近世代数

欧阳毅 叶郁
中国科学技术大学
数学科学学院

Email: yiouyang@ustc.edu.cn, yeyu@ustc.edu.cn

目 录

第一章　群的基本概念与性质

§1.1　集合与映射

§1.1.1　集合的定义

我们首先回顾一下集合的定义.

将一些不同的对象放在一起, 即为**集合** (set), 其中的对象称为集合的**元素** (element). 在本书中, 我们将使用大写字母 $A, B, C, \ldots$ 来表示集合, 用小写字母 $a, b, c, \ldots$ 来表示集合的元素. 记 A 为一个集合. 如果 a 是 A 中的元素, 则称 a 属于 A, 记为 $a \in A$, 否则记为 $a \notin A$. 我们也可以将集合 A 表示为 $A = \{a \mid a \in A\}$, 其中 $a \in A$ 可以用 A 中元素满足的共同性质代替, 比如说偶数集合=$\{a$为整数 $\mid a \equiv 0 \mod 2\}$. 注意到集合中元素总是不重复的.

如果集合 A 中的每一个元素均是集合 B 中元素, 则称 A 是 B 的**子集** (subset), 换言之, 即若 $a \in A$, 则 $a \in B$. 此时我们记为 $A \subseteq B$ 或 $B \supseteq A$. 可以用图 1.1 来表示 $A \subseteq B$.

如果集合 $A \subseteq B$ 且 $B \subseteq A$, 即 $a \in A$ 当且仅当 $a \in B$, 称 A 与 B **相等**, 并记为 $A = B$. 如果 $A \subseteq B$ 且 $A \neq B$, 我们称 A 为 B 的**真子集** (proper subset), 记为 $A \subset B$ 或者$A \subsetneq B$.

不含任何元素的集合称为**空集** (empty set), 记为 $\varnothing$. 由定义可知, 空集 $\varnothing$ 是任何集合的子集, 且是任何非空集合的真子集.

如果集合A的元素个数有限, 称A 为**有限集** (finite set), 其元素个数称为**集合的阶** (cardinality 或order of finite set), 记为$|A|$. 元素个数无限的集合, 即**无限集** (infinite set), 它的阶定义为 ∞.

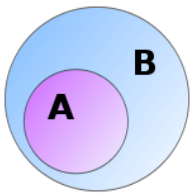


图 1.1: 集合的包含关系

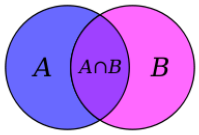


图 1.2: 集合的交

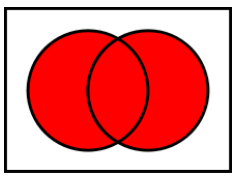


图 1.3: 集合的并

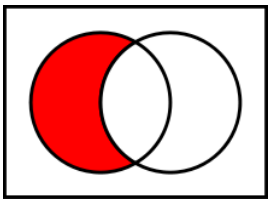


图 1.4: 集合的补集$A-B$

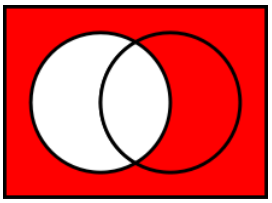


图 1.5: 集合的补集A^c

§1.1.2 集合的基本运算

一般来说, 集合有如下的四种基本运算.

(I) **集合的交** 设 A, B 为两个集合, 则A **与** B **的交集** (intersection)为

$$A \cap B := \{x \mid x \in A \text{ 且 } x \in B\}.$$

可以用图 1.2 表示集合的交.

更一般地, 设 I 为集合, 设 I 中每个元素 i 对应集合 A_i, 则集合 $A_i (i \in I)$ 的交为

$$\bigcap_{i \in I} A_i := \{x \mid x \in A_i \text{ 对每个 } i \in I \text{ 成立}\}.$$

(II) **集合的并** 设集合 A, B 如上所示, 则A **与** B **的并集** (union)为

$$A \cup B := \{x \mid x \in A \text{ 或 } x \in B\}.$$

可以用图 1.2 表示集合的并. 更一般地, 集合 $A_i (i \in I)$ 的并为

$$\bigcup_{i \in I} A_i := \{x \mid x \in A_i \text{ 对某个 } i \in I \text{ 成立}\}.$$

如果 A_i 两两不交(即交集为空集), 我们称 $\bigcup\limits_{i \in I} A_i$ 为**不交并**(disjoint union), 并记为 $\bigsqcup\limits_{i \in I} A_i$.

(III) **集合的差集与补集** 设 A, B 为某固定集合 U 的子集, 则A **对** B **的补集或差集** (complement)为

$$A - B := \{x \mid x \in A \text{ 且 } x \notin B\}.$$

它可用图 1.4 表示. 由补集定义, 我们有

$$A = (A \cap B) \sqcup (A - B).$$

A **在** U **中的补集**为

$$A^c := \{x \in U \mid x \notin A\}.$$

它可用图 1.5 表示.

由定义可知, 如果 A, B 为有限集, 记 $|A|$ 为 A 的元素个数, 则 $A \cup B, A \cap B$ 均为有限集, 且

$$|A \cup B| = |A| + |B| - |A \cap B|. \tag{1.1}$$

更进一步地, 我们有

命题1.1 (容斥原理)**.** *设 $A_i,\ i = 1, \ldots, n$ 为某固定集合 U 的有限子集, 则*

$$|A_1 \cup \ldots \cup A_n| = \sum_{j=1}^{n} (-1)^{j-1} \sum_{\{i_1,\ldots,i_j\} \subseteq \{1,\ldots,n\}} |A_{i_1} \cap \ldots \cap A_{i_j}|. \tag{1.2}$$

证明. 对集合个数n用归纳法. □

命题1.2. *设 $A_i\ (i \in I)$ 为某固定集合 U 的子集, 则*

$$\bigcap_{i \in I} A_i^c = \Big(\bigcup_{i \in I} A_i\Big)^c. \tag{1.3}$$

证明. 我们有

$$\begin{aligned} x \in \bigcap_{i \in I} A_i^c &\iff x \in A_i^c \text{ 对任意} i \in I \text{ 成立} \\ &\iff x \notin A_i \text{ 对任意} i \in I \text{ 成立} \\ &\iff x \notin \bigcup_{i \in I} A_i, \text{ 即 } x \in \Big(\bigcup_{i \in I} A_i\Big)^c. \end{aligned}$$

等式得证. □

(IV) **集合的笛卡尔积** 集合 A 与 B 的**笛卡尔积** (Cartesian product)是所有元素对 (a, b), 其中 $a \in A, b \in B$ 构成的集合, 即

$$A \times B := \{(a, b) \mid a \in A, b \in B\}.$$

更进一步地, 集合族 $A_i\ (i \in I)$ 的笛卡尔积为

$$\prod_{i \in I} A_i := \{(a_i)_{i \in I} \mid a_i \in A_i\}.$$

注记. 我们可以用一个简单例子来理解集合.

- 班级 $\longleftrightarrow$ 集合,
- 班上的学生 $\longleftrightarrow$ 元素,
- 班上的一个学习小组 $\longleftrightarrow$ 子集合,
- 所有不参加该学习小组的人 $\longleftrightarrow$ 补集,
- 学校的所有班级 $\longleftrightarrow$ 集合构成的集族.

§1.1.3 一些常用的集合记号

在本书中, 我们将经常使用如下集合:

- $\mathbb{Z}_+$: 正整数集合;
- $\mathbb{N} = \mathbb{Z} \cup \{0\}$: 自然数集合;
- $\mathbb{Z}$: 整数集合;
- $\mathbb{Q}$: 有理数集合;
- $\mathbb{R}$: 实数集合;
- $F[X]$: F ($F = Z, \mathbb{Q}, \mathbb{R}$ 等) 上的(一元) 多项式的集合.

§1.1.4 映射, 合成律和结合律

设 A, B 为两个集合. 如果对 A 中每个元素 a, 均有唯一元素 $b \in B$ 与之对应, 我们称此对应为 A 到 B 的**映射** (map), 记之为

$$f : A \to B, \quad a \mapsto b = f(b).$$

A 称为 f 的**定义域**, $f(A) = \{f(a) \mid a \in A\} \subseteq B$ 称为f 的**值域** 或像集. b 称为a 的像, a 称为b 的原像.

当集合B 是数(有理数, 实数等) 的集合时, 映射f 习惯上称为**函数** (function).

如果对 $a_1, a_2 \in A$, 当 $f(a_1) = f(a_2)$ 时, 则有 $a_1 = a_2$, 我们称映射 f 为**单射** (injective); 如果对任意 $b \in B$, 存在 $a \in A$, 使得 $f(a) = b$, 我们称 f 为**满射** (surjective); 如果 f 既是单射, 又是满射, 我们称 f 为**一一对应** (one-to-one correspondence), 或**双射** (bijective).

对于映射$g, g : A \to B$, 如果对于任意$a \in A$, $f(a) = g(a)$, 称映射f 与g 相等, 记为$f = g$.

设 $f : A \to B, g : B \to C$ 为映射, 则映射

$$g \circ f : A \to C, \quad a \mapsto g(f(a))$$

称为 f 与 g 的**复合映射**(或谓复合律, composition law).

命题1.3 (结合律)**.** 设 $f : A \to B$ 和 $g : B \to C, h : C \to D$ 为集合间的映射, 则

$$(h \circ g) \circ f = h \circ (g \circ f).$$

定义1.4. 设 S 为集合. 我们称映射 $f : S \times S \to S$, $(a, b) \mapsto p$ 为 S 上的一个**二元运算** (binary operation).

注记. 在数学应用中, 记号 $p = f(a, b)$ 并不是一个很适宜的记号. 实际上, 我们经常使用 $+, \times, *, \cdot$ 等符号来表示二元运算, 即

$$\boxed{p = ab,\ a \times b,\ a + b,\ a * b,\ a \cdot b, \text{诸如此类.}}$$

例1.5. 四则运算均是二元运算.

例1.6. 记 Σ_A 为集合 A 到自身的所有映射的集合, 则映射的复合构成 Σ_A 上的二元运算.

记 S_A 为集合 A 到自身的所有双射构成的集合, 则映射的复合构成 S_A 上的二元运算.

定义1.7. 集合 S 上的二元运算如果满足条件对所有 $a, b, c \in S$,

$$(ab)c = a(bc), \tag{1.4}$$

则称该二元运算满足**结合律** (associative law). 如果对任意 $a, b \in S$,

$$ab = ba, \tag{1.5}$$

则称其满足**交换律** (commutative law).

注记. 如果直接用$f(a,b)$ 表示二元运算ab, 则(1.4) 即等式

$$f(f(a,b),c) = f(a,f(b,c)),$$

而(1.5) 即等式

$$f(a,b) = f(b,a).$$

由此可以看出使用乘法记号表示二元运算的简洁性.

容易看出, 上面例子中的二元运算均满足结合律, 但映射的复合并不满足交换律. 事实上, 我们有如下基本事实:

结合律是更一般的规律.

在本书中, 我们将赋予给定集合一个或数个(满足结合律)的二元运算, 从而赋予该集合群, 环或者域的代数结构.

§1.1.5 等价关系, 等价类与分拆

定义1.8. 集合 A 中的元素间的关系 $\sim$ 称为**等价关系** (equivalence relation), 如果下述三性质成立:

(1) (**自反性**) 对所有 $a \in A, a \sim a$.

(2) (**对称性**) 如果 $a \sim b$, 则 $b \sim a$.

(3) (**传递性**) 如果 $a \sim b$ 且 $b \sim c$, 则 $a \sim c$.

定义1.9. 集合 A 作为它的一些子集合的不交并, 称为 A 的一个**分拆** (partition).

设 $\sim$ 是 A 上的一个等价关系. 如 $a \in A$, 记 $[a] = \{b \in A \mid b \sim a\}$, 即 $[a]$ 为 A 中所有与 a 等价的元素构成的子集合, 则

$$[a] \cap [b] = \begin{cases} [a] = [b], & \text{如果} a \sim b, \\ \varnothing, & \text{如果} a \nsim b. \end{cases}$$

故A 可以写为不交并

$$A = \bigsqcup_{a \in A} [a]. \tag{1.6}$$

我们得到 A 的一个分拆. 另一方面, 如果 $A = \bigsqcup_{i\in I} A_i$, 我们很容易在 A 上定义一个等价关系:

$$a \sim b \quad \text{如果} \quad a, b \text{ 属于同一个 } A_i,$$
$$a \nsim b \quad \text{如果} \quad a, b \text{ 属于不同的 } A_i.$$

故我们有如下定理

定理1.10. 集合 A 的分拆与其上的等价关系一一对应.

例1.11. 整数集合 $\mathbb{Z}$ 可以分拆为偶数集合和奇数集合的不交并. 另一方面, 在 $\mathbb{Z}$ 上可以定义等价关系: $a \sim b$ 如果 $a \equiv b \pmod 2$, 故偶数集合是 0 所在的等价类, 奇数集合为 1 所在的等价类.

设 $f : A \to B$ 为集合间的映射. 对于 $b \in B$, 令b 的原像集合 $f^{-1}(b) = \{a \in A \mid f(a) = b\}$. 则 $f^{-1}(b)$ 为 A 的子集, 两两不交, 且 $f^{-1}(b) = \varnothing$ 当且仅当 $b \notin f(A)$. 故我们得到分拆

$$A = \bigsqcup_{b\in f(A)} f^{-1}(b), \tag{1.7}$$

我们称为**集合A 由映射 f 决定的分拆**. 该分拆决定的等价关系即

$$a \sim a' \iff f(a) = f(a').$$

例1.12. 定义映射 $f : \mathbb{Z} \to \{0, 1\}$, 其中 $f(2n) = 0$, $f(2n + 1) = 1$. 则映射 f 决定的等价关系和分拆即与例*1.11* 给出的一致.

例1.13. 设 $f : \mathbb{R}^2 = \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ 为实数减法映射 $(x, y) \mapsto x - y$, 则 $f^{-1}(a)$ 为直线 $y = x - a$. 实平面 $\mathbb{R}^2$ 在映射 f 下是平行直线束 $y = x - a$ $(a \in \mathbb{R})$ 的并, 由此我们得到 $\mathbb{R}^2$ 的一个分拆和对应等价关系.

习　　题

习题1.1. 设B, $A_i (i \in I)$均是集合Ω的子集, 试证:

(1) $B \bigcap (\bigcup_{i\in I} A_i) = \bigcup_{i\in I} (B \bigcap A_i)$.

(2) $B\bigcup(\bigcap_{i\in I}A_i)=\bigcap_{i\in I}(B\bigcup A_i)$.

(3) $(\bigcup_{i\in I}A_i)^c=\bigcap_{i\in I}A_i^c$.

(4) $(\bigcap_{i\in I}A_i)^c=\bigcup_{i\in I}A_i^c$.

习题1.2. 设 $f:A\to B$ 是集合的映射, A 是非空集合. 试证:

(1) f 为单射$\Leftrightarrow$存在 $g:B\to A$, 使得 $g\circ f=1_A$;

(2) f 为满射$\Leftrightarrow$存在 $h:B\to A$, 使得 $f\circ h=1_B$.

习题1.3. 如果 $f:A\to B$, $g:B\to C$ 均是一一对应, 则 $g\circ f:A\to C$ 也是一一对应, 且 $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$.

习题1.4. 证明容斥原理(命题 *1.1*).

习题1.5. 设 A 是有限集, $P(A)$ 是 A 的全部子集 (包括空集) 所构成的集族, 试证 $|P(A)|=2^{|A|}$, 换句话说, n 元集合共有 2^n 个子集.

习题1.6. 设 $f:A\to B$ 是集合间的映射. 在集合 A 上如下定义一个关系: 对任意 $a,a'\in A, a\sim a'$ 当且仅当 $f(a)=f(a')$. 试证这样定义的关系是一个等价关系.

习题1.7. 证明等价关系的三个条件是互相独立的, 也就是说, 已知任意两个等价不能推出第三个条件.

习题1.8. 设 A,B 是两个有限集合.

(1) A 到 B 的不同映射共有多少个?

(2) A 上不同的二元运算共有多少个?

§1.2 群的基本概念和例子

§1.2.1 群的定义和例子

们首先给出群的定义.

定义1.14. 集合 G 及其上的二元运算 $\cdot$ 如果满足下述三条件:

(1) 结合律成立, 即对元素 $a,b,c\in G$, $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.

(2) 存在**单位元** (identity element) $1 = 1_G$, 即对任意 $a \in G$,

$$a \cdot 1 = 1 \cdot a = a.$$

单位元也称为**幺元**.

(3) G 上每个元素 a 均有**逆元** (inverse), 即存在元素 $b \in G$ 使得

$$a \cdot b = b \cdot a = 1.$$

则称 $(G, \cdot)$ 为**群** (group), 二元运算 $\cdot$ 称为**群的乘法** (multiplication).

注记. (1) 习惯上, 我们常常省略乘法运算, 称 G 为群, 且记 $a \cdot b$ 为 ab.

(2) 如果 $(G, \cdot)$ 仅满足结合律, 我们称之为**半群** (semigroup); 如果 $(G, \cdot)$ 满足结合律且存在单位元, 我们称之为**含幺半群** (monoid).

本书中的很大篇幅, 从群论的定义开始, 到有限域的知识, 直至书的最后一章*Galois*理论, 都离不开*200*年前诞生的法国天才数学家埃瓦里斯特 · 伽罗瓦*(Évariste Galois, 1811*年*10*月*25*日 — *1832*年*5*月*31*日, 图 *1.6)* 的伟大工作. 伽罗瓦在不到*21*岁的生命里给数学留下了辉煌一笔. 他奠定了抽象代数两大基本理论*:* 群论和以他命名的*Galois*理论. 这些理论是当代代数和数论研究的基本支柱, 是数学走向抽象化的标志. 他的理论, 完美证明了一般n 次方程根式解不存在, 以及回答了古典几何难题中两大难题*:* 不能用直尺和圆规任意三等分角*;* 素数边正多边形可以用直尺和圆规构造当且仅当该素数是费马素数. 伽罗瓦的工作在生前不被承认, 直到*1843*年才由刘维尔*(Joseph Liouville)* 检查并确认, *1846*年由刘维尔整理在他的杂志*Journal de Mathématiques Pures et Appliquées* 出版.

例1.15. 由群的定义, 群 G 一定包含单位元 1_G. 另一方面, 仅由单位元构成的集合$\{1\}$ 在乘法$1 \cdot 1 = 1$ 下满足群的三个公理, 因此它构成群. 这是最简单的群.

图 1.6: 伽罗瓦像

命题1.16. *设 G 为群, 则下述性质成立:*

(1) *G 中元素的逆元唯一.*

(2) **消去律**成立, *即: 如果 $ab = ac$, 则 $b = c$; 如果 $ba = ca$, 则 $b = c$.*

证明. (1) 如果 b, c 为 $a \in G$ 的逆元, 则

$$b = b \cdot 1 = b(ac) = (ba)c = 1 \cdot c = c.$$

(2) 如果 $ab = ac$, 则 $a^{-1}(ab) = a^{-1}(ac)$, 由结合律即得 $b = c$. □

定义1.17. 如果群 G 的元素个数有限, 称 G 为**有限群** (finite group), 其元素个数称为 G 的**阶** (order). 无限群的阶记为无穷.

定义1.18. 如果群 G 上的乘法运算满足交换律, 我们称 G 为**阿贝尔群** (abelian group), 亦称为**交换群** (commutative group). 我们常常用加法 $+$ 来表示阿贝尔群 G 的二元运算, 并将其上的单位元记为 0 或 0_G, 记 a 的逆元为 $-a$.

