设 E/F 是域扩张, 则以下条件彼此等价.

(1) E/F 是有限伽罗瓦扩张

(2) E 有一个有限自同构群 G 满足 $\mathrm{Inv}(G)=F$.

(3) E/F 是有限扩张, 并且有一个 F-自同构群 G' 满足 $|G'|=[E:F]$.

(4) $|\mathrm{Gal}(E/F)|=[E:F]<\infty$.

条件成立时, 总有 $G=G'=\mathrm{Gal}(E/F)$.

证明 我们先证明 (1)(2) 等价.

(1) $\Longrightarrow$ (2) 此时 $\mathrm{Inv}(\mathrm{Gal(E/F)})=F$. 由推论 5.1.1, $|\mathrm{Gal}(E/F)|\le[E:F]$. 我们只需取 $G=\mathrm{Gal}(E/F)$ 即可.

(2) $\Longrightarrow$ (1) 由定义, $F\subseteq\mathrm{Inv}(\mathrm{Gal}(E/F))$. 因为 $G\subseteq\mathrm{Gal}(E/F)$, 所以 $\mathrm{Inv}(\mathrm{Gal}(E/F))\subseteq\mathrm{Inv}(G)=F$. 这就推出 $\mathrm{Inv}(\mathrm{Gal}(E/F))=F$, 即 E/F 是伽罗瓦扩张. 由 Artin 引理及引理 5.1.2, 我们可得 $|G|=[E:F]$. 这也表明 E/F 也是有限扩张.

当 (1)(2) 成立时, 前面已证 $|\mathrm{Gal}(E/F)|\le[E:F]$. 再由 Artin 引理, $[E:F]\le|\mathrm{Gal}(E/F)|$. 这就迫使 $[E:F]=|\mathrm{Gal}(E/F)|$, 因此 (1)(2) 蕴含了 (4). 这就推出 (2) 中的 G 满足 $|G|=|\mathrm{Gal}(E/F)|$. 由于 $G\subseteq\mathrm{Gal}(E/F)$, 故 $G=\mathrm{Gal}(E/F)$.

再证 (3)(1) 等价.

(3) $\Longrightarrow$ (1) 设 $\mathrm{Inv}(G')=F_1$. 此时 E/F_1 满足 (2) 的条件, 因而推出 E/F_1 是伽罗瓦扩张, 并且 $G'=\mathrm{Gal}(E/F_1)$. 再由 (1) 得 $|G'|=[E:F_1]$. 所以 $[E:F]=[E:F_1]$. 由望远镜定理得 $[F_1:F]=1$, 即 $F_1=F$. 因此 E/F 是伽罗瓦扩张. 这也蕴含了 $G'=\mathrm{Gal}(E/F)$.

(1) $\Longrightarrow$ (3) 取 $G'=\mathrm{Gal}(E/F)$ 即可.

(1) $\Longrightarrow$ (4) 前已说明.

(4) $\Longrightarrow$ (1) 取 $G=\mathrm{Gal}(E/F)$, 它满足条件 (3), 由此知 E/F 是伽罗瓦扩张.

5.2 伽罗瓦基本定理

设 E/F 是有限伽罗瓦扩张, $G = \mathrm{Gal}(E/F)$.

引理 5.2.1 设 L 是 E/F 的中间域, 则 E/L 也是有限伽罗瓦扩张.

证明 $L_1 = \mathrm{Inv}(\mathrm{Gal}(E/L))$. 显然, $L \subseteq L_1$. 我们的目标是证 $L_1 = L$. 这等价于证 $[L : F] = [L_1 : F]$ (利用望远镜定理). 由于$[L : F] \leq [L_1 : F]$ 是显然的, 因此可归结为证明 $[L : F] \geq [L_1 : F]$.

因为 $\mathrm{Gal}(E/L) < \mathrm{Gal}(E/F)$ 是有限群, 故由定理 5.1.1,

$$[E : L_1] = |\mathrm{Gal}(E/L)|, \quad [E : F] = |G|.$$

因此由望远镜定理得 $[L_1 : F] = [G : \mathrm{Gal}(E/L)]$. 这样, 我们需证明 $[L : F] \geq [G : \mathrm{Gal}(E/L)]$.

考虑 G 关于 $\mathrm{Gal}(E/L)$ 的左陪集

$$G = \bigcup_{i=1}^{r} \sigma_i \mathrm{Gal}(E/L), \quad \sigma_1 = Id_E.$$

设 σ, τ 来自于同一陪集, 那么 $\tau^{-1}\sigma|_L = Id_L$. 这意味着 $\sigma|_L = \tau|L : L \to E$ 是同一个 F-嵌入同态. 因此每个陪集唯一确定了一个从 L 到 E 的 F-嵌入同态.

现在我们证明对任何两个不同的 σ_i, σ_j, 它们诱导的上述嵌入同态不相同. 若不然, $\sigma_i(a) = \sigma_j(a), \forall a \in L$, 即 $\sigma_j^{-1}\sigma_i(a) = a, \forall a \in L$. 这表明 $\sigma_j^{-1}\sigma_i \in \mathrm{Gal}(E/L)$, 即它们属于同一陪集, 矛盾! 因此这也推出 $\sigma_i \in \mathrm{Gal}(E/F)$ 是两两不同的映射. 由引理 5.1.2, $[G : \mathrm{Gal}(E/F)] = r \leq [L : F]$. ■

定理 5.2.1 (**伽罗瓦基本定理**) 设 E/F 是有限伽罗瓦扩张, $G = \mathrm{Gal}(E/F)$. 设 A 是 G 的所有子群构成的集合, B 是 E/F 的所有中间域构成的集合. 那么