图 1.7: 挪威钞票上的阿贝尔像

*19*世纪二十年代的数学天空, 双星闪耀, 其中一位是伽罗瓦, 另外一位就是挪威数学家尼尔斯 · 阿贝尔(*Niels Abel*, *1802*年*8*月*5*日 — *1829*年*4*月*6*日). 阿贝尔和伽罗瓦都是在年纪轻轻的时候做出了数学史上影响深远的结果, 但又都是命途多舛, 英年早逝. 阿贝尔以证明五次方程的根式解的不可能性和对椭圆函数论的研究而闻名. 由于他发现方程的(伽罗瓦)群的交换性可以推出求根公式的存在性, 法国数学家*Camille Jordan* (若当标准型的发现者) 将交换群命名为阿贝尔群. 为纪念阿贝尔, 挪威政府从*2003*年起开始颁发阿贝尔奖, 这是当今数学界的最高荣誉之一. 图 *1.7* 为挪威政府*1978*年发行以阿贝尔像为背景的*500*克朗钞票.

我们首先给出阿贝尔群的一些例子.

例1.19. (1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 在加法运算下构成无限阿贝尔群, 0 为加法单位元.

(2) $\mathbb{Q}^\times = \mathbb{Q} - \{0\}$, $\mathbb{R}^\times = \mathbb{R} - \{0\}$, $\mathbb{C}^\times = \mathbb{C} - \{0\}$ 在乘法运算下构成阿贝尔群, 1 为乘法单位元.

例1.20. 整数集 $\mathbb{Z}$ 模 n 的剩余类集合 $\{\bar{0} = 0 \mod n, \bar{1}, \cdots, \overline{n-1}\}$ 构成加法阿贝尔群, 我们记之为 $\mathbb{Z}/n\mathbb{Z}$. 今后如不特别说明, 在 $\mathbb{Z}/n\mathbb{Z}$ 中, 我们将移除 $^-$, 将 $\bar{a}$ 直接记为a.

特别地, 如果 $n = p$ 是素数, 记 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, 则 $\mathbb{F}_p$ 是加法阿贝尔群. 同时, $\mathbb{F}_p^\times = (\mathbb{F}_p - \{0\}, \times)$ 是乘法阿贝尔群, 这是因为根据整数的同余理论, 如果 $a \not\equiv 0 \mod p$, 则存在 $b \in \mathbb{Z}$, 使得 $ab \equiv 1 \mod p$.

注记. 在上述两个例子中, 我们实际上给出了**域**的几个常见例子: 有理数域 $\mathbb{Q}$, 实数域 $\mathbb{R}$, 复数域 $\mathbb{C}$ 和有限域 $\mathbb{F}_p$. 它们的共同点都是: 本身是加法阿贝尔群, 而其中非零元集合又构成乘法阿贝尔群, 而且加法和乘法满足**分配律**, 即 $(a+b)c = ac+bc$ 对其中任何 3 个元素 a, b, c 均成立. 这些共同点将构成域的定义, 我们将在本书稍后详细阐述. 在此之前, 我们提到的域即是指上述 4 个例子.

例1.21. 令 $\zeta_n = \exp(\frac{2\pi i}{n}) = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, 则集合 $\mu_n = \{1, \zeta_n, \ldots, \zeta_n^{n-1}\}$ 是由复数域 $\mathbb{C}$ 上所有 n 次单位根构成的集合. 在复数乘法意义下, μ_n 是乘法阿贝尔群, 称为 n **次单位根群** (*group of roots of unity*). 更进一步地, 单位圆 $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ 是乘法阿贝尔群.

我们再来看非交换群的例子.

例1.22 (一般线性群)**.** 设 V 是域 F 上的 n 维线性空间, 其中$F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 或 $\mathbb{F}_p$. 由线性代数可知, 取定 V 上的一组基, 则 V 上线性变换由它在这组基下的n 阶方阵唯一确定. 记

$$\mathrm{M}_n(F) = \{F\text{上}n\text{阶方阵}\},$$
$$\mathrm{GL}_n(F) = \{F\text{上}n\text{阶可逆方阵}\}.$$

则 $\mathrm{M}_n(F)$ 在矩阵加法意义下是阿贝尔群, 在乘法意义下是含幺半群, 但不是群. $\mathrm{GL}_n(F)$ 在矩阵乘法意义下构成群, 我们称之为F 上的**一般线性群** (*general linear group*). 如果 $n = 1$, 则 $\mathrm{GL}_n(F) = F^\times$, 即 F 的乘法群, 它是一个交换群; 如果 $n > 1$, 则 $\mathrm{GL}_n(F)$ 不是交换群. 今后如果不强调域 F, 我们记一般线性群为 GL_n.

例1.23. 正四面体$ABCD$ 的旋转群. 考虑所有保持四面体不变的旋转变换, 这里有三种情况.

- 有两个顶点不动, 则剩下两个点也不动, 故为恒等变换.
- 有且仅有一个顶点 A 不动, 则正三角形 BCD 的中心 O 也不动. 旋转变换通过旋转 $\frac{2\pi}{3}$ 或 $\frac{4\pi}{3}$ 将 B, C, D 旋转到 C, D, B 或 D, B, C, 共有两个变换. 将顶点 A 变动, 则得到 $4 \times 2 = 8$ 种旋转变换.

- 如果所有顶点都动, 则若 A 旋转到 B, 则 B 不能旋转到 C 或 D (否则 D 或 C 不动), 即 B 必然旋转到 A. 因此 C 旋转到 D, D 旋转到 C. 即 AB 中点 M 与 CD 中点 N 连接的直线保持不动. 这样的情况共有 3 种.

所有正四面旋转变换在变换复合作为乘法意义下构成群, 恒等变换为单位元. 可以验证第二类变换和第三类变换的复合不交换, 故正四面体的旋转变换群是12 阶非阿贝尔群.

例1.24. 更一般地, 设 S 是一个刚体, 即不可压缩和拉伸的物体. 保持 S 不变的运动构成一个群, 称为 S 的**刚体运动群**. 一般而言它不是阿贝尔群.

例1.25 (对称群)**.** 设 A 为非空集合. 记 A 到自身的映射集合为 M_A. A 到自身的一一对应称为 A 的**置换** (*permutation*). 记A 的所有置换集合为 S_A. 则 M_A 在映射复合作为乘法意义下是含幺半群但不是群, 而 S_A 是群, 其单位元为恒等映射, 我们称 S_A 为 A 的**对称群** (*symmetric group*) 或**置换群** (*permutation group*).

特别地, 设 $A = \{1, 2, \ldots, n\}$, 记 $S_A = S_n$, 则 S_n 为 $\{1, \ldots, n\}$ 所有置换构成的集合. 我们知道 S_n 中含有 $n!$ 个置换. 如果 $n = 2$, 则 $S_2 = \{\mathrm{id}, \tau\}$, 其中 $\tau(1) = 2, \tau(2) = 1$. 容易验证 S_2 为阿贝尔群. 当 $n \geqslant 3$ 时, S_n 不是交换群.

例1.26. 我们来计算一下有限域 $\mathbb{F}_p$ 的一般线性群 $\mathrm{GL}_n(\mathbb{F}_p)$ 的阶.

如果 $A = (a_{ij}) \in \mathrm{GL}_n(\mathbb{F}_p)$, 记$\alpha_i = (a_{ij})_{j=0}^n$ 为A 的第i行行向量. 则 $\alpha_1 \neq 0$, 有$p^n - 1$ 种选择方式; α_2 不在α_1 生成的1维 $\mathbb{F}_p$ 向量空间中, 有$p^n - p$ 种选择方式; 同理对 $2 \leqslant i \leqslant n$, α_i 不在由$\alpha_1, \cdots, \alpha_{i-1}$ 生成的$i-1$维 $\mathbb{F}_p$ 向量空间中, 有$p^n - p^{i-1}$ 种选择方式. 故A 共有 $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$ 可能选择. 故 $\mathrm{GL}_n(\mathbb{F}_p)$ 是有限群, 阶为 $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$.

§1.2.2 子群和群的直积

有了群的概念和例子, 我们希望

(1) 研究群的结构,

(2) 构造更多的群的例子.

这时候, 需要子群与直积的概念.

定义1.27. 设 G 为群. 如果 H 是 G 的子集, 且对 G 的乘法运算构成群, 则称 H 是 G 的**子群** (subgroup), 记为 $H \leqslant G$. 如果 $H \neq G$, 称 H 为 G 的**真子群** (proper subgroup), 记为 $H < G$.

例1.28. 对任意群 G, $\{1\}$ 和 G 均是 G 的子群, 称为 G 的**平凡子群** (*trivial subgroup*).

例1.29. 加法群$n\mathbb{Z}$ 是 $\mathbb{Z}$ 的子群. 乘法群μ_n 和 S^1 是 $\mathbb{C}^\times$ 的子群. $\{\pm 1\}$ 是 $\mathbb{R}^\times$ 的子群.

由定义可知, 要验证 H 为 G 的子群, 只需验证如下三点, 即
(1) $1 \in H$.
(2) 如果 $a \in H$, 则 $a^{-1} \in H$.
(3) 如果 $a, b \in H$, 则 $ab \in H$.

命题1.30. 子集合 H 恰是群 G 的子群当且仅当对任意 $a, b \in H, ab^{-1} \in H$.

证明. 如果 $H \leqslant G, a, b \in H$, 则 $b^{-1} \in H, ab^{-1} \in H$. 反过来, 取 $a = b \in H$, 则 $1 = aa^{-1} \in H$. 取 $a = 1, b = a$, 则 $1 \cdot a^{-1} = a^{-1} \in H$. 取 $a = a, b = b^{-1}$, 则 $a(b^{-1})^{-1} = ab \in H$. 故$H$ 是G 的子群. □

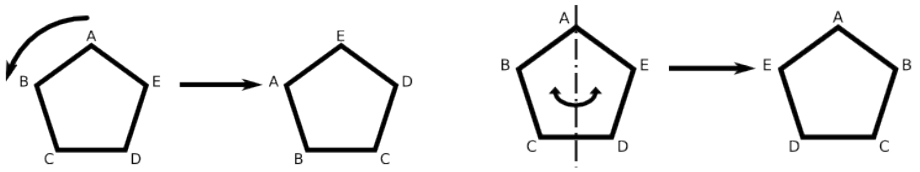
例1.31. 令$H = \left\{ \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \,\middle|\, a \in \mathbb{R} \right\}$, 则$H$ 是一般线性群$\mathrm{GL}_2(\mathbb{R})$ 的子群. 这是因为

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a-b \\ 0 & 1 \end{pmatrix}.$$

例1.32 (二面体群)**.** 设 P 是正 n 边形 $(n \geqslant 3)$, 保持 P 不变的所有刚性变换有两种: 旋转和反射, 如图 *1.8* 所示.

记 D_n 为所有旋转和反射在复合意义下构成的群, 则 D_n 为正 n 边形的对称群, 称为**二面体群** (*dihedral group*). D_n 的所有元素包括: 恒等变换, $n-1$ 个旋转, n 个反射, 故为$2n$ 阶群.

由于保持正n 边形不变的每个刚性变换由它的n 个顶点的置换唯一确定, 故 二面体群D_n 是S_n 的子群.



(a) 旋转 (b) 反射

图 1.8: 正5边形的旋转和反射

注记. 二面体群在不同文献中记为 D_n 或 D_{2n}. 习惯上, 几何学家喜欢用 D_n(强调正多边形的边数), 代数学家喜欢用 D_{2n} (强调正多边形对称群的阶).

定义1.33. 设 G_1, G_2 为群, 则 G_1 与 G_2 (作为集合的) 的笛卡尔积 $G = G_1 \times G_2$ 在乘法运算

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 h_1, g_2 h_2)$$

下构成群: 它的单位元是 $1_G = (1_{G_1}, 1_{G_2})$, 元素 (g_1, g_2) 的逆是 (g_1^{-1}, g_2^{-1}). 群 G 称为 G_1 与 G_2 的**直积** , 或者称为**笛卡尔积**.

注记. (1) 由定义立知群的直积的阶等于群的阶的乘积.

(2) 如果 H_1 和 H_2 分别是 G_1 和 G_2 的子群, 则 $H_1 \times H_2$ 是 $G_1 \times G_2$ 的子群. 特别地, $G_1 \times G_2$ 有子群 $\{1_{G_1}\} \times G_2$ 和 $G_1 \times \{1_{G_2}\}$.

§1.2.3 GL_n 的子群: 典型群

在数学研究中, 最重要的一类群是一般线性群 GL_n 的子群, 称为**典型群** (classical group). 关于典型群的研究和应用贯穿于数学的各个学科分支. 由于一般线性群来自于线性代数, 线性代数知识在研究典型群的时候起着十分重要的作用. 我们下面介绍几类典型群.

(I) **特殊线性群**

设 F 为域, 则 F 上行列式为 1 的 n 阶方阵集合

$$\mathrm{SL}_n(F) = \{A \in \mathrm{GL}(F) \mid \det A = 1\} \tag{1.8}$$

构成 $\mathrm{GL}_n(F)$ 的一个子群, 称为 F 上的 n 阶**特殊线性群** (special linear group). 另外, 我们令

(i) $T_n(F)$ 为对角线元全为 1 的 n 阶上三角阵;

(ii) $\mathrm{Diag}_n(F)$ 为 n 阶可逆对角阵集合;

(iii) $B_n(F)$ 为 n 阶可逆上三角阵集合.

则它们均为 $\mathrm{GL}_n(F)$ 的子群, 且 $T_n(F) \leqslant \mathrm{SL}_n(F)$, $\mathrm{Diag}_n(F) \leqslant B_n(F)$.

在 2阶一般线性群 $\mathrm{SL}_2(\mathbb{R})$ 中, 所有整系数矩阵构成子群 $\mathrm{SL}_2(\mathbb{Z})$, 即 $\mathbb{Z}$ **上的 2 阶特殊线性群**. 类似地, 设 N 为大于 1 的正整数. 我们仍然可以在 $\mathbb{Z}/N\mathbb{Z}$ 系数的 2 阶矩阵上定义行列式, 其中行列式为 1 的矩阵的集合

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, a,b,c,d \in \mathbb{Z}/N\mathbb{Z},\ ad-bc=1 \right\} \tag{1.9}$$

以矩阵乘法作为乘法, 就构成 $\mathbb{Z}/N\mathbb{Z}$ **上的 2 阶特殊线性群**. 当阶数 2 换成一般的 n 时, 我们就得到 $\mathbb{Z}$ 上和$\mathbb{Z}/N\mathbb{Z}$ 上的特殊线性群.

(II) **正交群与特殊正交群**

在 $\mathbb{R}^n$ 上给定标准内积

$$\langle X, Y \rangle = X^T Y,$$

其中 ^{T}表示转置, 则 R^n 成为欧几里得空间. 方阵 A 称为**正交方阵**(orthogonal matrix) 或**正交阵**, 是指 A 保持 $\mathbb{R}^n$ 上的标准内积不变, 即对任意 $X, Y \in \mathbb{R}^n$,

$$\langle AX, AY \rangle = X^T A^T A Y = X^T Y,$$

亦即

$$A^T A = A A^T = I. \tag{1.10}$$

由此我们知道: (i) 单位矩阵是正交阵; (ii) 正交阵的乘积是正交阵; (iii) 正交阵的逆也是正交阵. 因此所有正交方阵的集合

$$\mathrm{O}_n(\mathbb{R}) := \{ A \in \mathrm{GL}_n(\mathbb{R}) \mid A^T A = A^T A = I \} \tag{1.11}$$

构成一个群, 即 $\mathbb{R}$ 上的 n 阶**正交群** (orthogonal group). 更一般地, 设 Q 为 n 维实空间 V 上非退化对称双线性型. 由惯性定理, 存在 V 上一组基使得 Q 由如下形式给出:

$$Q(u,v) = X^T \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix} Y \quad (p+q=n),$$

其中 X, Y 为向量 u, v 在此基下的坐标. 所有保持双线性型 Q 不变的可逆方阵的集合

$$\mathrm{O}_{p,q}(\mathbb{R}) := \left\{ A \in \mathrm{GL}_n(\mathbb{R}) \mid A^T \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix} A = \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix} \right\} \tag{1.12}$$

也构成群, 称为**广义正交群** (generalized orthogonal group). 我们称

$$\mathrm{SO}_n(\mathbb{R}) := \mathrm{O}_n(R) \cap \mathrm{SL}_n(\mathbb{R}), \tag{1.13}$$

$$\mathrm{SO}_{p,q}(\mathbb{R}) := \mathrm{O}_{p,q}(R) \cap \mathrm{SL}_n(\mathbb{R}) \tag{1.14}$$

为**特殊正交群** (special orthogonal group) 和**广义特殊正交群** (generalized special orthogonal group).

例1.34. 当 $n = 2$ 时, 我们有

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \;\middle|\; \theta \in \mathbb{R} \right\},$$

$$\mathrm{O}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \pm\sin\theta & \pm\cos\theta \end{pmatrix} \;\middle|\; \theta \in \mathbb{R} \right\}.$$

更进一步地, 对一般的域 F, 设 Q 为域F 上 n 维线性空间 V 上的非退化对称双线性型, 我们可以类似定义 F 上保持双线性型 Q 不变的正交群和特殊正交群.

(III) **酉群和特殊酉群**

设 V 是 n 维复线性空间, Q 是 V 上非退化Hermite 双线性型, 则存在 V 的一组基, 使得 Q 在此基下可表示如下:

$$Q(u, v) = Q(X, Y) = \overline{X}^T Y.$$

方阵 A 称为**酉阵** (unitary matrix) 是指它保持 Q 不变, 即 A 满足

$$\overline{A}^T A = A\overline{A}^T = I. \tag{1.15}$$

由此我们知道: (i) 单位矩阵是酉阵; (ii) 酉阵的乘积是酉阵; (iii) 酉阵的逆也是酉阵. 因此

$$\mathrm{U}(n) := \{ A \mid \overline{A}^T A = A\overline{A}^T = I \} \tag{1.16}$$

是 $\mathrm{GL}_n(\mathbb{C})$ 的一个子群, 称为**酉群** (unitary group). 它的子群

$$\mathrm{SU}(n) = U(n) \cap \mathrm{SL}_n(\mathbb{C}), \tag{1.17}$$

称为**特殊酉群** (special unitary group).

例1.35. 当 $n = 1$ 时, $\mathrm{U}(1) = S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$, $\mathrm{SU}(1) = \{1\}$.

当 $n = 2$ 时,

$$\mathrm{SU}(2) = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1 \right\}.$$

(IV) **辛群**

设 V 是实线性空间, $Q(x, y)$ 是 V 上的非退化反对称双线性型. 由 Q 的非退化性, 我们知 $\dim V = 2n$ 为偶数, 且存在 V 的一组基使得

$$Q(u, v) = X^T \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} Y,$$

其中 X, Y 为 u, v 在基下的坐标. 所有保持 Q 不变的方阵的集合, 即为群

$$\mathrm{Sp}_{2n}(\mathbb{R}) = \left\{ A \mid A^T \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} A = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \right\}, \tag{1.18}$$

称为**辛群** (symplectic group).

注记. 如果 $A \in \mathrm{Sp}_{2n}(\mathbb{R})$, 可以证明 $\det A = 1$, 故没有特殊辛群的说法.

§1.2.4 群的同态与同构

研究群的性质, 离不开研究群与其它群的关系, 这些关系如同研究集合间的关系一样, 是由群之间的映射来决定的. 但必须注意到, 群不仅是集合, 它上面有乘法运算, 故群与群之间的映射应该保持乘法运算. 我们有如下的定义.

定义1.36. 设 G_1 与 G_2 为群, 映射 $f : G_1 \to G_2$ 称为**群同态** (homomorphism) 是指对任意 $g, h \in G_1$,

$$f(gh) = f(g)f(h).$$

(注意到上式左边 $g \cdot h$ 是群 G_1 中的乘法运算, 右边 $f(g) \cdot f(h)$ 是 G_2 中的乘法运算.)

如 f 作为集合映射为单射, 称 f 为**单同态** (epimorphism). 如 f 为满射(epimorphism), 称 f 为**满同态**. 如 f 为双射, 则称 f 为**同构** (isomorphism), 记为 $f: G_1 \cong G_2$.

命题1.37. 设$f: G_1 \to G_2$ 为群同态, 则

(1) 群同态总是将单位映到单位, 即$f(1_{G_1}) = 1_{G_2}$.

(2) 群同态总是将逆元映到逆元, 即对于$g \in G_1$, $f(g^{-1}) = f(g)^{-1}$.

证明. 由$f(1_{G_1}) = f(1_{G_1} \cdot 1_{G_1}) = f(1_{G_1}) \cdot f(1_{G_1})$, 再由消去律即得(1).

若$g \in G_1$, 则

$$f(g) \cdot f(g^{-1}) = f(g \cdot g^{-1}) = f(1_{G_1}) = 1_{G_2},$$

故 $f(g^{-1}) = f(g)^{-1}$, (2) 得证. □

我们来看一些群同态和同构的例子.

例1.38. 如果H 是G 的子群, 则包含映射$i: H \to G$, $h \mapsto h$ 为群同态, 且是单同态.

例1.39. 行列式映射 $\det: \mathrm{GL}_n(F) \to F^\times$, $A \mapsto \det A$ 是群的满同态.

例1.40. 我们定义 $\varphi: \mathbb{Z}/n\mathbb{Z} \to \mu_n$, $\bar{m} = m \mod n \mapsto \zeta_n^m$, 则 φ 是群同构.

例1.41. 对于 $\sigma \in S_n$, 我们定义 $A_\sigma \in \mathrm{GL}_n$ 如下

$$A_\sigma \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}(1)} \\ x_{\sigma^{-1}(2)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{pmatrix},$$

则 $A_\sigma = (a_{ij})$ 为 $(0,1)$ 矩阵, 且

$$a_{ij} = \begin{cases} 1 & 若 j = \sigma^{-1}(i), \\ 0 & 若不然. \end{cases}$$

映射 $\sigma \mapsto A_\sigma$ 为 S_n 到 GL_n 的单同态. 由此我们可以视对称群 S_n 为一般线性群 GL_n 的子群, A_σ 也称为**置换矩阵**.

例1.42. 酉群$S^1 = \mathrm{U}(1)$ 和特殊正交群 $\mathrm{SO}_2(\mathbb{R})$ 同构, 同构映射为

$$e^{2\pi i\theta} \mapsto \left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right).$$

例1.43. 设$\mathbb{R}_+^\times$ 为所有正实数构成的乘法群, 则指数函数

$$\exp:\ \mathbb{R} \to \mathbb{R}_+^\times, \quad x \mapsto e^x$$

是群同构. 其逆为对数函数

$$\log = \ln:\ \mathbb{R}_+^\times \to \mathbb{R},\ y \mapsto \ln y.$$

在群论研究中, 经常会将同构视为相同, 或者说在同构意义下一样. 另一方面, 也会问及同构群之间可以构造多少种同构. 我们有

定义1.44. 群同态如是群 G 到自身的同构, 则称为 G 的**自同构** (automorphism).

命题1.45. (1) 群 G 的所有自同构在复合映射作为乘法下构成群, 称为 G 的**自同构群**, 记为 $\mathrm{Aut}G$.

(2) 如 $\varphi: G \to H$ 为 G 到 H 同构. 则 G 到 H 的所有同构为 $\varphi\mathrm{Aut}G = \{\varphi \circ f \mid f \in \mathrm{Aut}G\}$.

证明. (1) 只需验证群论3公理即可, 而这些都是显然的.

(2) 首先, $\varphi \circ f : G \xrightarrow{f} G \xrightarrow{\varphi} H$ 为 G 到 H 的同构. 另一方面, 如 φ' 为 $G \to H$ 的同构, 则 $\varphi^{-1} \circ \varphi' : G \to H \to G$ 为 G 的自同构. 故 $\varphi' = \varphi \circ (\varphi^{-1} \circ \varphi') \in \varphi\mathrm{Aut}G$. □

习 题

习题2.1. 令 A 是任意一个集合, G 是一个群, $\mathrm{Map}(A, G)$ 是 A 到 G 的所有映射的集合, 对任意两个映射 $f, g \in \mathrm{Map}(A, G)$, 定义乘积 fg 是这样的映射: 对任意 $\alpha \in A$, $fg(\alpha) = f(\alpha)g(\alpha)$. 试证 $\mathrm{Map}(A, G)$ 是群.

习题2.2. 从平面到自身的函数如果保持平面上任何两点的距离, 则称为**保距映射**. 证明保距映射都是双射, 且所有保距映射在函数复合意义下构成群.

习题2.3. 设G 是群, $x, y \in G$. 证明: $(x^{-1})^{-1} = x$ 且 $(xy)^{-1} = y^{-1}x^{-1}$.

习题2.4. 判断下面哪些2 阶方阵集合在矩阵乘法意义下构成群:

(1) $\left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$, $ac \neq b^2$.

(2) $\left(\begin{smallmatrix} a & b \\ c & a \end{smallmatrix}\right)$, $a^2 \neq bc$.

(3) $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$, $ac \neq 0$.

(4) $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $a, b, c, d \in \mathbb{Z}$, $ad \neq bc$.

习题2.5. 证明集合$\bigcup_{n\geq 1} \mu_n$ 在复数乘法意义下构成群.

习题2.6. 如果 A 是群 G 的子群, B 是群 H 的子群, 证明$A \times B$ 是$G \times H$ 的子群. 举例说明不是所有 $\mathbb{Z} \times \mathbb{Z}$ 的子群都是如此得到的.

习题2.7. 设 $(G, \cdot)$ 是群. 证明 $G^{\mathrm{op}} = (G, \circ)$, $a \circ b = b \cdot a$ 是一个群, 称为 G 的**反群**.

习题2.8. 设 G 是一个含幺半群, 证明 G 中的可逆元集合 $G^\times$ 构成群.

习题2.9. 令 G 是 n 阶有限群, $a_1, a_2, \ldots, a_n$ 是群 G 的任意 n 个元素, 不一定两两不同. 试证: 存在整数 p 和 q, $1 \leqslant p \leqslant q \leqslant n$, 使得

$$a_p a_{p+1} \cdots a_q = 1.$$

习题2.10. 在偶数阶群 G 中, 方程 $x^2 = 1$ 总有偶数个解.

习题2.11. (1) 验证 $\mathrm{SL}_n(F)$, $T_n(F)$, $\mathrm{Diag}_n(F)$, $B_n(F)$ 均为 $\mathrm{GL}_n(F)$ 的子群, 且 $T_n(F) \leqslant \mathrm{SL}_n(F)$, $\mathrm{Diag}_n(F) \leqslant B_n(F)$.

(2) 验证 $\mathrm{O}_n(\mathbb{R})$, $\mathrm{O}_{p,q}(\mathbb{R})$, $\mathrm{Sp}_{2n}(\mathbb{R})$ 均为 $\mathrm{GL}_n(\mathbb{R})$ 的子群.

(3) 验证 $\mathrm{U}(n)$ 是 $\mathrm{GL}_n(\mathbb{C})$ 的子群.

习题2.12. 试证群 G 的任意多个子群的交仍是 G 的子群.

习题2.13. 设 A 和 B 分别是群 G 的两个子群. 试证: $A \cup B$ 是 G 的子群当且仅当 $A \leqslant B$ 或 $B \leqslant A$. 利用这个事实证明: 群 G 不能表为两个真子群的并.

习题2.14. 设 A, B 是群 G 的两个子群. 试证 AB 是 G 的子群当且仅当 $AB = BA$.

习题2.15. 设 A 和 B 是有限群 G 的两个非空子集. 若 $|A|+|B|>|G|$, 证明 $G=AB$. 特别地, 如果 S 是 G 的一个子集, $|S|>|G|/2$. 证明对任意 $g\in G$, 存在 $a,b\in S$ 使得 $g=ab$.

习题2.16. (1) 确定 $\mathbb{Z}$ 的所有子群.

(2) 确定 $\mathbb{Z}/n\mathbb{Z}$ 的所有子群, 其中 $n\in\mathbb{N}, n\geqslant 2$.

习题2.17. 证明: 映射 $f:G\to G,\ a\mapsto a^{-1}$ 是 G 的自同构当且仅当 G 是阿贝尔群.

习题2.18. 设 G_1,G_2,G_3 为群, 证明:

(1) $G_1\times G_2\cong G_2\times G_1$;

(2) $(G_1\times G_2)\times G_3\cong G_1\times(G_2\times G_3)$.

习题2.19. 对下面每一情形, 确定 G 是否同构于 H 和 K 的积.

(1) $G=\mathbb{R}^\times,\ H=\{\pm 1\},\ K=\mathbb{R}_+^\times$.

(2) $G=B_n(F),\ H=\mathrm{Diag}_n(F),\ K=T_n(F)$.

(3) $G=\mathbb{C}^\times,\ H=S^1,\ K=\mathbb{R}_+^\times$.

习题2.20. 证明有理数加法群 $\mathbb{Q}$ 和乘法群 $\mathbb{Q}^\times$ 不同构.

习题2.21. (1) 令 G 是实数对 $(a,b), a\neq 0$ 的集合. 在 G 上定义

$$(a,b)(c,d)=(ac,ad+b).$$

试证 G 是群.

(2) 证明 G 同构于 $\mathrm{GL}_2(\mathbb{R})$ 的子群

$$H=\left\{\left(\begin{smallmatrix}a & b\\ & 1\end{smallmatrix}\right)\mid a\in\mathbb{R}^\times, b\in\mathbb{R}\right\}$$

习题2.22. 群 G 的自同构 α 称为没有不动点, 是指对 G 的任意元素 $g\neq 1$, $\alpha(g)\neq g$. 如果有限群 G 具有一个没有不动点的自同构 α 且 $\alpha^2=1$, 证明 G 一定是奇数阶阿贝尔群.

习题2.23. (1) 设 G 是奇数阶有限群, $\alpha\in\mathrm{Aut}(G)$ 且 $\alpha^2=1$. 令

$$G_1=\{g\in G\mid \alpha(g)=g\},\quad G_{-1}=\{g\in G\mid \alpha(g)=g^{-1}\}.$$

证明: $G = G_1G_{-1}$ 且 $G_1 \cap G_{-1} = 1$.

(2) 设 G 满足对任意 $g \in G$, 存在 $h \in G$ 使得 $h^2 = g$, 则上述结论仍然成立. 由此证明:

(i) 任何 F 上的矩阵可以写成对称阵和反对称阵之和, 其中 $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(ii) 任何函数 $f : \mathbb{R} \to \mathbb{R}$ 可以写成奇函数和偶函数之和.

§1.3 子群与陪集分解

在上面一节我们给出了群与子群的定义与具体例子. 在本节, 我们假设 G 为任意(抽象)群, 我们来研究它上面的子群与它自身的关系.

§1.3.1 元素的阶与循环群

定义1.46. 设 G 是群, g 是 G 中的元素, 由 g **生成的子群**即是包含 g 的最小子群. 我们用 $\langle g \rangle$ 来表示它. 同样, 如 $S \subseteq G$ 为 G 的子集合, 则由 S 中元素生成的子群称为 S **生成的子群**, 记为 $\langle S \rangle$.

我们首先讨论 $\langle g \rangle$ 中的元素, 由群的公理, 它必包含

(i) $g^k = g \cdots g$, k 个 g 相乘.

(ii) $1 = g^0$.

(iii) $g^{-k} = g^{-1} \cdots g^{-1}$, k 个 g^{-1} 相乘.

另一方面, 由(i),(ii),(iii)的所有元素构成的集合的确是 G 的子群. 故

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}, \text{ 此处 } g^k \text{ 可能相同.}$$

定义1.47. 群 G 中元素 g 的**阶**是指满足 $g^k = 1$ 的最小正整数, 此时称 g 为 k **阶有限元**. 如这样的 k 不存在, 称 g 的阶为无穷大, 此时称 g 为**无限阶元**.

引理1.48. 如 g 为 k 阶有限元, 则 $g^n = 1$ 当且仅当 $n \equiv 0 \mod k$, $g^i = g^j$ 当且仅当 $i \equiv j \mod k$. 此时, g 生成的子群 $\langle g \rangle = \{1, g, \ldots, g^{k-1}\}$ 是k 阶有限群.

如 g 为无限元, 则对于整数$i \neq j$, 均有 $g^i \neq g^j$.

证明. 如 g 为 k 阶有限元, 设 $n = kq + r$, $0 \leq r < k$. 如 $r \neq 0$, 则 $g^r \neq 1$. 故 $g^n = g^{kq+r} = (g^k)^q \cdot g^r = g^r \neq 1$. 如 $r = 0$, 则 $g^n = g^{kq} = 1$. 综上即证明了 $g^n = 1$ 当且仅当 $n \equiv 0 \mod k$. 由于 $g^i = g^j$ 当且仅当 $g^{i-j} = 1$, 故也等价于 $i \equiv j \mod k$. 由于对任意 n, $n = kq + r$, $g^n = g^r$, 而$1, g, \cdots, g^{k-1}$ 两两不同, 故 $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} = \{1, g, \ldots, g^{k-1}\}$.

当 g 为无限阶元时, $g^i = g^j \Leftrightarrow g^{i-j} = 1 \Leftrightarrow i - j = 0$, 即 $i = j$. □

定义1.49. 如 $G = \langle S \rangle$, 称 G 由 S 生成. 如 S 为有限集, 称 G 为**有限生成群** (finitely generated). 特别地, 如 G 由一个元素 g 生成, 称 G 为**循环群** (cyclic group), g 为 G 的一个**生成元** (generator).

由定义知循环群必是交换群. 更进一步地, 我们有

定理1.50. *设 G 为循环群.*

(1) *如 G 为有限群, 其阶为 n, 则 $G \cong \mathbb{Z}/n\mathbb{Z}$.*

(2) *如 G 为无限群, 则 $G \cong \mathbb{Z}$.*

证明. 设 g 为 G 的生成元. 定义

$$\varphi : \mathbb{Z} \to G,\ k \mapsto g^k.$$

易知 φ 为满同态.

当 G 为无限群时, 由引理 1.48, 如 $i \neq j$, 则 $g^i \neq g^j$, 故 φ 为单同态. 因此 φ 为同构.

当 G 为 n 阶有限群时, φ 诱导同态 $\mathbb{Z}/n\mathbb{Z} \to G$, $k \mod n \mapsto g^k$. 由引理 1.48, 此同态既单又满, 故为同构. □

定理1.51. *设 G 为循环群, g 为 G 的生成元, 则*

(1) *如 G 为无限群, 则 G 的生成元为 g 或 g^{-1}.*

(2) *如 G 为 n 阶有限群, 则 G 的生成元集合为*

$$\{g^k \mid 0 \leq k < n, (k, n) = 1\}.$$

(3) *G 的自同构群*

$$\mathrm{Aut}G \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{如 } G \text{ 为无限群;} \\ (\mathbb{Z}/n\mathbb{Z})^\times, & \text{如 } G \text{ 为 } n \text{ 阶有限群,} \end{cases}$$

且 G 的每个自同构将生成元映为生成元.

证明. (1)和(2): 元素$h = g^a$ 是 G 的生成元当且仅当 $g = h^b$ 对某个 $b \in \mathbb{Z}$ 成立. 故 $g^{ab} = g$. 如 G 为无限群, 则 $ab = 1$, 故 $a = \pm 1$, 即 $h = g$ 或 g^{-1}. 如果 G 的阶为 n, 则 $ab \equiv 1 \mod n$, 所以 $(a, n) = 1$.

(3): 如 $f : G \to G$ 为自同构, g 为生成元, 则 $G = \{f(g^k) = f(g)^k \mid k \in \mathbb{Z}\}$, 故 $f(g)$ 也是G 的生成元. 我们定义映射 φ 如下:

(i) 如 G 为无限群,

$$\varphi : \mathrm{Aut}G \to \{\pm 1\}, \quad f \mapsto \begin{cases} 1, & \text{如 } f(g) = g; \\ -1, & \text{如 } f(g) = g^{-1}. \end{cases}$$

(ii) 如 G 的阶为n,

$$\varphi : \mathrm{Aut}G \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad f \mapsto a \mod n \text{ 如 } f(g) = g^a.$$

则 φ 既单又满, 且 $\varphi(f_1 f_2) = \varphi(f_1) \cdot \varphi(f_2)$, 即 φ 为群同构. □

以下我们设 G 是 n 阶循环群. 固定它的一个生成元 g. 则对于任何元素 $a \in G$, 存在整数 k 使得 $a = g^k$, 且所有满足条件的 k 构成模 n 的一个同余类. 我们定义

$$\log_g : \ G \to Z/n\mathbb{Z}, \quad a \mapsto k, \tag{1.19}$$

这是循环群之间的同构, 即有

$$\log_g 1 = 0, \quad \log_g(ab) = \log_g(a) + \log_g(b). \tag{1.20}$$

我们称 $k = \log_g a$ 为 a 关于 g 的**离散对数** (discrete logarithm). 数学在信息安全应用中最重要的一个核心问题就是

问题1.52 (离散对数问题)**.** *已知循环群 G的阶和生成元 g. 对元素 $a \in G$, 如何求 a 关于 g 的离散对数?*

命题1.53. *设G 为n 阶循环群, g 是G 的一个生成元, $a \in G$. 则方程$x^k = a$ 在G 中有解当且仅当$d = (k, n) \mid \log_g a$. 且当此条件成立时, 方程共有d 个解.*

证明. 设$x = g^y$. 则方程$x^k = a$ 有解等价于存在y, 使得$g^{ky} = g^{\log_g a}$, 即$ky \equiv \log_g a \mod n$ 有解. 根据整数同余理论即知, 方程$x^k = a$ 在G 中有解当且仅当$d = (k, n) \mid \log_g a$.

当$d \mid \log_g a$ 时. 同余方程$ky \equiv \log_g a \mod n$ 的解为$y \equiv \frac{\log_g a}{d} c \mod \frac{n}{d}$, 其中$c$ 为$\frac{k}{d}$ 模$\frac{n}{m}$ 的逆, 故$x^k = a$ 有d 个解g^y, 其中$y = \frac{c \log_g a + in}{d}$ $(0 \leq i < d)$. □

§1.3.2 陪集和陪集分解

设 H 是群 G 的子群.

定义1.54. 对于 $a \in G$, 集合 $aH = \{ah \mid h \in H\}$ 称为 G 关于 H 的**右陪集** (right coset), $Ha = \{ha \mid h \in H\}$ 称为 G 关于 H 的**左陪集** (left coset).

引理1.55. *陪集 aH 与 bH 要么不交, 要么重合. 且 $aH = bH$ 当且仅当 $b^{-1}a \in H$ (或 $a^{-1}b \in H$). 同理 Ha 与 Hb 要么不交, 要么重合. 且 $Ha = Hb$ 当且仅当 ab^{-1} 或 $ba^{-1} \in H$.*

证明. 如 $aH \cap bH \neq \varnothing$. 令 $ah_1 = bh_2$, 则 $b^{-1}a = h_2 h_1^{-1} \in H$. 此时

$$ah = ah_1(h_1^{-1}h) = bh_2(h_1^{-1}h) \in bH,$$

$$bh = bh_2(h_2^{-1}h) = ah_1(h_2^{-1}h) \in aH,$$

故 $aH = bH$. 同理可得左陪集情形. □

由引理 1.55, 设 $\{a_i H \mid i \in I\}$ 为 G 关于 H 的所有右陪集构成的集合, 即$a_i H$ 过所有G 关于H 的右陪集, 且两两不交. 则

$$G = \bigsqcup_{i \in I} a_i H \tag{1.21}$$

为 G 的一个分拆.