(1) 存在 A, B 间的一一对应

$$\Phi : A \longrightarrow B, \quad H \to \mathrm{Inv}(H).$$

$\Phi^{-1}(K) = \mathrm{Gal}(E/K)$. 特别地, 我们有

$$\mathrm{Gal}(E/\mathrm{Inv}(H)) = H,$$
$$\mathrm{Inv}(\mathrm{Gal}(E/K)) = K.$$

(2) 上述对应是反序的, 即

$$H_1 \subseteq H_2 \Longleftrightarrow \mathrm{Inv}(H_1) \supseteq \mathrm{Inv}(H_2).$$

(3)

$$[E : \mathrm{Inv}(H)] = |H|,$$
$$[\mathrm{Inv}(H) : F] = [G : H].$$

(4) $\mathrm{Inv}(\sigma H \sigma^{-1}) = \sigma(\mathrm{Inv}(H)), \sigma \in G$.

(5) $H \lhd G$ 当且仅当 $\mathrm{Inv}(H)/F$ 是伽罗瓦的, $\mathrm{Gal}(\mathrm{Inv}(H)/F) \cong G/H$.

证明 (1) 设

$$\Psi : B \longrightarrow A, \quad K \to \mathrm{Gal}(E/K).$$

因为 $H < G$ 是有限群, 故由定理 5.1.1 知 $E/\mathrm{Inv}(H)$ 是伽罗瓦扩张, 且 $H = \mathrm{Gal}(E/\mathrm{Inv}(H))$. 这就证明了 $\Psi\Phi = Id_A$.

设 K 是 E/F 的中间域, 则由引理 5.2.1, E/K 是伽罗瓦扩张, $K = \mathrm{Inv}(\mathrm{Gal}(E/K))$. 这证明了 $\Phi\Psi = Id_B$. 因此 Φ 是一一对应.

(2) 由 Φ 定义即得.

(3) 因为 $E/\mathrm{Inv}(H)$ 是伽罗瓦扩张, 所以由定理 5.1.1,

$$[E : \mathrm{Inv}(H)] = |H|.$$

又由 $[E : F] = |G|$ 及望远镜定理,

$$[\mathrm{Inv}(H) : F] = \frac{[E : F]}{[E : \mathrm{Inv}(H)]} = |G|/|H| = [G : H].$$

(4) 设 $H' := \Psi(\sigma(\mathrm{Inv}(H)))$. 利用 Φ 的双射性, 我们只需要证明 $H' = \sigma H \sigma^{-1}$. 先证 $\sigma H \sigma^{-1} \subseteq H'$, 即对任意 $\tau \in H$, 要证 $\sigma\tau\sigma^{-1}$ 作用在 $\sigma(\mathrm{Inv}(H))$ 是不动的. 任取 $a \in \mathrm{Inv}(H)$, 我们有

$$\sigma\tau\sigma^{-1}(\sigma(a)) = \sigma\tau(a) = \sigma(a).$$

反过来证, $H' \subseteq \sigma H \sigma^{-1}$. 类似上面讨论, 可得 $\sigma^{-1} H' \sigma \subseteq H$, 故得结论.

(5) ($\Longrightarrow$) 已知 H 在 G 中正规. 由 (4) 知, $\sigma(\mathrm{Inv}(H)) = \mathrm{Inv}(H)$. 因而 σ 诱导了 $\mathrm{Inv}(H)$ 的 F-自同构 $\bar{\sigma} \in \mathrm{Gal}(\mathrm{Inv}(H)/F)$. 由此可构造群同态

$$G \longrightarrow \mathrm{Gal}(\mathrm{Inv}(H)/F), \quad \sigma \to \bar{\sigma},$$

其核是 H. 由同态基本定理得单同态

$$G/H \to \mathrm{Gal}(\mathrm{Inv}(H)/F).$$

由 (3), $[\mathrm{Inv}(H) : F] = [G : H]$, 以及 $|\mathrm{Gal}(\mathrm{Inv}(H)/F)| \leq [\mathrm{Inv}(H) : F]$ (推论 5.1.1), 可知上述同态也是满的, 因此也是同构. 此时有 $|\mathrm{Gal}(\mathrm{Inv}(H)/F)| = [\mathrm{Inv}(H) : F]$, 故由定理 5.1.1 知 K/F 是伽罗瓦的.

($\Longrightarrow$) 已知 K/F 是伽罗瓦扩张, 设

$$r := [K : F] = |\mathrm{Gal}(K/F)|.$$

K 有 r 个 F-自同构. 要证 $\forall \sigma \in G$, 有 $\sigma(K) = K$.

假设存在 $\sigma \in G$, 使得 $\sigma(K) \neq K$, 则 σ 诱导的 F-嵌入同态 $K \to E$ 不可能与上述 r 个嵌入不同, 这样我们有至少 $r + 1$ 个不同的 F-嵌入同态 $K \to E$. 但这与引理 5.2.1 的讨论矛盾! 因此 $\sigma(K) = K$. 这样, 由 (4) 即得结论. ■

(今年课时不够, 暂时写到这儿, 明年再续)

5.3 可分正规扩张

5.4 多项式的伽罗瓦群

5.5 应用: 方程根式解的判则

本章习题

加 $*$ 号的习题表示有一定难度.

习题 5.1

参 考 文 献

[HW10] 华罗庚, 万哲先: *华罗庚文集: 代数卷 I*, 科学出版社, 2010.

[ND88] 聂灵沼, 丁石孙: *代数学引论*, 高等教育出版社, 1988.

[God13] R. Godement: *代数学教程*, 高等教育出版社, 2013.

索 引