定义1.56. $\{a_i \mid i \in I\}$ 称为 G 的一个**右陪集代表元系** (right coset representatives).

同理, 如 $\{Hb_j \mid j \in J\}$ 为 G 关于 H 的所有左陪集构成的集合, 则 $\{b_j \mid j \in J\}$ 称为 G 的一个**左陪集代表元系**. 注意到, $\{b_j \mid j \in J\}$ 为左陪集代表元系当且仅当

$$G = \bigsqcup_{j\in J} Hb_j \tag{1.22}$$

为 G 的分拆.

引理1.57. *如果 $\{a_i \mid i \in I\}$ 是 G 关于 H 的左(右)陪集代表元系, 则 $\{a_i^{-1} \mid i \in I\}$ 是 G 关于 H 的右(左)陪集代表元系. 特别地, 如 G 关于 H 的左或右陪集代表元系有限, 则左、右陪集代表元系均有限, 且阶数相同.*

证明. 因为作为集合

$$(aH)^{-1} = \{(ah)^{-1} \mid h \in H\} = \{h^{-1}a^{-1} \mid h \in H\} = Ha^{-1}.$$

故引理得证. □

定义1.58. 群 G 关于子群 H 的**指数** (index) $(G : H)$ 是指 G 关于 H 的陪集代表元的个数. 如陪集代表元个数无限, 我们规定 $(G : H)$ 等于 ∞.

定理1.59 (拉格朗日定理)**.** *如 G 为有限群, 则*

$$|G| = |H| \cdot (G : H) \tag{1.23}$$

注记. 如果规定 $\infty \cdot$ 正整数 $= \infty \cdot \infty = \infty$, 则 G 为无限群时(1.23)也成立.

证明. 由(1.21), 我们有

$$|G| = \sum_{i\in I} |a_i H| = \sum_{i\in I} |H| = |H| \cdot |I| = |H| \cdot (G : H).$$

定理得证. □

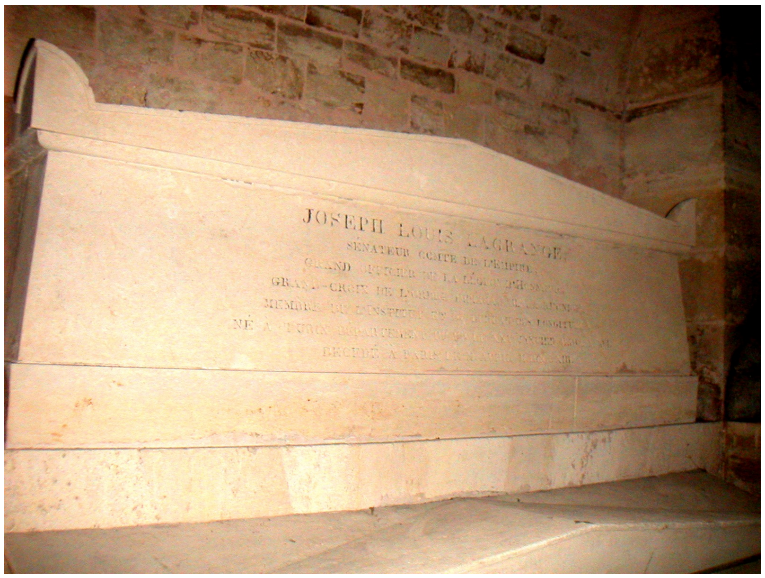


图 1.9: 拉格朗日之墓

约瑟夫-路易·拉格朗日(*Joseph-Louis Lagrange*, *1736*年*1*月*25*日 – *1813*年*4*月*10*日) 是法国籍意大利裔数学家和天文学家, 在数学, 物理和天文等领域做出了很多重大的贡献, 他的成就包括我们熟知的微积分拉格朗日中值定理。在文章 *Réflexions sur la résolution algébrique des équations* 中, 拉格朗日说明如果将 n 元多项式的 n 个变量用所有 $n!$ 个置换作用, 得到的多项式个数总是 $n!$ 的因子. 这个数实际上就是多项式的稳定子群 H 在对称群 S_n 的指数, 即陪集分解的个数. 这就是拉格朗日定理的起源. 附图 *1.9*是巴黎先贤祠(*Pantheon*) 中拉格朗日墓.

拉格朗日定理是群论中第一个重要定理, 它有很多重要推论.

推论1.60. 设 G 为有限群, $x \in G$, 则 $x^{|G|} = 1$, 即元素 x 的阶总是群 G 的阶的因子.

证明. 这是由于元素x 的阶等于子群$\langle x\rangle$ 的阶. □

推论1.61. 素数阶群均是循环群.

证明. 设 $g \neq 1, g \in G$, 则 g 的阶必为 p. 故 $G = \{1, g, \ldots, g^{p-1}\} \cong \mathbb{Z}/p\mathbb{Z}$. □

图 1.10: 费马的墓碑

推论1.62 (费马小定理)**.** 设 p 是素数, 则对所有与 p 互素的整数 a,

$$a^{p-1} \equiv 1 \mod p.$$

证明. 这是由于 $a \in \mathbb{F}_p^\times$ 的阶整除$\mathbb{F}_p^\times$ 的阶 $p-1$. □

皮埃尔 · 德 · 费马(*Pierre de Fermat, 1601*年*8*月*17*日 — *1665*年*1*月*12*日), 是最伟大的业余数学家, 他对数论, 微积分, 解析几何和概率论的建立都卓有贡献. 在数论上费马大定理众所周知, 但费马小定理有着更多的实际应用. 用群论的观点而言, 费马小定理及其推广形式欧拉定理都是拉格朗日定理的推论. 在费马的墓碑(图 *1.10*) 上, 刻着如下文字*:* "在此处于*1865*年*1*月*13*日安葬了皮埃尔 · 德 · 费马, *Edit*市议会议员和杰出数学家, 因他的定理 $a^n + b^n \neq c^n$ $(n > 2)$ 而闻名于世. "

推论1.63. 设 G 为 n 阶循环群, 则对于任意 $d \mid n, d \geq 1$, G 中有唯一 d 阶循环群 $\{1, x^{\frac{n}{d}}, \ldots, x^{\frac{n}{d}(d-1)}\}$, 其中 x 为 G 的生成元. 此子群也是循环群.

证明. 首先易验证 $\{1, x^{\frac{n}{d}}, \ldots, x^{\frac{n}{d}(d-1)}\}$ 是 G 的 d 阶循环子群. 另一方面, 设 H 是G 的 d 阶子群, $y \in H$. 记 $y = x^a$, 由于 y 的阶数整除 d, 故 $y^d = x^{ad} = 1$. 所以 $ad = kn$, $y = x^{\frac{n}{d}k}$. □

推论1.64. *对于任意正整数 n, 有下列恒等式:*

$$n = \sum_{1 \le d \mid n} \varphi(d). \tag{1.24}$$

证明. 我们对 n 阶循环群的元素按阶分类, 则阶为 d 的元素生成唯一的 d 阶循环子群. 由于 d 阶循环群中共有 $\varphi(d)$ 个生成元(定理 1.51), 故恰有 $\varphi(d)$ 个元素阶为 d. 故 $n = \sum_{d \mid n} \varphi(d)$. □

引理1.65. *如果群 G 中任何元素 x 的阶为 1 或者 2, 则 G 为阿贝尔群.*

证明. 由于 x 的阶为 1 或 2, 则 $x = x^{-1}$, 故对 $a, b \in G$,

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

因此 G 为阿贝尔群. □

例1.66. *我们来讨论一下 4 阶群 G 的情况. 如果 G 中包含 4 阶元, 则必为循环群. 否则它的元素的阶均是 1 或者 2, 故它是阿贝尔群, 故必为 $\{1, a, b, ab\}$ 的形式, 其中 $a^2 = b^2 = 1$ 且 $ab = ba$. 则 G 与 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 通过映射 $a \mapsto (1, 0)$, $b \mapsto (0, 1)$ 同构. 我们记 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = K_2$, 称为* ***Klein*** *群.*

菲利克斯 · 克莱因(*Felix Klein, 1849*年*4*月*25*日– *1925*年*6*月*22*日, 图 *1.11*) 以恢复了哥廷根在世界数学的统治地位而闻名于世, 他将哥廷根大学建设成为*19*世纪末到上个世纪*30*年代世界数学的中心. 但毋庸置疑, 他*1872*年发表的爱尔兰根纲领(*Erlangen Program*) 对于数学研究的影响尤其深远, 其中克莱因开创性的思想是: 几何学分类由它的变换群决定. 从此以后对称群的思想走进几何和物理研究的前沿. 值得说明的是, *100*年后领导数学研究前沿的朗兰兹纲领(*Langlands Program*) 也离不开克莱因与庞加莱对于模函数和自守函数的开创性工作.

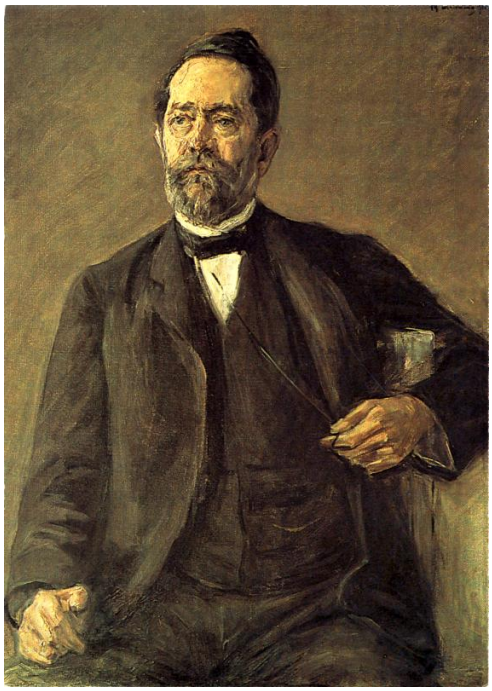


图 1.11: 克莱因像

定理1.67. 非阿贝尔群的最小阶数为 6.

证明. 如果 G 的阶为 $2, 3, 5$, 即为素数, 故由推论 1.61, G 为阿贝尔群. 如 G 的阶是4, 上面例子说明 G 为阿贝尔群. 我们知道 S_3 的阶为 6 且它不是阿贝尔群. 综上所述,非阿贝尔群的最小阶数为 6. □

由于Lagrange 定理只是 G 关于 H 的陪集分解的一个推论, 直接使用陪集分解公式

$$G = \bigsqcup_{i \in I} g_i H, \tag{1.25}$$

我们有更进一步的应用.

定理1.68. 设群 $K \leqslant H \leqslant G$, 且 $(G : K)$ 有限, 则

$$(G : K) = (G : H) \cdot (H : K).$$

注记. Lagrange 定理, 即为上述定理在 $K = \{1\}$, G 为有限群的特殊情形.

证明. 设G 关于H 以及H 关于K 的左陪集分解分别为

$$G = \bigsqcup_{i\in I} g_i H, \qquad H = \bigsqcup_{j\in J} h_j K.$$

则

$$G = \bigcup_{(i,j)\in I\times J} g_i h_j K.$$

更进一步, 如果 $g_i h_j K = g_{i'} h_{j'} K$, 则 $g_i H \cap g_{i'} H \neq \emptyset$, 所以 $i = i'$, 故 $h_j K = h_{j'} K$, 所以 $j = j'$. 即

$$G = \bigsqcup_{(i,j)\in I\times J} g_i h_j K,$$

为不交并, 故 $\{g_i h_j : i \in I, j \in J\}$ 为 G 关于 K 的左陪集分解, 所以

$$(G : K) = (G : H) \cdot (H : K).$$

定理得证. □

定理1.69. *设 G 为有限群, H 与 K 为 G 的子群, 则*

(1) $|H| \cdot |K| = |HK| \cdot |H \cap K|$.

(2) $(G : H \cap K) \leqslant (G : H)(G : K)$, *且等号成立当且仅当$HK = G$. 如果 $(G : H)$ 与 $(G : K)$ 互素, 则等号成立.*

证明. 首先证明(2). 注意到(2) 中的不等式等价于 $|H \cap K| \cdot |G| \geq |H| \cdot |K|$. 由于 $|HK| \leq |G|$, 由(1), 不等式立证, 且等号成立当且仅当 $|HK| = |G|$, 即 $HK = G$. 由于 $(G : H)$ 与
$(G : K)$ 均是 $(G : H \cap K)$ 的因子, 如果它们互素, 则等号必成立.

对于(1), 设 $H \cap K = L$, 令 $\{x_i \mid i = 1, \cdots, m\}$ 为 H 关于 L 的左陪集代表元系, $\{y_j \mid j = 1, \cdots, n\}$ 为 K 关于 L 的右陪集代表元系, 则

$$HK = \bigcup_{i=1}^{m} x_i L \ \bigcup_{j=1}^{n} L y_j = \bigcup_{i,j} x_i L y_j.$$

我们只需证明上述陪集两两不交即可. 如果 $xLy = x'Ly'$, 则 $(x')^{-1}xL = Ly'y^{-1}$, 故 $(x')^{-1}x \in K$ 且 $y'y^{-1} \in H$. 因此 $(x')^{-1}x \in L$ 且 $y'y^{-1} \in L$, 即 $x = x'$ 且 $y = y'$. □

习　　题

习题3.1. 设

$$A=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},\quad B=\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}.$$

试求A, B, AB 和BA 在$\mathrm{GL}_2(\mathbb{R})$ 中的阶.

习题3.2. 证明群中元素a 的阶≤ 2 当且仅当$a=a^{-1}$.

习题3.3. 设a,b是群G的两个元素, a的阶是7且$a^3b=ba^3$. 证明$ab=ba$.

习题3.4. (1) 设G 是有限阿贝尔群. 证明:

$$\prod_{g\in G} g=\prod_{\substack{a\in G\\ a^2=1}} a.$$

(2) 证明*Wilson*定理: 如p 是素数, 则$(p-1)!\equiv -1 \mod p$.

习题3.5. 证明 $f=\frac{1}{x}$, $g=\frac{x-1}{x}$ 生成一个函数群, 合成法则是函数的合成, 它同构于二面体群 D_3.

习题3.6. (1) S^1 的任意有限阶子群均为循环群.

(2) $\mathbb{Q}$ 不是循环群, 但它的任意有限生成子群都是循环群.

(3)* 设 p 是一个素数,

$$G=\{x\in\mathbb{C}\mid \text{存在 } n\in\mathbb{N} \text{ 使得 } x^{p^n}=1\}$$

的任意真子群都是有限阶循环群.

习题3.7. 设 a 和 b 是群 G 的元素, 阶数分别是 n 和 m, $(n,m)=1$ 且 $ab=ba$. 试证 $\langle ab\rangle$ 是 G 的 mn 阶循环子群.

习题3.8. 设 G 是 n 阶有限群. 若对 n 的每一因子 m, G 中至多只有一个 m 阶子群, 则 G 是循环群.

习题3.9. 举一个无限群的例子, 它的任意阶数不为 1 的子群都有有限指数.

习题3.10. (1) 设G 是阿贝尔群, H 是G 中所有有限阶元素构成的集合. 证明H 是G 的子群.

(2)* 举例说明上述结论对于一般群不正确.

习题3.11. (1) 设 G 是奇数阶阿贝尔群. 证明由 $\varphi(x) = x^2$ 定义的映射 $\varphi : G \to G$ 是一个自同构.

(2)* 推广(1)的结果.

习题3.12. (1) 求有理数加法群 $\mathbb{Q}$ 的自同构群 $\mathrm{Aut}(\mathbb{Q})$.

(2) 求整数加法群 Z 的自同构群 $\mathrm{Aut}(\mathbb{Z})$.

(3) 计算 *Klein* 群的自同构群.

(4) 求非零有理数乘法群 $\mathbb{Q}^\times$ 的自同态群 $\mathrm{End}(\mathbb{Q}^\times)$.

习题3.13. 回答下列问题:

(1) 设p是素数, p方幂阶群是否一定含有p阶元?

(2) 35阶群是否一定同时含有5阶和7阶元素?

(3) 若有限群 G含有 10 阶元 x 和 6阶元 y, 那么群 G 的阶应该满足什么条件?

习题3.14. 如果H 与K 是G的子群且阶互素, 证明$H \cap K = 1$.

习题3.15. 设 R^m 为 m 维实向量空间, A 是任意 $n \times m$ 实矩阵, $W = \{X \in R^m \mid AX = 0\}$. 证明线性方程 $AX = B$ 的解空间或者是空集, 或者是 R^m (作为加法群)关于W的陪集.

习题3.16. 设 H 和 K 分别是有限群 G 的两个子群, $HgK = \{hgk \mid h \in H,\ k \in K\}$. 试证:

$$|HgK| = |H| \cdot |K : g^{-1}Hg \cap K|.$$

习题3.17. 设 a, b 是群 G 的任意两个元素. 试证: a 和 a^{-1}, ab 和 ba 有相同的阶.

习题3.18. 设 $f : G \to H$ 是群同态. 如果 g是 G的有限阶元, 则 $f(g)$的阶整除g 的阶.

习题3.19. 设 A 是群 G 的具有有限指数的子群. 试证: 存在 G 的一组元素 $g_1, \ldots, g_n$, 它们既可以作为 A 在 G 中的右陪集代表元系, 又可以作为 A 在 G 中的左陪集代表元系.

习题3.20. (1) 证明 $\mathrm{SL}_n(\mathbb{R})$ 由第一类初等矩阵 $I + aE_{ij}(i \neq j)$ 生成, 其中 E_{ij} 的第 (i,j) 元为 1, 其他元为 0.

(2) 证明 $\mathrm{GL}_n(\mathbb{R})$ 由第一类初等矩阵和第三类初等矩阵生成.

(3)* 证明 $\mathrm{SL}_2(\mathbb{Z})$ 可以由 $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ 和 $T = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ 生成.

§1.4 正规子群与商群

我们在上节定义了群 G 关于其子群 H 的左陪集分解

$$G = \bigsqcup_{i \in I} g_i H = \{gH \mid g \in G\}.$$

记 $G/H = \{g_i H \mid i \in I\}$ 为 G 的所有左陪集构成的集合类. 回忆在线性代数中, 如果 W 是 V 的子空间, 则商空间

$$V/W = \{v + W \mid v \in V\},$$

它首先是加法子群 W 关于群 V的陪集集合类. 然后在上面可以定义线性空间的结构, 从而有商空间的概念. 自然, 我们希望 G/H 具有 V/W 有**商**的群结构, 其乘法能够**继承** G 的乘法. 如果要此项条件成立, 我们需要对任意 $a, b \in G$, 有

$$aHbH = abH.$$

而此时在集合意义上,

$$aHbH = \{ah_1bh_2 \mid h_1, h_2 \in H\},$$

故对 $h_1, h_2 \in H$, 需存在 $h \in H, ah_1bh_2 = abh$, 即 $h_1 b = b(hh_2^{-1})$. 所以, 要使 G/H 上有自然的乘法结构, 我们需要条件:

对任意 $b \in G$, 有 $Hb = bH$ 或等价条件 $b^{-1}Hb = H$ 成立.

定义1.70. 设G 是群, $x \in G$. 对任意 $g \in G$, gxg^{-1} 称为 x 的**共轭元**, 或者称x 与$x' = gxg^{-1}$ **共轭** (conjugate).

定义1.71. 子群 N 称为 G 的**正规子群** (normal subgroup), 是指对所有 $g \in G$ 有 $g^{-1}Ng = N$. 此时记 $N \lhd G$.

由定义容易验证共轭关系是等价关系, 且子群 N 是 G 的正规子群当且仅当 N 中任意元素的所有共轭元都在 N 中, 即 N 是G 中一些**共轭类** 之并.

例1.72. (1) 如果G 是阿贝尔群, 则$gxg^{-1} = x$ 对所有$g \in G$ 成立, 故x 是它所在共轭类唯一的元素, 因此G 的任何子群都是正规子群.

(2) 更进一步说, 对于任意群G, 元素x 所在共轭类只有一个元素当且仅当它与 G 中所有元素都交换. 所有这些元素构成的集合是G 的正规子群(参考*4.4*), 称为G 的**中心** (*center*), 记为$Z(G)$.

我们来看一个常见的正规子群例子.

定义1.73. 设 $\varphi : G \to H$ 是群同态.

(1) 映射 φ 的**核** (kernel)为

$$\ker\varphi = \{g \in G \mid f(g) = 1\}.$$

(2) 映射 φ 的**像** (image)为

$$\mathrm{im}\varphi = \{h \in H \mid 存在g \in G, f(g) = h\}.$$

命题1.74. 设 $\varphi : G \to H$ 是群同态, 则 $\ker\varphi$ 是 G 的正规子群, $\mathrm{im}\varphi$ 是 H 的子群.

证明. 由 $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$, 我们有

$$\varphi(1) = 1, \quad \varphi(g)^{-1} = \varphi(g^{-1})$$

设 $a, b \in \ker\varphi$, 则

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = 1,$$

故 $ab^{-1} \in \ker\varphi$, $\ker\varphi$ 是 G 的子群.

设 $g \in G, a \in \ker\varphi$, 则

$$\varphi(g^{-1}ag) = \varphi(g)^{-1}\varphi(a)\varphi(g) = \varphi(g)^{-1}\varphi(g) = 1,$$

所以 $g^{-1}ag \in \ker\varphi$, 故

$$g^{-1}(\ker\varphi)g \subseteq \ker\varphi,$$

$$\ker\varphi \subseteq g(\ker\varphi)g^{-1}.$$

由对称性 $g^{-1}(\ker\varphi)g = \ker\varphi$, 所以 $\ker\varphi$ 是 G 的正规子群.

如果 $h_1, h_2 \in \mathrm{im}\varphi$, 令 $\varphi(g_1) = h_1, \varphi(g_2) = h_2$, 则

$$\varphi(g_1g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = h_1h_2^{-1},$$

所以 $h_1h_2^{-1} \in \mathrm{im}\varphi$, 故 $\mathrm{im}\varphi$ 是 H 的子群. □

例1.75. 行列式映射 $\det : \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times$ 的核是 $\mathrm{SL}_n(\mathbb{C})$, 故 $\mathrm{SL}_n(\mathbb{C})$ 是 $\mathrm{GL}_n(\mathbb{C})$ 的正规子群.

现在设 $N \lhd G$, 则 G 关于 N 的左陪集为

$$G/N = \{aN \mid a \in G\} = \{Na \mid a \in G\},$$

且

$$aNbN = a(bN)N = abN.$$

记 $\overline{a} = aN$, 定义乘法

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

由上述推理, G/N 成为一个群, 称为 G 关于 H 的**商群** (quotient group).

记

$$\pi : G \to G/N, \quad a \mapsto \overline{a} = aN,$$

则 π 是群的满同态, 且 $\ker\pi = N$. 故我们有如下重要注记:

注记. 如果 N 是 G 的正规子群, 则存在群同态 φ, 使得 $N = \ker\varphi$; 反之, 如果 N 是群 G 到另一群的群同态 φ 的核, 则 N 是 G 的正规子群. 我们常常利用此项性质来寻找和判定群 G 的正规子群.

例1.76. (1) 由线性代数可知, 与所有可逆矩阵都可交换的矩阵是数量矩阵 xI_n $(x \in F)$, 由此可知 $\{xI_n \mid x \in F^\times\}$ 是一般线性群 $\mathrm{GL}_n(F)$ 的中心, 它对应的商群记为 $\mathrm{PGL}_n(F)$, 称为**射影一般线性群**.

(2) $\mathrm{SL}_2(\mathbb{Z})$ 关于其中心$\{\pm I_2\}$ 的商群记为$\mathrm{PSL}_2(\mathbb{Z})$, 即$\mathbb{Z}$ 上的 2 阶射影特殊线性群. 此群是当代数学研究最著名的一个群之一, 也称为**模群** (*modular group*).

现在我们讨论群论中最重要定理:

定理1.77 (同态基本定理)**.** 设 $\varphi : G \to H$ 为群的同态, 则 φ 诱导的同态

$$\begin{aligned} \overline{\varphi} : G/\ker\varphi &\to \mathrm{im}\varphi \\ \overline{\varphi}(\overline{g}) &= \varphi(g) \end{aligned}$$

为群同构.

证明. (i) 我们首先证明 $\overline{\varphi}$ 是良好定义的, 即它的定义与 g 的选取无关. 事实上, 若 $g\ker\varphi = g'\ker\varphi$, 则 $g' = ga, a \in \ker\varphi$, 所以 $\varphi(g') = \varphi(ga) = \varphi(g)$.

(ii) $\overline{\varphi}$ 是同态. 如果 $\overline{g}_1, \overline{g}_2 \in G/\ker\varphi$, 则

$$\overline{\varphi}(\overline{g_1 g_2}) = \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(\overline{g}_1)\overline{\varphi}(\overline{g}_2).$$

(iii) $\overline{\varphi}$ 是单同态. 如果 $\overline{\varphi}(\overline{g}_1) = \overline{\varphi}(\overline{g}_2)$, 则 $\varphi(g_1) = \varphi(g_2)$, 故 $g_2 = g_1(g_1^{-1}g_2) \in g_1\ker\varphi$, 即 $\overline{g}_2 = \overline{g}_1$.

(iv) $\overline{\varphi}$ 是满同态是显然的.

由(i)-(iv), 定理得证. □

推论1.78. 设$\varphi : G \to H$ 为群同态, 则

(1) φ 是单同态当且仅当 $\ker\varphi = \{1\}$.

(2) φ 是满同态当且仅当 $G/\ker\varphi \cong H$.

例1.79. (1) 映射 $\mathbb{R} \to S^1$, $x \mapsto e^{2\pi ix}$ 的核是 $\mathbb{Z}$, 而像就是 S^1, 故由同态基本定理得到群同构 $\mathbb{R}/\mathbb{Z} \cong S^1$.

(2) 对于域 F, 行列式映射诱导同构 $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong F^\times$.

例1.80. (1) 群同态 $\varphi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a \bmod N & b \bmod N \\ c \bmod N & d \bmod N \end{pmatrix}$$

为满同态, 其核为

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, a \equiv d \equiv 1 \bmod N, b \equiv c \equiv 0 \bmod N \right\}, \quad (1.26)$$

称为**主同余子群** (*principal congruence subgroup*). 由同态基本定理, $\Gamma(N)$ 是$\mathrm{SL}_2(\mathbb{Z})$ 的正规子群, 且$\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

(2) 设$N > 2$. 考虑群同态$\tau : \Gamma(N) \to \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z})$. 则$\ker \tau = \Gamma(N) \cap \{\pm I_2\} = \{I_2\}$, 故$\tau$ 是单同态. 由此我们可以将主同余子群 $\Gamma(N)$ 视为模群$\mathrm{PSL}_2(\mathbb{Z})$ 的子群.

由同态基本定理, 我们可以得到很多重要的结果. 我们来看一下其中一些结果.

定理1.81. 设 N 是 G 的正规子群. 记 $\mathcal{M}$ 为 G 中包含 N 的所有子群的集合, $\overline{\mathcal{M}}$ 为 $\overline{G} = G/N$ 的所有子群集合, 即

$$\mathcal{M} = \{M \mid N \leqslant M \leqslant G\},$$
$$\overline{\mathcal{M}} = \{\overline{M} \mid \overline{M} \leqslant \overline{G} = G/N\}.$$

则映射 $\alpha : \mathcal{M} \to \overline{\mathcal{M}}$, $M \mapsto M/N$ 为一一对应.

证明. 首先, 如果 $N \lhd G$, 则对所有 $N \leqslant M \leqslant G$, $N \lhd M$, 故 M/N 是 G/N 的子群, 即 α 是定义好的.

对于 $\overline{M} \in \overline{\mathcal{M}}$, 记 $\beta(\overline{M}) = \{g \in G \mid \overline{g} \in \overline{M}\}$, 则 $\beta(\overline{M}) \supseteq N$, 且由于 $\overline{M}$ 为群, 因此 $\beta(\overline{M})$ 也是群, 故 β 是 $\overline{\mathcal{M}}$ 到 M 的映射.

现在我们只需检查

$$\alpha\beta(\overline{M}) = \overline{M}, \quad \beta\alpha(M) = M$$

即可, 而这是显然的. □

定理1.82. 如果 $N \lhd G, H \leqslant G$, 则

$$(H \cap N) \lhd H, \quad N \lhd NH \leqslant G$$

且

$$NH/N \cong H/H \cap N.$$

证明. 由于 $N \lhd G$, 则对于 $a_1h_1, a_2h_2 \in NH$,

$$a_1h_1(a_2h_2)^{-1} = a_1h_1h_2^{-1}a_2^{-1} = a_1a_2^{-1}h \in NH,$$

故 $NH \leqslant G$, 且 $N \lhd NH$.

现在我们定义同态

$$\varphi : H \to NH/N, \quad h \mapsto \overline{h} = hN,$$

自然 φ 为满同态, 且

$$\ker\varphi = \{h \mid \varphi(h) = 1\} = \{h \mid h \in N\} = H \cap N.$$

由同态基本定理

$$(H \cap N) \lhd H$$

且

$$NH/N \cong H/H \cap N.$$

定理证毕. □

定理1.83. 如果 $N \lhd G, M \lhd G$ 且 $N \leqslant M$, 则

$$G/M \cong \frac{G/N}{M/N}.$$

证明. 首先定义同态

$$\varphi : G/N \to G/M, \quad gN \mapsto gM.$$

由 $N \leqslant M$ 知 φ 为满同态, 且

$$\ker\varphi = \{gN \mid gM = M\} = \{gN \mid g \in M\} = M/N,$$

由同态基本定理,

$$G/M \cong \frac{G/N}{M/N}.$$

定理证毕. □

习　　题

习题4.1. 令 $G=\{(a,b)\mid a\in\mathbb{R}^\times, b\in\mathbb{R}\}$, 乘法定义为

$$(a,b)(c,d)=(ac,ad+b).$$

试证: $K=\{(1,b)\mid b\in\mathbb{R}\}$ 是 G 的正规子群且 $G/K\cong\mathbb{R}^\times$.

习题4.2. 证明行列式为正的实矩阵组成的 $G=\mathrm{GL}_n(\mathbb{R})$ 的子集 H 构成一个正规子群, 并描述商群G/H.

习题4.3. 设 G 是群, $N\lhd M\lhd G$.

(1) 如果 $N\lhd G$, 则 $N\lhd M$;

(1) 如果 $N\lhd M$, 则 N 是否一定是 G 的正规子群?

习题4.4. 试证:

(1) 群 G的中心 $Z(G)$ 是 G的正规子群.

(2) 群 G的指数为 2的子群一定是 G的正规子群.

习题4.5. 证明积群 $G\times G'$ 的子集 $G\times 1$是一个与 G同构的正规子群, 且 $G\times G'/G\times 1\cong G'$.

习题4.6. 若 $G/Z(G)$ 是循环群, 则 G 是阿贝尔群.

习题4.7. 设 $G_i(1\leq i\leq n)$ 为群, 则

(1) $C(G_1\times G_2\times\cdots\times G_n)=C(G_1)\times C(G_2)\times\cdots\times C(G_n)$;

(2) $G_1\times G_2\times\cdots\times G_n$ 为阿贝尔群当且仅当每个 G_i 均为阿贝尔群.

习题4.8. 设 G 为群.

(1) 对于 $x\in G$, 证明映射 $\sigma_x: g\mapsto xgx^{-1}$ 是 G 的自同构. σ_x 称为**内自同构** (*inner automorphism*).

(2) 令 $I(G)$ 表示所有 σ_x: $x\in G$ 组成的集合. 试证$I(G)$ 是$\mathrm{Aut}(G)$ 的子群. $I(G)$ 称为**内自同构群**.

(3) 证明$I(G)\cong G/Z(G)$.

习题4.9. 设 $f: G\to H$ 是群同态, $M\leqslant G$. 试证 $f^{-1}(f(M))=KM$, 这里 $K=\ker f$.

习题4.10. 设 M, N 为 G 的正规子群. 若 $M \cap N = \{1\}$, 则对任意 $a \in M$, $b \in N$, $ab = ba$.

习题4.11. 设 $N \lhd G$, g 是群 G 的任意一个元素. 如果 g 的阶和 $|G/N|$ 互素, 则 $g \in \mathbb{N}$.

习题4.12. 当 n 为奇数时, 证明 $\mathrm{O}_n(\mathbb{R}) \cong \mathrm{SO}_n(\mathbb{R}) \times \mathbb{Z}/2\mathbb{Z}$.

第二章　群在集合上的作用

数学研究对象中, 常常需要研究集合的性质, 但集合本身并不是孤立的, 从代数的观点而言, 群在集合上的作用是研究集合的最主要代数方法.

我们首先给出定义.

定义2.1. 设 X 是集合, G 为群. G **在** X **上的作用** (The action of G on the set X)是指映射

$$G \times X \to X, \quad (g, x) \mapsto g \cdot x,$$

满足条件

(1) 对任意的 $x \in X$, $1 \cdot x = x$.

(2) (结合律) 对任意 $x \in X, g, h \in G$,

$$g(hx) = (gh)x.$$

此时, 我们亦称 X 为 G**-集** (G-set).

§2.1　置换群

我们首先以**置换群** (对称群) S_n 作为例子来考虑一下群在集合上的作用. 令 $X_n = \{1, \ldots, n\}$, 则 $S_n = S_{X_n}$ 自然作用在 X_n 上.

§2.1.1　置换及其表示

对置换 $\sigma \in S_n$, 我们一方面可以用**两行式**来表示 σ, 即

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}. \tag{2.1}$$

另一方面, 我们可以用另外一种方式来表示 σ:

定义2.2. 设 $k \leqslant n$, $\{a_1, \ldots, a_k\} \subseteq X_n$, 置换 σ 称为一个 k **轮换** (k-cycle), 是指

- $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\ldots, \sigma(a_k) = a_1$;

- 对于 $i \in X_n - \{a_1, \ldots, a_k\}$, $\sigma(i) = i$.

此时记 $\sigma = (a_1, \ldots, a_k)$.

特别地, 2 轮换也称作**对换** (transposition).

注记. (1) 任何一个1 轮换都是恒等置换, 即S_n 中的单位元 1.

(2) k 轮换 $(a_1 a_2 \cdots a_k) = (a_2 \cdots a_k a_1) = \cdots = (a_k a_1 a_2 \cdots a_{k-1})$.

定义2.3. 如果 $\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_j\} = \emptyset$, 称轮换 $(a_1 a_2 \cdots a_k)$ 与 $(b_1 b_2 \cdots b_j)$ **不相交** (disjoint).

定理2.4. (1) 不相交轮换可交换, 即如果 $\sigma = (a_1 \cdots a_k), \tau = (b_1 \cdots b_j)$ 不相交, 则 $\sigma\tau = \tau\sigma$.

(2) 任意置换 $\sigma \in S_n$ 均可写为两两不相交轮换的乘积, 且在不计先后次序的情况下方式唯一.

证明. (1) 设 $\sigma = (i_1\ i_2 \cdots i_k)$, $\tau = (j_1\ j_2 \cdots j_l)$, 则

$$\sigma\tau(i_1) = \sigma(i_1) = i_2 = \tau\sigma(i_1)$$
$$\cdots$$
$$\sigma\tau(i_k) = \sigma(i_k) = i_1 = \tau\sigma(i_k)$$
$$\sigma\tau(j_1) = \sigma(j_2) = j_2 = \tau\sigma(j_1)$$
$$\cdots$$
$$\sigma\tau(j_l) = \sigma(j_1) = j_1 = \tau\sigma(j_l)$$
$$\sigma\tau(\alpha) = \alpha = \tau\sigma(\alpha), \forall \alpha \notin \{i_1, \ldots, i_k, j_1, \ldots, j_l\}$$

故$\sigma\tau = \tau\sigma$.

(2) 对于 $\sigma \in S_n$, 固定 i, 则集合$T_i = \{\sigma^k(i) \mid k \in \mathbb{Z}\} \subseteq X_n$ 是有限集, 故存在 $\sigma^{k_1}(i) = \sigma^{k_2}(i), k_1 \neq k_2$, 所以 $\sigma^{k_1 - k_2}(i) = i$. 令 m_i 为最小的正整数使得 $\sigma^{m_i}(i) = 1$, 则

$$T_i = \{\sigma^k(i) \mid k \in \mathbb{Z}\} = \{i, \sigma(i), \ldots, \sigma^{m_i - 1}(i)\}.$$

由于 $X_n = \bigsqcup_{i \in I} T_i$ 为不交并, 且这种方式唯一. 我们有

$$\sigma = \prod_{i \in I} (i\ \sigma(i)\ \cdots\ \sigma^{m_i - 1}(i)),$$

且方式唯一. □

例2.5. 对于 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 5 & 1 \end{pmatrix}$, 则 $\sigma = (1\ 6)(2\ 4\ 3)(5) = (1\ 6)(2\ 4\ 3)$.

例2.6. 对于小的n, 置换群可以如下详细给出.

(1) 对于 $n = 2$, $S_2 = \{1, (12)\}$.

(2) 对于 $n = 3$, $S_3 = \{1, (12), (13), (23), (123), (132)\}$.

(3) 对于 $n = 4$, 则

$$\begin{aligned} S_4 = \{&1, (12), (13), (14), (23), (24), (34), \\ &(123), (132), (124), (142), (134), (143), (234), (243), \\ &(1234), (1243), (1324), (1423), (1342), (1432), \\ &(12)(34), (14)(23), (13)(24)\}. \end{aligned}$$

由于 k 轮换 $(i_1 \cdots i_k)$ 中哪个元素放在首位不是本质的, 将$i_1, \cdots i_k$ 这k个点依顺时针次序均匀放置在时钟上, 则k 轮换可以看做是将时钟顺时针转动角度 $2\pi/k$, 其逆也就是逆时钟转动相同角度. 即有

引理2.7. 如 $\sigma = (i_1 \cdots i_k)$ 为 k 轮换, 则 σ 的阶为 k, 且 $\sigma^{-1} = (i_k\ i_{k-1} \cdots i_1)$.

定义2.8. 设 $\sigma \in S_n$. 当 σ 写为不交轮换乘积时, k 轮换的个数为 λ_k, 则称 σ 的**型** 为 $1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}$.

由型的定义, 整数 $\lambda_1, \ldots, \lambda_n \geq 0$, 满足方程

$$\sum_{i=1}^{n} i\lambda_i = n. \tag{2.2}$$

所以S_n 中置换的型的个数即为满足 (2.2) 的非负整数组 $\lambda_1, \ldots, \lambda_n$ 的个数. 在组合数学中, 这样的数组称为正整数 n 的一个**分拆** (partition). . 分拆的个数称为**分拆函数**, 常用$p(n)$ 表示.

例2.9. 由$p(2) = 2$, $p(3) = 3$, $p(4) = 5$ 知置换群 S_2, S_3 和S_4 中元素的型分别有$2, 3$ 和5 种, 这与例 *2.6* 一致.

命题2.10. 置换 σ 与 σ' 的型相同当且仅当 σ 与 σ' 在 S_n 中共轭, 即存在 $\tau \in S_n$, $\sigma' = \tau\sigma\tau^{-1}$. 故置换群$S_n$ 中共轭类的个数等于分拆函数$p(n)$.

证明. 设 $\sigma=(i_1\cdots i_k)(j_1\cdots j_l)\cdots$, 则

$$\tau\sigma\tau^{-1}=(\tau(i_1)\cdots\tau(i_k))(\tau(j_1)\cdots\tau(j_l))\cdots,$$

它的型与 σ 一致.

反过来, 如 $\sigma=(i_1\cdots i_k)(j_1\cdots j_l)\cdots)$, $\sigma'=(i_1'\cdots i_k')(j_1'\cdots j_l)'\cdots)$. 令

$$\tau=\begin{pmatrix} i_1 & \cdots & i_k & j_1 & \cdots & j_l & \cdots \\ i_1' & \cdots & i_k' & j_1' & \cdots & j_l' & \cdots \end{pmatrix}$$

则 $\tau\sigma\tau^{-1}=\sigma'$, 即 σ 与 σ' 共轭. □

§2.1.2 奇置换与偶置换

命题2.11. (1) 任何k 轮换可以写为$k-1$ 个对换的乘积.

(2) S_n 由对换生成. 更一般地, S_n 可由对换 $(12),(13),\ldots,(1n)$ 生成.

证明. (1) 这是由于$(i_1\cdots i_k)=(i_1i_k)(i_1i_{k-1})(i_1i_2)$.

(2) 由于每个置换都是轮换的乘积, 故由(1), S_n 由对换生成. 由于对每个对换

$$(ij)=(1i)(1j)(1i),$$

故S_n 可由对换 $(12),(13),\ldots,(1n)$ 生成. □

设 $f=f(x_1,\ldots,x_n)$ 是 $\mathbb{Z}^n$ 到 $\mathbb{Z}$ 的 n 变量函数, 对于 $\sigma\in S_n$ 定义

$$\sigma(f)(x_1,\ldots,x_n)=f(x_{\sigma(1)},\ldots,x_{\sigma(n)}). \tag{2.3}$$

故 $\sigma(f)$ 也是 $\mathbb{Z}^n$ 到 $\mathbb{Z}$ 上的 n 变量函数.

例2.12. 设 $n=3$, $\sigma=(123)$, $f(x_1,x_2,x_3)=x_3^2-x_1$, 则

$$\sigma(f)(x_1,x_2,x_3)=x_1^2-x_2.$$

引理2.13. 我们有

(1) 如 $\sigma=1$, 则 $\sigma(f)=f$.

(2) 如 $\sigma,\tau\in S_n$, 则 $\sigma\tau(f)=\sigma(\tau(f))$.

(3) 如 f,g 为 n 变量函数, c 为整常数, 则

$$\sigma(f+g)=\sigma(f)+\sigma(g),\quad \sigma(cf)=c\sigma(f).$$

证明. (1), (3) 留给读者.

(2) 一方面,

$$\sigma\tau(f)(x_1,\ldots,x_n)=f(x_{\sigma\tau(1),\ldots,x_{\sigma\tau(n)}}).$$

另一方面, 由$\tau(f)(x)=f(x_{\tau(1)},\ldots,x_{\tau(n)})$ 得

$$\sigma(\tau(f))(x)=f(x_{\sigma(\tau(1))},\ldots,x_{\sigma(\tau(n))})=f(x_{\sigma\tau(1)},\ldots,x_{\sigma\tau(n)}).$$

故 $\sigma\tau(f)=\sigma(\tau(f))$. □

定理2.14. *存在唯一的群同态* $\varepsilon: S_n\to\{\pm1\}$, *使得对所有对换* τ *有*

$$\varepsilon(\tau)=-1.$$

证明. 令 $\Delta(x_1,\ldots,x_n)=\prod\limits_{1\le i<j\le n}(x_i-x_j)$. 如果 σ 是 i 个对换的积, 使用引理 2.13 经计算即得

$$\sigma\Delta=(-1)^i\Delta.$$

特别地, $\tau\Delta=-\Delta$ 对所有对换 τ 成立. 令 $\varepsilon(\sigma)=(-1)^i$, 由 $\sigma\tau(\Delta)=\sigma(\tau(\Delta))$ 有 $\varepsilon(\sigma\tau)=\varepsilon(\sigma)\varepsilon(\tau)$. 故 ε 为群同态.

唯一性显然, 因为所有置换均由对换生成. □

由定理知, 一个置换写成对换乘积时, 对换个数的奇偶性不变. 我们有如下定义.

定义2.15. 如果置换 σ 为偶数个对换的乘积, 称 σ 为**偶置换** (even permutation). 如果 σ 为奇数个对换的乘积, 称 σ 为**奇置换** (odd permutation).

下面命题给出置换奇偶性的一个简单判定:

命题2.16. *如果置换* $\sigma\in S_n$*的型为*$1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$, *则*$\sigma$ *的奇偶性与*$\sum\limits_{i=1}^{n}\lambda_i(i-1)$ *的奇偶性一致*.

证明. 这是由于每个k 轮换均是$k-1$ 个对换的乘积. □

§2.1.3 交错群

定义2.17. S_n 中所有偶置换构成的子群, 即 $\ker\varepsilon$, 称为 n 阶**交错群** (alternating group), 记为 A_n.

由奇偶置换的讨论即知, A_n 是 S_n 的正规子群, 阶为 $\frac{n!}{2}$.

定义2.18. 没有非平凡正规子群的群称为**单群** (simple group).

例2.19. *最简单的单群是素数阶群. 事实上, 素数阶群是仅有的阿贝尔单群. 如 G 是阿贝尔群, $1 \neq g \in G$. 设 g 的阶为 n 而 p 是 n 的素因子, 则 $\langle g^{n/p}\rangle$ 是 G 的 p 阶正规子群. 要使 G 为单群, 则必有 $G = \langle g^{n/p}\rangle$.*

本节剩余内容将致力于证明下述著名定理:

定理2.20. *$A_n (n \geqslant 5)$ 是单群.*

注记. $A_2 = \{1\}, A_3$ 的阶为3, 显然都是单群. 但 A_4 不是单群, 事实上

$$\{1, (12)(34), (13)(24), (14)(23)\} \lhd S_4,$$

自然也是 A_4 的正规子群.

Galois 利用定理 2.20 证明了五次以上多项式没有求根公式, 这是群论诞生的标志. 我们将在第六章阐述 Galois 的著名结果.

引理2.21. *A_n 由 3 轮换生成.*

证明. 事实上, 我们有

$$(ij)(rs) = \begin{cases} 1 & \text{如 } (ij) = (rs), \\ (jsi) & \text{如 } j = r, i \neq s, \\ (ris)(ijr) & \text{如 } \{i,j\} \neq \{r,s\}. \end{cases}$$

引理得证. □

引理2.22. *如果 $n \geqslant 3$, 则对于 3 轮换 (ijk) 和 $(i'j'k')$, 存在 $\gamma \in A_n$, 使得*

$$\gamma(ijk)\gamma^{-1} = (i'j'k').$$

证明. 由命题 2.10, 存在 $\gamma \in S_n$, 使得

$$\gamma(ijk)\gamma^{-1} = (i'j'k').$$

如果 γ 是奇置换, 设 $r, s \neq i', j', k'$, 则 $(rs)\gamma \in A_n$, 且 $(rs)\gamma(ijk)\gamma^{-1}(rs)^{-1} = (i'j'k')$. □

定理 2.20 的证明. 设 $\{1\} \neq N \lhd A_n$. 我们要证明 $N = A_n$. 由正规子群定义知, 如 $x \in N$, 则 $gxg^{-1} \in N$, 故由引理 2.21 和引理 2.22. 我们只需证明 N 中包含一个 3 轮换.

设 $1 \neq \sigma \in N$, 且 σ 保持 X_n 中尽可能多的元素不动. 我们证明 σ 恰好变动三个元素, 即为 3 轮换.

首先注意到 σ 至少变动三个元素, 我们只需证明如果 σ 变动超过了三个元素, 则存在 $\sigma' \in N$ 变动元素个数比 σ 少. 记 σ 为不相交轮换之积, 且最长轮换在左边.

(i) 如果 σ 最长轮换为对换, 则

$$\sigma = (a_1a_2)(a_3a_4)\cdots.$$

令 $\tau = (a_3a_4a_5)$, 则

$$\tau\sigma\tau^{-1}\sigma^{-1} = (a_3a_4a_5) \in N.$$

(ii) 如果 σ 最长轮换长度 $\geqslant 3$, 则 σ 至少变动 5 个元素.

- $\sigma = (a_1a_2a_3a_4)\cdots$. 令 $\tau = (a_2a_3a_4)$, 则

$$\tau\sigma\tau^{-1}\sigma^{-1} = (a_1a_2a_3) \in N.$$

- $\sigma = (a_1a_2a_3a_4a_5\cdots)\cdots$. 令 $\tau = (a_2a_3a_4)$, 则

$$\tau\sigma\tau^{-1}\sigma^{-1} = (a_2a_3a_5) \in N.$$

- $\sigma = (a_1a_2a_3)(a_4a_5\cdots a_6)\cdots, \sigma$ 最少变动 6 个元素. 令 $\tau = (a_2a_3a_4)$, 则

$$\tau\sigma\tau^{-1}\sigma^{-1} = (a_1a_4a_2a_3a_5) \in N,$$

且最多变动 5 个元素.

综上所述, 定理得证. □

习 题

习题1.1. 把置换 $\sigma=(456)(567)(761)$ 写成不相交轮换的积.

习题1.2. 直接证明置换 $(123)(45)$ 与 $(241)(35)$ 共轭.

习题1.3. 讨论置换

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ n & n-1 & \cdots & 1\end{pmatrix}$$

的奇偶性.

习题1.4. 一个置换的阶等于它的轮换表示中各个轮换的长度的最小公倍数.

习题1.5. 证明 S_n 中型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换共有 $n!/\prod\limits_{i=1}^{n}\lambda_i!i^{\lambda_i}$ 个. 由此证明

$$\sum_{\substack{\lambda_i\geqslant 0\\ \lambda_1+2\lambda_2+\cdots+n\lambda_n=n}}\frac{1}{\prod\limits_{i=1}^{n}\lambda_i!i^{\lambda_i}}=1.$$

习题1.6. 试确定 $S_n(n\geqslant 2)$ 的全部正规子群.

习题1.7. 置换 σ 的**交错数** $n(\sigma)$ 定义为集合$\{(i,j)\mid \sigma(i)>\sigma(j)$ 但 $i<j\}$ 的阶.

(1) 证明 $n(\sigma)=\sum\limits_{i=1}^{n}\Big|\{j\mid \sigma(j)>i$ 且 $j<\sigma^{-1}(i)\}\Big|$.

(2) 证明置换 σ 可以写为 $n(\sigma)$ 个对换的乘积. 故置换的奇偶性和它的交错数的奇偶性相同.

习题1.8. (1) 试证 A_5 中置换的型为 1^5, $2^2\cdot 1^1$, $3^1\cdot 1^2$ 和 5^1.

(2) 证明 A_5 中型为 $2^2\cdot 1^1$ 的置换共轭, 型为 $3\cdot 1^2$ 的置换也共轭.

(3) 试求 A_5 中型为 5^1 的置换的共轭类.

(4) 由此证明 A_5 是单群.

习题1.9. 试证: 当 $n\geq 3$时, $Z(S_n)=1$.

习题1.10. 试证 A_4 没有 6 阶子群.

习题1.11. 试计算:

(1) S_6 中 2 阶元的个数.

(2) A_8 中阶最大的元素个数.

习题1.12. 计算 S_n 中使任意指标都变动的置换的个数.

习题1.13. 证明当$n \geq 2$ 时, A_n 是 S_n 唯一的指数为 2 的子群.

习题1.14. 当 $n \geqslant 2$ 时, (12) 和 $(123\cdots n)$ 是 S_n 的一组生成元.

§2.2 群在集合上的作用

§2.2.1 轨道与稳定子群

我们再回顾一下群在集合上的作用的定义.

定义2.23. 设 X 是集合, G 为群. G 在 X 上的作用是指映射

$$G \times X \to X, \quad (g, x) \mapsto g \cdot x,$$

且满足条件

(1) 对任意的 $x \in X, 1 \cdot x = x$.

(2) (结合律) 对任意 $x \in X, g, h \in G$,

$$g(hx) = (gh)x.$$

此时, 我们亦称 X 为 G-**集**.

定义2.24. 如果 X 为 G-集, $x \in X$. 则

$$O_x = Gx = \{gx \mid g \in G\} \subseteq X \tag{2.4}$$

称为 x 所在的**轨道** (orbit). 如果存在 $x \in X$ 使得 $O_x = X$, 称 G 在 X 上的作用**可迁** (transitive).

由定义知 X 上不同的轨道不相交, 且 X 是 G 作用下所有轨道的不交并. 由此我们可以定义 X 上的等价关系

$$x \sim y \qquad \text{如果} \quad \text{存在 } g \in G,\ y = gx,\ \text{即 } y \in O_x.$$

令 $\{O_x \mid x \in I\}$ 为 X 上所有轨道构成的集合, 则

$$X = \bigsqcup_{x \in I} O_x. \tag{2.5}$$

对 $x \in X$, 令

$$G_x = \{g \in G \mid gx = x\}, \tag{2.6}$$

即 G 上所有作用在 x 上平凡的元素的集合, 容易验证 G_x 是 G 的子群.

定义2.25. 设 X 为 G-集, $x \in X$. G_x 称为 x 的**稳定子群** (stabilizer).

例2.26. 设 $\mathcal{H}$ 为上半平面 $\{z \in \mathbb{C} \mid \operatorname{im} z > 0\}$. 则群 $G = \mathrm{SL}_2(\mathbb{R})$ 作用在 $\mathcal{H}$ 上: 对于 $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$, 令

$$\gamma z = \frac{az + b}{cz + d}. \tag{2.7}$$

由计算易知 G 在 $\mathcal{H}$ 上的作用是可迁的, 且 i 的稳定子群是 $SO_2(\mathbb{R})$.

例2.27. 设 M 是平面上刚性运动构成的群. 我们由解析几何知 M 是由平移、旋转与反射生成. 如果在平面上建立坐标系, 则 M 中一个元素可以如此表出

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \pm\sin\theta & \pm\cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}.$$

特别地, **旋转**为

$$\rho_\theta : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \pm\sin\theta & \pm\cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}; \tag{2.8}$$

平移为

$$\tau_P : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}, \text{ 其中 } P = (x_0, y_0); \tag{2.9}$$

反射为

$$r : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x \\ -y \end{pmatrix}. \tag{2.10}$$

则 M 作用在平面上的点集上, 平面上的直线集上, 和平面上的三角形集上.

如果 X 是平面上的点集, 则 M 在 X 上的作用是可迁的, 且原点 O 的稳定子群是 $M_O = \mathrm{O}_2(\mathbb{R})$, 即正交群.

例2.28. 设 $H \leqslant G$, 设 $G/H = \{aH \mid a \in G\}$ 是 G 关于 H 的左陪集的集合, 则

$$G \times G/H \to G/H, \qquad (g, aH) \mapsto gaH$$

是 G 在 G/H 上的左乘作用, 我们称为 G 关于 H 的**左诱导表示** (*left induced representation*). 容易看出 G 在 G/H 上的作用是可迁的, 且对于陪集 $H \in G/H$, 稳定子群 $G_H = H$.

例2.29. 设 $G = \mathbb{R}$, X 为 $\mathbb{R}$ 上连续函数的集合. 对于 $f \in X$, $a \in \mathbb{R}$, 定义

$$a \circ f(x) = f(x + a).$$

则加法群 $\mathbb{R}$ 作用在连续函数集合上. 注意到:

(1) f 的稳定子群 $G_f = \mathbb{R}$ 当且仅当 f 是常值函数.

(2) f 的稳定子群 $G_f = t\mathbb{Z}$ $(t > 0)$ 当且仅当 f 为最小正周期 t 的连续周期函数.

命题2.30. 设 X 是 G-集, $x \in X$, O_x 是 x 所在的轨道, 稳定子群 G_x 为 G 的子群 H. 则存在自然的双射

$$\varphi : G/H \to O_x, \quad aH \mapsto ax.$$

此映射与 G 的作用相洽, 即对于 $g \in G, \varphi(gaH) = g\varphi(aH)$.

证明. 首先, 如果 $aH = bH$, 则 $b = ah, bx = ahx = ax$, 故 φ 的定义与 a 的选取无关. 另由定义, φ 与 G 相洽. 其次, 如果 $ax = bx$, 则 $x = a^{-1}ax = a^{-1}bx$, 所以 $a^{-1}b \in H$, 即 $aH = bH$, 故 φ 是单射. 又由于 φ 显然是满射, 故 φ 是双射. □

推论2.31 (计数公式)**.** 设 X 为 G-集.

(1) 如果 $x \in X$, 则 $|O_x| = [G : G_x]$.

(2) 如果X 为有限集, 则

$$|X| = \sum_{x \in I} |O_x| = \sum_{x \in I} [G : G_x]. \tag{2.11}$$

证明. 由命题 2.30, $|O_x| = |G/G_x| = [G : G_x]$, 故(1)成立. (2) 由(1) 及(2.5) 即得. □

命题2.32. 设 X 为 G-集, $x \in X, x' = ax \in O_x$, 则

(1) $\{g \in G \mid gx = x'\} = aG_x$.

(2) $G_{x'} = aG_xa^{-1} = \{g \in G \mid g = aha^{-1}, h \in G_x\}$.

证明. (1) 注意到 $gx = x' = ax$ 当且仅当 $a^{-1}gx = x$, 即 $a^{-1}g \in G_x$, 换言之 $g \in aG_x$.

(2) $gx' = x'$ 当且仅当 $gax = ax$, 即 $a^{-1}gax = x$, 亦即 $a^{-1}ga \in G_x$, $g \in aG_xa^{-1}$. □

例2.33. *在例 2.27 中, 对于平面上的任意一点 P, 稳定子群*

$$M_P = \tau_p \, \mathrm{O}_2(\mathbb{R}) \, \tau_P^{-1} = \tau_P \, \mathrm{O}_2(\mathbb{R}) \, \tau_{-P}.$$

例2.34. *二面体群 D_n 的阶为 $2n$. 事实上, D_n 在正 n 边形的 n 个顶点上的作用可迁, 且固定某一顶点的元素恰好为两个: 单位元和沿过此顶点和对称中心的直线的反射.*

§2.2.2 G 在集合 X 上的作用与 G 到群 S_X 的群同态的关系

设 X 是 G-集, 对于 $g \in G$,

$$\rho_g : X \longrightarrow X, \quad x \longmapsto gx$$

是 X 的双射, 事实上 $\rho_{g^{-1}}$ 是 ρ_g 的逆. 故 $\rho \in S_X$ (X 的对称群). 由此, 我们有映射

$$\rho : G \longrightarrow S_X, \quad g \longmapsto \rho_g, \tag{2.12}$$

并且由 $gh(x) = g(h(x))$, 我们有 $\rho_{gh} = \rho_g\rho_h$, 故 ρ 为群同态. 我们称 ρ 为**群作用诱导的同态** 或者说 ρ 为 G的一个**表示**.

反过来, 给定群同态 $\rho : G \to S_X$, 则对 $g \in G, x \in X$, 令 $gx = \rho(g)x$, 则我们定义了群 G 在 X 上的作用.

我们来讨论一下 ρ 的核. 如果 $\rho_g = 1$, 则对于所有的 $x \in X, gx = x$, 即 $g \in G_x$, 所以

$$\ker \rho = \bigcap_{x \in X} G_x. \tag{2.13}$$

由同态基本定理, 我们得到单同态

$$\bar{\rho} : G \Big/ \bigcap_{x \in X} G_x \longrightarrow S_X. \tag{2.14}$$

例2.35. 设 H 是 G 的子群, G/H 为 H 的左陪集集合, 则 G 在 H 上的左诱导表示的诱导映射为

$$\rho : G \longrightarrow S_{G/H},$$

其核为 $\ker\rho = \bigcap\limits_{g\in G} gHg^{-1}$.

命题2.36. $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$.

证明. 令向量空间 $V = \mathbb{F}_2^2 = \{0, e_1, e_2, e_1 + e_2\}$, 则 $\mathrm{GL}_2(\mathbb{F}_2)$ 通过$v \mapsto Av$ 作用在 V 上, 故也作用在 $X = V - \{0\}$ 上, 由此我们有同态

$$\rho : \mathrm{GL}_2(\mathbb{F}_2) \to S_3.$$

如果 $\rho_A = 1$, 则 $Ae_1 = e_1, Ae_2 = e_2$, 故 $A = I$, 所以 ρ 是单同态. 由于 $|\mathrm{GL}_2(\mathbb{F}_2)| = |S_3| = 6$, 故 ρ 是同构. □

习　　题

习题2.1. 设群 G 在集合 Σ 上的作用是传递的, N 是 G 的正规子群, 则 Σ 在 N 作用下的每个轨道有同样多的元素.

习题2.2. 设X 是$\mathbb{R}$ 上所有函数的集合. 验证

$$a \circ f(x) = f(ax)\ (a \in \mathbb{R}^\times)$$

给出乘法群$\mathbb{R}^\times$ 在X 上的作用, 并确定所有稳定子群为$\mathbb{R}_+^\times$ 的函数f.

习题2.3. 集合 $A \subseteq \mathbb{R}^n$ 的对称群是指将 A 映为自身的所有刚体变换得到的群.

(1) 求正方形, 除正方形外的长方形, 除正方形外的菱形, 圆的对称群.

(2) 求正四面体, 正立方体, 正八面体, 正十二面体, 正二十面体的对称群各有多少元素? 这五个对称群当中是否有同构的?

习题2.4. 设群 G 作用在集合Σ 上. 令 t 表示 Σ 在 G 作用下的轨道个数, 对任意 $g \in G$, $f(g)$ 表示 Σ 在 g 作用下的不动点个数. 试证

$$\sum_{g\in G} f(g) = t|G|.$$

这就是说, G 的每个元素在 Σ 上的作用平均使得 t 个元素不动.

习题2.5. 例 *2.26* 诱导了 $\mathrm{SL}_2(\mathbb{Z})$ 在 $\mathcal{H}$ 上的作用. 哪些点的稳定子群非平凡? 共有几个这样的轨道?

习题2.6. 设群 H 作用在群 N 上, 且每个元素 $g \in H$ 诱导了 N 上的群同构, 即有群同态 $\varphi : H \to \mathrm{Aut}(N)$. 令集合 $G = N \times H$, 定义运算

$$(x_1, y_1)(x_2, y_2) = (x_1 \cdot \varphi(y_1)(x_2), y_1 y_2).$$

(1) 证明 G 成为一个群, 称为 N 和 H 的**半直积** *(semidirect product)*, 记为 $G = N \rtimes H$.

(2) N 同构于 G 的一个正规子群, H 同构于 G 的一个子群. 由此说明上述定义等价于

$$N \lhd K,\ G \leqslant K,\ K = NG,\ N \cap G = \{1\},$$

此时 H 在 N 上的作用为内自同构.

(3) 证明 $G/N \cong H$.

(4) 证明 $S_n = A_n \rtimes \langle (12) \rangle$, 其中 $n \geqslant 3$.

习题2.7. 正四面体的 4 个顶点用 4 种颜色染色, 求真正不同的染色的方案个数.

§2.3 群在自身上的作用

§2.3.1 左乘作用

设 G 为群, 则群的乘法自然诱导 G 在自身上的作用

$$G \times G \to G, \quad (g, x) \mapsto gx, \tag{2.15}$$

此作用称为**左乘作用** (action by left multiplication). 由此诱导同态 $G \to S_G$. 由于对于 $x \in G$, $gx = x$ 当且仅当 $g = 1$, 故 $G_x = \{1\}$, ρ 为单同态. 由此, 我们有

定理2.37 (Caylay)**.** 每个有限群均是对称群的子群. 如果 G 的阶为 n, 则 G 是 S_n 的子群.

注记. 由于 $n!$ 随着 n 的增大而迅速增大, 这个定理在实际中的作用不大.

命题2.38. *设 G 的阶为 $2n$, 其中 n 为奇数, 则 G 有指数为 2 的子群, 故 G 不是单群.*

证明. 考虑 G 的左乘表示 $\rho : G \hookrightarrow S_{2n}$, 则我们可以将 G 视为 S_{2n} 的子群. 令 $H = G \cap A_{2n}$, 则

$$(G : H) \leqslant (S_{2n} : A_{2n}) = 2.$$

我们要证明 $(G : H) = 2$, 即 G 中存在奇置换.

事实上, 由于 G 中满足 $x^2 = 1$ 的元素为偶数, 故 G 中存在 2 阶元 σ, 它在 G 的左乘作用下的轨道必为 $\{a, \sigma(a)\}$ 的形式, 故

$$\sigma = (a_1\ \sigma(a_1))(a_2\ \sigma(a_2)) \cdots (a_n\ \sigma(a_n))$$

为 n 个对换的乘积, 为奇置换. 故得证.

设 $H \leqslant G$, $(G : H) = 2$. 令 $g \notin H$, 则 $G = H \bigsqcup Hg = H \bigsqcup gH$, 所以 $Hg = gH$, H 为 G 的正规子群. 故 G 不是单群. □

§2.3.2 共轭作用

群对自身的作用中, 更有意义的作用是**共轭作用** (action by conjugation), 即映射

$$G \times G \to G, \quad (g, x) \mapsto gxg^{-1}. \tag{2.16}$$

容易验证上述作用的确是群的作用. 对于 $x \in G$, 我们记

- $Z(x) = G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}$,
- $C_x = O_x = \{x' \in G \mid x = gxg^{-1}\}$.

子群 $Z(x)$ 是 G 中所有与x 可交换的元素的集合, 称为 x 的**中心化子** (centralizer), C_x 即 x 所在的**共轭类** (conjugate class).

由中心化子的定义, 我们知群 G 的中心 $Z(G)$ 即

$$Z(G) = \bigcap_{x \in G} Z(x) = \{g \in G \mid gx = xg, \text{ 对任意 } x \in G \text{ 成立}\}. \tag{2.17}$$

再由式 (2.13), 它就是共轭作用所诱导的同态 $\pi : G \to S_G$ 的核 $\ker \pi$.

由推论 2.31 的计数公式, 我们有

命题2.39. *设 G 为有限群, 则*

(1) $|G| = |C_x| \cdot |Z(x)|$.

(2) **类方程**成立*:*

$$|G| = \sum_{G \text{ 中共轭类}} |C_x| = |Z(G)| + \sum_{|C_x|\neq 1} |C_x|. \tag{2.18}$$

证明. 只需要证明类方程的第二个等式. 这是由于元素 $x \in Z(G)$ 当且仅当 $\{x\} = C_x$, 亦或 $Z(x) = G$. □

我们下面给出类方程的一些应用.

定义2.40. 如果有限群 G 的阶是素数 p 的方幂, 则称 G 为 p **群** (p-group).

命题2.41. *p 群的中心非平凡.*

证明. 由于 p 是 $|G|$ 的唯一素因子, 故也是所有 $|C_x|$ ($C_x \neq \{x\}$) 的素因子. 由 (2.18), p 整除 $|Z(G)|$, 所以 $Z(G)$ 非平凡. □

同理, 由公式 (2.18), 可以证明 (留作练习):

命题2.42. *设 G 为 p 群, X 是有限 G-集, 且 $p \nmid |X|$, 则存在 $x \in X$, 对所有 $g \in G, gx = x$, 即 X 中存在 G 作用下的不动点.*

命题2.43. *p^2 阶群 G 必为阿贝尔群.*

证明. 令 Z 为 G 的中心. 设 $Z \neq G$, 由命题 2.41, Z 非平凡, 故 $|Z| = p$. 令 $x \in G$ 但 $x \notin Z$, 则 $Z \subseteq Z(x)$ 且 $x \in Z(x)$, 故 $|Z(x)| > p$. 所以 $Z(x) = G$, 我们得到 $x \in Z$, 矛盾. 于是假设不成立, 所以 $Z = G$, 即 G 为阿贝尔群. □

命题2.44. *p^2 阶群或为循环群, 或为两个 p 阶循环群的乘积.*

证明. 如果 G 中包含 p^2 阶元, 则 G 为循环群. 否则 G 中所有非单位元的阶均为 p. 令 $1 \neq x \in G$, 且 $y \in G\backslash\langle x\rangle$. 则 $\langle x\rangle \cap \langle y\rangle = \{1\}$. 考虑映射

$$\varphi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G, \quad (m, n) \mapsto x^m y^n.$$

我们容易验证 φ 为同态. 如果 $\varphi(m, n) = 1$, 则 $x^m = y^{-n} \in \langle x\rangle \cap \langle y\rangle$, 故 $m = n = 0$, 所以 φ 为单同态. 由于 $|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}| = p^2 = |G|$, 所以 φ 为同构. □

§2.3.3 G 在 H 上的共轭作用

设 H 为 G 的子群. 令 $X_H = \{gHg^{-1} \mid g \in G\}$, 即 X_H 为所有与 H 共轭的群的集合. 注意到

$$X_H = \{H\} \text{ 当且仅当 } H \lhd G. \tag{2.19}$$

G 在 X_H 上的**共轭作用**为

$$\begin{aligned} G \times X_H &\longrightarrow X_H \\ (g, aHa^{-1}) &\longmapsto gaHa^{-1}g^{-1} = (ga)H(ga)^{-1}. \end{aligned}$$

我们容易验证, G 在 X_H 上的作用可迁.

定义2.45. H 关于 G 的**正规化子** (normalizer)为

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}, \tag{2.20}$$

即为 H 在共轭作用下的稳定子群.

由计数公式 (2.11), 我们有

$$|G| = |N_G(H)| \cdot |X_H|,$$

故由公式 (2.19)有

$$N_G(H) = G \text{ 当且仅当 } H \lhd G. \tag{2.21}$$

令 $\pi : G \to S_{X_H}$ 为 G 在 X_H 上的共轭作用诱导的同态, 则

$$\ker \pi = \bigcap_{a \in G} G_{aHa^{-1}} = \bigcap_{a \in G} aN_G(H)a^{-1}. \tag{2.22}$$

例2.46. 如果 $(G : N) = p$, 且 p 为 $|G|$ 的最小素因子, 则 $N \lhd G$.

证明. 考虑 G 在 N 的左陪集表示, 我们得到群同态

$$\rho_N : G \to S_p.$$

其核 $\ker \rho_N = \bigcap\limits_{a \in G} a^{-1}Na \lhd N$. 我们有

- 由同态基本定理, $G/\ker\rho_N$ 为 S_p 的子群, 故 $(G:\ker\rho_N)$ 是 $p!$ 的因子;
- $|G|$ 没有小于 p 的素因子;
- $p=(G:N)$ 是 $(G:\ker\rho_N)$ 的因子.

故 $p=(G:\ker\rho_N)$ 且 $N=\ker\rho_N$. □

习 题

习题3.1. 确定 $\mathrm{GL}_2(\mathbb{F}_5)$ 中 $\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$ 的共轭类的阶.

习题3.2. 设 p 是素数, G 是 p 的方幂阶的群. 试证 G 子群中非正规子群的个数一定是 p 的倍数.

习题3.3. 令 G 是单群, 如果存在 G 的真子群 H 使得 $[G:H]\leqslant 4$, 则 $|G|\leqslant 3$.

习题3.4. 设 H 是无限群 G 的有限指数真子群, 则 G 一定含有一个有限指数的真正规子群.

习题3.5. 证明$\mathrm{GL}_n(R)$ 的上三角矩阵构成的子群与下三角矩阵构成的子群共轭.

习题3.6. 证明命题 *2.42*.

习题3.7. 一般线性群 $\mathrm{GL}_n(\mathbb{C})$ 不含有指数有限的真子群.

习题3.8. 令 G 是阶数为 2^nm 的群, 其中 m 是奇数. 如果 G 含有一个 2^n 阶的元素, 则 G 含有一个指数为 2^n 的正规子群.

习题3.9. 将S_n 视为 $\mathrm{GL}_n(R)$ 的置换矩阵构成的子群. 确定 S_n 在 $\mathrm{GL}_n(R)$中的正规化子.

习题3.10. 求对称群 S_3 的自同构群 $\mathrm{Aut}(S_3)$.

习题3.11. 设 α 是有限群 G 的自同构. 若 α 把每个元素都变到它在 G 中的共轭元素, 即对任意 $g\in G$, g 和 $\alpha(g)$ 共轭, 则 α 的阶的素因子都是 $|G|$ 的因子.

习题3.12. 设 p 是 $|G|$ 的最小素因子. 若 p 阶子群 $A \lhd G$, 则 $A \leqslant Z(G)$.

习题3.13. 令 $G = \mathrm{GL}_n(\mathbb{C})$, $T = T_n(\mathbb{C})$ 为 G 中对角线元全为 1 的上三角阵构成的子群. 确定 $N_G(T)$, $Z_G(T)$ 和 T 的中心 $Z(T)$.

习题3.14. 设 $N \lhd G$, M 是 G 的子群且 $N \leq M$, 则 $N_G(M)/N = N_{\overline{G}}(\overline{M})$, 这里 $\overline{G} = G/N$, $\overline{M} = M/N$.

习题3.15. 试证有限群 G 的一个真子群的全部共轭子群不能覆盖整个群 G. 结论对无限群是否成立?

习题3.16. 设 K是群 G的一个 2 阶正规子群, 且设 $\overline{G} = G/K$. 设 $\overline{C}$ 是 $\overline{G}$ 的一个共轭类. 设 S是 $\overline{C}$ 在 G 中的逆像. 证明下列两种情形之一必成立:

(1) $S = C$ 是单独一个共轭类且 $|C| = 2|\overline{C}|$。

(2) $S = C_1 \bigcup C_2$ 由两个共轭类组成且 $|C_1| = |C_2| = |\overline{C}|$。

习题3.17. (1) 若 $G/Z(G)$ 是循环群, 证明 G 为阿贝尔群, 故非交换有限群 G 的中心 $Z(G)$ 的指数 $\geqslant 4$.

(2) 如果 G 为 n 阶有限群, t 为 G 中共轭类的个数, $c = \frac{t}{n}$. 证明 $c = 1$ 或者 $c \leqslant \frac{5}{8}$.

§2.4 Sylow 定理及其应用

本节将讨论有限群论中最主要的一个定理: Sylow 定理.

§2.4.1 Sylow 定理

设 G 为 n 阶有限群. 设 p 为 n 的一个素因子, 记 $n = p^r m$, 其中 p 与 m 互素. 一个自然的问题是, G 中是否含有 p 阶元? 更进一步地, G 中是否存在 p^r 阶子群?

定义2.47. 阶为 p^r 的子群称为 G 的 **Sylow p子群** (Sylow p-subgroup).

定理2.48 (Sylow 第一定理)**.** *G 中存在 Sylow p子群.*

证明. 设 X 为 G 中所有 p^r 元子集构成的族, 即

$$X = \{U \subseteq G \mid |U| = p^r\}.$$

则

$$N = |X| = \binom{mp^r}{p^r} = \frac{mp^r \cdot (mp^r - 1) \cdots (mp^r - p^r + 1)}{1 \cdot 2 \cdots p^r}.$$

由于 i 与 $mp^r - i (1 \leqslant i \leqslant p^r - 1)$ 被 p 整除的次数一样, 我们有 $(p, N) = 1$.

考虑 G 在 X 上的左乘作用, 必存在一个轨道, 不妨设为 $O_U (U \in X)$, $|O_U|$ 与 p 互素. 由计数公式 (2.11), $U = \bigcup\limits_{x \in U} G_U x$ 是 G_U 的一些陪集的并, 故 $|G_U|$ 是 p 的方幂. 由公式 (2.11), $|G_U| \cdot |O_U| = |G|$, 由于 $|G_U|$ 是 p 的幂, $|O_U|$ 与 p 互素, 故 $|G_U| = p^r$, 所以 G_U 是 G 的 Sylow p子群. □

定理2.49 (Sylow 第二定理)**.** *设 K 为 G 的子群, 且 p 整除 K 的阶, H 是 G 的一个 Sylow p子群. 则存在 $H' = gHg^{-1}$ 使得 $H' \cap K$ 是 K 的 Sylow 子群.*

证明. 我们知道 G 在 $X = G/H = \{gH \mid g \in G\}$ 上的左乘作用可迁, 且对于 $x = aH \in X$, 它的稳定子群是 aHa^{-1}.

将 G 在 X 上的作用限制到 K 在 X 上的作用. 由于 $|X| = m$, 故存在 K-轨道 O_x, $|O_x|$ 与 p 互素, 此时 $K_x = G_x \cap K = aHa^{-1} \cap K$, 它的阶为 p 的幂次. 由 $|O_x| \cdot |K_x| = |K|$, 故 K_x 的阶恰好为 $|K|$ 的 p 部分, 即 K_x 是 K 的 Sylow p子群. □

由 Sylow 第二定理, 我们有

推论2.50. (1) *如果 $K \leqslant G$ 是 p 群, 则 K 是 G 的某个 Sylow p子群 H 的子群.*

(2) *所有 G 的 Sylow p子群共轭.*

证明. (1) 由于 K 是 p 群, 因此 K 的 Sylow p 子群是自身, 故 $H' \cap K = K$, 即 $K \leqslant H'$.

(2) 设 H, H_1 为 G 的两个 Sylow p子群. 由 Sylow 第二定理, 存在 $H' = gHg^{-1}$ 使得 $H' \cap H_1 = H_1$, 但由于 $|H_1| = |H|$, 我们有 $H_1 = H' = gHg^{-1}$, 它与 H 共轭. □

定理2.51 (Sylow 第三定理)**.** *令$X_H = \{aHa^{-1} \mid a \in G\}$, 且记*

$$N(p) = |X_H| = G \text{ 的 } Sylow\ p \text{ 子群的个数}. \tag{2.23}$$

则 $N(p) \equiv 1 \mod p$.

证明. 我们知道 G 在 X_H 上的共轭作用可迁, 且 $N(p) = (G : N)$, 其中 $N = N_G(H)$. 我们将 X_H 分解为 H 在其上的共轭作用的轨道. 如果轨道中只有一个元素 H_i, 则 $H \leqslant N_G(H_i)$. 另一方面, $H_i \lhd N_G(H_i)$ 是 $N_G(H_i)$ 唯一的 Sylow p子群, 故 $H = H_i$. 这说明仅包含一个元素的轨道只有 $\{H\}$.

对于其他轨道 O_{H_i}, 由于

$$|O_{H_i}| \cdot |N_G(H_i) \cap H| = |H|$$

且 $N_G(H_i) \cap H$ 是 H 的真子群, 故 $p \mid |O_{H_i}|$. 综上所述, $N(p) \equiv 1 \mod p$. □

上面的 Sylow 第一, 第二, 第三定理常常综合为如下定理:

定理2.52 (Sylow 定理)**.** 设 G 为有限群, 其阶为 $p^r m$, 其中 $(m, p) = 1$, 则

(1) G 中存在 *Sylow* p子群, 即阶为 p^r 的子群.

(2) 所有 G 中的 *Sylow* p子群共轭.

(3) G 的 *Sylow* p子群个数 $N(p) \equiv 1 \mod p$ 且 $N(p) \mid m$.

> 路德维希 · 希洛(*Ludwig Sylow, 1832*年*12* 月*12*日 – *1918*年*9*月 *7*日, 图 *2.1*) 是挪威数学家, 长期担任高中数学教师. *1862*年在克里斯蒂安尼亚大学*(*现奥斯陆大学*)* 当代课讲师, 教授伽罗瓦理论时, 他提出的问题最终导致他发现希洛子群和希洛定理, 希洛定理在*1872*年发表. 希洛还花了 *8*年时间和索福斯 · 李(*Sophus Lie,* 李群李代数的发现者) 一起编辑阿贝尔的数学全集.

§2.4.2 Sylow 定理的应用

Sylow 定理在研究有限群的结构中起着关键作用. 我们首先证明一个引理.

引理2.53. 设 H, K 是群 G 的正规子群, 且满足条件 $HK = G$, $H \cap K = \{1\}$. 则 $G \cong H \times K$.

证明. 设 $h \in H, k \in K$, 则

$$khk^{-1}h^{-1} = (khk^{-1})h^{-1} \in H \quad \text{且} \quad khk^{-1}h^{-1} = k(hk^{-1}h^{-1}) \in K.$$

图 2.1: 希洛像

故 $khk^{-1}h^{-1}=1$, 即 $hk=kh$. 记

$$\varphi: H\times K\to G,\quad (h,k)\mapsto hk,$$

则

$$\begin{aligned}&\varphi((h_1,k_1)(h_2,k_2))=\varphi(h_1h_2,k_1k_2)\\ =&h_1h_2k_1k_2=h_1k_1h_2k_2=\varphi(h_1,k_1)\varphi(h_2,k_2),\end{aligned}$$

故 φ 是群同态. 由 $HK=G$, φ 为满同态. 若 $hk=1$, 则 $h=k^{-1}\in H\cap K, h=k=1$, 故 φ 为单同态, 所以 φ 为同构. □

例2.54. 150 阶群不是单群. 事实上, 首先 $N(5)=1$ 或 6. 如果 $N(5)=1$, 则 G 不是单群. 如果 $N(5)=6$, 设 H 为 G 的一个 *Sylow* 5子群, 则 G 在 H 的左陪集作用诱导同态

$$\rho: G\to S_6.$$

由于 $150\nmid 6!$, 故 $\ker\rho\neq\{1\}$, 因此 $\ker\rho$ 为 G 的非平凡正规子群.

命题2.55. *设 p,q 为不相同的奇素数, 则*

(1) *pq 阶群不是单群.*

(2) *p^2q 阶群也不是单群.*

证明. 由于素数幂次群有非平凡中心, 它们均不是单群. 不妨假设 $p \neq q$.

(1) 不妨设 $p < q$, 则由 $N(q) = 1$ 或 p 且 $N(q) \equiv 1 \mod q$ 有 $N(q) = 1$, 即 Sylow p子群是 G 的正规子群.

(2) 如果 $p > q$, 则同上推理 $N(p) = 1$, G 不是单群. 如果 $p < q$, 则 $N(p) = 1$ 或 q 且 $N(q) = 1$ 或 p^2(由于 $p \not\equiv 1 \mod q$, $N(q)$ 不可能等于p). 如果 $N(q) = p^2$, 则 G 中有 p^2 个 q 阶循环群, G 的 q 阶元个数为 $p^2(q-1)$, 故 G 中 p 幂次元最多有 p^2 个, 即 $N(p) = 1$. □

定理2.56. *最小有限非阿贝尔单群 G 同构于 A_5, 即*

(1) *如果 $|G| < 60$, G 不是非阿贝尔单群.*

(2) *如果 $|G| = 60$ 且 G 为非阿贝尔单群, 则 $G \cong A_5$.*

证明. (1) 我们已知

(i) 素数阶群均是循环群(推论 1.61);

(ii) 素数幂次(次数$\geqslant 2$)阶群不是单群(命题 2.41);

(iii) pg, p^2q 阶群(p,q 为不相同的奇素数) 不是单群(命题 2.55);

(iv) $2m$(m 为奇数) 阶群不是单群(命题 2.38).

故只需考虑 $n = |G| = 24, 36, 40, 48, 56$.

(a) $n = 24 = 2^3 \cdot 3$, 则 $N(2) = 1$ 或 3. 若 $N(2) = 3$, 设 H 为 G 的 Sylow 2 子群. G 在 X_H 上的共轭作用诱导同态 $\rho : G \to S_3$. 由于 ρ 不是平凡同态, 且 $24 > 6$, 故 $\ker\rho \neq \{1\}$ 是 G 的正规子群, 故G 非单. 同理可得 $n = 48$ 的情形.

(b) $n = 36$, 则 $N(3) = 1$ 或 4. G 在 Sylow 3 子群上的共轭作用得到同态 $\rho : G \to S_4$. 由于 ρ 不是平凡同态, 且 $36 > 24$, 故 $\ker\rho \neq \{1\}$ 是 G 的正规子群, G 非单.

(c) $n = 40$, 则 $N(5) \mid 8$ 且 $N(5) \equiv 1 \mod 5$, 我们有 $N(5) = 1$.

(d) $n = 56 = 7 \times 8$, $N(7) = 1$ 或 8, $N(2) = 1$ 或 7. 如果 $N(7) = 8$, 则 G 中 7 阶元素有 $8 \times (7-1) = 48$个, 其它阶元素只有 8个, 故 $N(2) = 1$, G 不是单群.

(2) 我们现在假设 $|G| = 60$ 且 G 为非阿贝尔单群.

(a) G 中没有指数 $\leqslant 4$ 的子群. 事实上, 如果 $[G : H] = m$, 则G 在 H 的左陪集上的表示诱导非平凡同态 $\rho : G \to S_m$. 如果 $m \leqslant 4$, 则 $\ker \rho \neq \{1\}$ 为G 的非平凡正规子群.

(b) 我们断言 G 中有指数为 5 的子群 H, 即 $|H| = 12$. 事实上, 考虑 G 的 Sylow 2 子群, 由(a)且 G 是单群知, $N(2) = 5$ 或15.

如果 $N(2) = 5$, 则可取 H 为 Sylow 2 子群的正规化子.

如果 $N(2) = 15$, 由于 $N(5) = 6$ 且 $N(3) = 10$, G 中 5 阶元和 3 阶元有 $24+20 = 44$ 个元素, 故必存在 G 的 Sylow 2 子群 $P_1, P_2, K = P_1 \cap P_2 \neq \{1\}$. 现在考虑 P_1, P_2 生成的群 H, 则由于 P_1, P_2 均为阿贝尔群, $H \lhd C_G(K) \neq G$. 而 $P_1 \neq H$, 故 H 的阶只能是 12 或 15, 但由(a)知 H 只能是 12 阶群.

(c) 考虑 G 在 H 的左陪集上的表示, 则有非平凡同态 $\rho : G \to S_5$, 故 $\ker \rho = \{1\}$, 即ρ 为单同态. 因此G 同构于 S_5 的一个 60 阶子群 M. 由 $\{1\} \neq M \cap A_5 \lhd A_5$ 知 $M = A_5$. □

习 题

习题4.1. *若 p 是 $|G|$ 的素因子, 则群 G 必有 p 阶元素.*

习题4.2. *给出 $\mathrm{GL}_n(\mathbb{F}_p)$ 的一个 Sylow p子群, 并求出 $\mathrm{GL}_n(\mathbb{F}_p)$ 中Sylow p 子群的个数.*

习题4.3. *设 G 是 n 阶群, p 是 n 的素因子. 证明方程 $x^p = 1$ 在群 G 中的解的个数是 p 的倍数.*

习题4.4. *证明 6 阶非阿贝尔群只有 S_3.*

习题4.5. *证明 150, 148, 200 阶群不是单群.*

习题4.6. *求对称群 S_4 的自同构群 $\mathrm{Aut}(S_4)$.*

习题4.7. *设 N 是有限群 G 的正规子群. 如果 p 和 $|G/N|$ 互素, 则 N 包含 G 的所有 Sylow p子群.*

习题4.8. 设 G 是有限群, N 是 G 的正规子群, P 是 G 的一个 *Sylow* p子群. 证明*:*

(1) $N \cap P$ 是 N 的 *Sylow* p子群*;*

(2) PN/N 是 G/N 的 *Sylow* p子群*;*

(3) $N_G(P)N/N \cong N_{G/N}(PN/N)$.

习题4.9. 令 $P_1, \ldots, P_N$ 是有限群 G 的全部 *Sylow* p子群. 如果对任意 $i \neq j$, 总有

$$|P_i : P_i \cap P_j| \geqslant p^r,$$

则 $N \equiv 1 (\mathrm{mod}\ p^r)$.

习题4.10. 证明*:* 若 G 的阶为 $n = p^e a$, 其中 $1 \leq a < p$, 且 $e \geq 1$, 则 G 一定有真正规子群.

习题4.11. 令 G 是集合 Σ 上的置换群, P 是 G 的 *Sylow* p子群, $a \in \Sigma$. 如果 p^m 整除 $|Ga|$, 则 p^m 整除 $|Pa|$.

习题4.12. 令 G 是集合 Σ 上的置换群. 对任意 $a \in \Sigma$, 设 P 是稳定子群 G_a 的 *Sylow* p子群, Δ 是轨道 Ga 在 P 作用下的全部不动点的集合. 证明 $N_G(P)$ 在 Δ 上的作用是传递的.

习题4.13. 设群 G 是 24 阶群且其中心平凡, 证明 G 同构于 S_4.

习题4.14. 证明*:* 没有 224 阶单群.

习题4.15. 设 P 是 G 的 *Sylow* p子群且 $N_G(P)$ 是 G 的正规子群. 证明 P 是 G 的正规子群.

§2.5 自由群与群的表现

§2.5.1 自由群

设 S 为任意集合. 我们期望由 S 来生成一个群 $F(S)$.

首先, 我们来看由字母生成字的过程: 将一串字母串起来, 就构成了一个字. 如此类比, 可以认为 $F(S)$ 是由 S 中的元素作为字母生成的字的全体, 但由于需要在 $F(S)$ 上得到群的结构, 因此

(i) $F(S)$ 上需要有**乘法**. 如果 $w_1 = x_1 \cdots x_n, w_2 = y_1 \cdots y_m$, 则乘法是将 w_1 与 w_2 串联起来, 得到

$$w_1 \cdot w_2 = x_1 x_n y_1 \cdots y_m.$$

(ii) $F(S)$ 中每个字需要有**逆元**. 特别地, 如 $x_1 \in S$, 则 $x_1^{-1} \in F(S)$ 且对于 $x_i \in S \cup S^{-1}$, $x_1 \cdots x_n \in F(S)$.

(iii) $F(S)$ 中需要有**单位元**. 它与任何其它字 w 串联起来还是 w.

由(i)-(iii),

$$F(S) = \{1\} \cup \{x_1 x_2 \cdots x_n \mid x_i \in S \cup S^{-1}, 1 \leqslant i \leqslant n\}. \tag{2.24}$$

这里还有一个问题. 由结合律知形如

$$w = \cdots x a a^{-1} y \cdots$$

的字应该与 $w' = \cdots xy \cdots$ 一样, 也就是可以消去其中字母串 aa^{-1} 得到简化. 但在一个字中可以有不同的简化方式, 例如

$$\begin{aligned} w = x^{-1}x(yy^{-1})x^{-1}yz &\ \to\ x^{-1}(xx^{-1})yz \ \to\ x^{-1}yz \\ w = (x^{-1}x)yy^{-1}x^{-1}yz &\ \to\ (yy^{-1})x^{-1}yz \ \to\ x^{-1}yz \end{aligned}$$

定义2.57. 字 w 称为**简化字**(或称**既约字**), 如果 w 中没有形如 $a^{-1}a (a \in S \cup S^{-1})$ 的字串.

命题2.58. *对一给定的字, 有唯一的简化(既约)形式.*

证明. 我们对字的长度 n 作归纳法. 如果 $n = 1$, 则它肯定是简化字. 在一般情况下, 如果 $w = \cdots xx^{-1} \cdots$ 的形式. 我们考虑将 w 变为简化字的过程.

(i) 如果在第 i 步消去 xx^{-1}, 我们可以将第 i 步换到第1步, 消去后得到的字的长度为 $n-2$. 由归纳假设可得唯一简化形式.

(ii) 如果在第 i 步, x 或 x^{-1} 中有一个消掉, 则第 $i-1$ 步时必为

$$\cdots x^{-1}(xx^{-1}) \cdots \quad \text{或} \quad \cdots (xx^{-1})x \cdots$$

的形式, 此时消去 $x^{-1}x$ 与消去 xx^{-1} 效果是一样的, 我们又归结到(i)的情形. □

定义2.59. 我们称 $w \sim w'$, 如果 w 与 w' 有相同的简化形式.

命题2.60. *如果 $w \sim w', u \sim u$, 则 $wu \sim w'u'$.*

证明. 设 w_0 为 w 与 w' 的简化形式, u_0 为 u 与 u' 的简化形式, 则 wu 经简化可得 w_0u_0(不一定是简化字!), 同理 $w'u'$ 简化后得 w_0u_0, 故 $wu \sim w'u'$. □

由命题 2.60, 我们有如下定义

定义2.61. 群

$$F(S) = \{1\} \cup \{x_1x_2\cdots x_n \mid x_i \in S \cup S^{-1}\} \tag{2.25}$$

称为由 S 生成的**自由群** (free group), 其乘法为字的串联, 且两个字相等当且仅当它们有相同的简化形式. 如果 S 有限, 称 $F(S)$ 为**有限生成自由群** (finitely generated free group).

例如 $S = \{a\}$, 则 $F(S) = \langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$ 为无限循环群. 如果 $|S| \geqslant 2$, $F(S)$ 为无限非阿贝尔群.

定理2.62 (自由群的泛性质)**.** *设 G 为群, S 为集合, $f : S \to G$ 为集合间的映射, 则 f 可以唯一扩充为群同态 $\varphi : F(S) \to G$.*

证明. 对 $w = a_1\cdots a_n, a_i \in S \cup S^{-1}$, 只需定义

$$\varphi(a_1\cdots a_n) = \varphi(a_1)\cdots\varphi(a_n)$$

且

$$\varphi(a_i) = \begin{cases} f(a_i), & \text{若 } a_i \in S, \\ f(a_i^{-1})^{-1}, & \text{若 } a_i \in S^{-1}. \end{cases}$$

则 φ 为唯一的延拓 f 的群同态. □

在定理 2.62的条件中取 $S \subseteq G$, 如果 S 生成 G, 则 $\varphi : F(S) \to G$ 是群的满同态, 即 G 为 $F(S)$ 的商群. 特别地

(1) 取 $S = G$, 我们得到 G 是自由群的商群.

(2) 如果 S 有限, 即 G 为有限生成群, 则 G 是有限生成自由群的商群.

综上所述, 我们有定理

定理2.63. *每个群都是自由群的商群, 每个有限生成群都是有限生成自由群的商群.*

§2.5.2 群的表现

设 G 为群, 根据定理 2.63, 存在集合 $S \subseteq G$ 使得 G 是自由群 $F(S)$ 的商群, 即 $G = F(S)/N$. 如果 G 是有限生成的, 我们可以假设 S 为有限集.

定义2.64. 如果 $G = F(S)/N$, 则 G 的**表现** (presentation)记为

$$\langle S \mid r = 1, \text{ 其中 } r \in N\rangle.$$

特别地, 如果 $R = \{r_1, \cdots, r_n\} \subseteq N$ 且包含 R 的最小正规子群为 N, 则 G 的表现为

$$G = \langle S \mid r_1 = r_2 = \cdots = r_n = 1\rangle.$$

S 中的元素称为 G 的**生成元** (generator), N 中的元素(或 R 中的元素)构成生成元的**生成关系** (relation).

例2.65. 循环群 $\mathbb{Z}/n\mathbb{Z} \cong \langle a\rangle/\langle a^n\rangle$, 从而可以表现为 $\langle a \mid a^n = 1\rangle$.

例2.66. 二面体群 D_n 的表现. 首先二面体群有生成元 σ(旋转), τ(反射), 其中 $\sigma^n = \tau^n = 1$ 且 $(\sigma\tau)^2 = 1$. 令 $S = \{\sigma, \tau\}$, 则 $S \hookrightarrow D_n$ 诱导 $F(S) \to D_n$ 的满同态 φ. 令 $N = \ker\varphi$, 则我们有 $\sigma^n, \tau^2, (\sigma\tau)^2 \in N$. 令 K 是由 $\sigma^n, \tau^2, (\sigma\tau)^2$ 生成的正规子群, 则 $K \subseteq N$, 即有

$$F(S)/K \twoheadrightarrow F(S)/N \twoheadrightarrow D_n.$$

另一方面, $F(S)/K$ 中的元素均可写为 $\sigma^i\tau^j (0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant 1)$ 的形式, 故 $|F(S)/K| \leqslant 2n$, 所有我们必有 $K = N$, 于是

$$D_n = \langle \sigma, \tau \mid \sigma^n = \tau^2 = (\sigma\tau)^2 = 1\rangle.$$

我们下面来讨论群 G 的换位子群.

定义2.67. 设 G 为群. 对于 $a, b \in G$, a, b 的**换位子** (commutator) $[a, b]$ 定义为 $aba^{-1}b^{-1}$. 由 G 中所有换位子生成的子群称为 G 的**换位子群** (commutator subgroup), 记为 $G' = [G, G]$.

命题2.68. (1) G' 是 G 的正规子群, G/G' 为阿贝尔群.

(2) 设 A 为阿贝尔群, $\varphi : G \to A$ 为满同态, 则 $\ker\varphi \supseteq G'$, 且 φ 诱导同态

$$\overline{\varphi} : G/G' \to A, \quad \overline{\varphi}(\overline{g}) = \varphi(g).$$

注记. 由命题可知 G/G' 是 G 的最大阿贝尔商群.

证明. (1) 我们有

$$g[a,b]g^{-1}=[ga,b][b,g],$$

故 $G'\lhd G$. 由 $\overline{a}\,\overline{b}\,\overline{a^{-1}}\,\overline{b^{-1}}=1$, 故 $\overline{a}\,\overline{b}=\overline{b}\,\overline{a}$, 即 G/G' 是阿贝尔群.

(2) 由 φ 为同态知

$$\varphi([a,b])=\varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1}=1,$$

故 $[a,b]\in\ker\varphi, G'\lhd\ker\varphi$, 所以我们有

$$\varphi: G\to G/G'\to G/\ker\varphi\to A,$$

得到诱导同态 $\overline{\varphi}: G/G'\to A$. □

命题2.69. 设 $\varphi: F(S)\to G$ 为满同态. 则 φ 诱导满同态

$$\overline{\varphi}: F(S)/F(S)'\to G/G',\quad \overline{\varphi}(\overline{g})=\overline{\varphi(g)}.$$

证明. 我们有同态

$$\varphi: F(S)\to G\to G/G',$$

再由命题 2.68(2) 立得. □

由命题 2.69 可知, 如果 G 的表现为

$$G=\langle S\mid r_1=r_2=\cdots=r_n=1\rangle,$$

则G/G' 的表现为

$$G/G'=\langle S\mid r_1=r_2=\cdots=r_n=1, xy=yx, \text{ 对任意的 } x,y\in S\rangle.$$

特别地, $F(S)/F(S)'$ 的表现为

$$F(S)/F(S)'=\langle S\mid xy=yx, \text{ 对任意的 } x,y\in S\rangle.$$

我们将在下节详细讨论此群.

习　　题

习题5.1. 证明或推翻: 两个生成元的自由群同构于两个无限循环群的积.

习题5.2. 设 F 是 x, y 生成的自由群.

(1) 证明两个元素 $u = x^2$ 和 $v = y^3$ 生成 F 的一个子群, 它同构于 u, v 上的自由群.

(2) 证明三个元素 $u = x^2$, $v = y^2$ 和 $z = xy$ 生成 F 的一个子群, 它同构于 u, v, z 上的自由群.

习题5.3. 若 n 为正奇数,求证: $D_{2n} \cong D_n \times \mathbb{Z}/2\mathbb{Z}$.

习题5.4. 若 $n \geq 3$, $A_n \times \mathbb{Z}/2\mathbb{Z}$ 与 S_n 是否同构?

习题5.5. 设 $G = G_1 \times \cdots \times G_n$, H 为 G 的子群. 问 H 是否一定形如 $H = H_1 \times \cdots \times H_n$, 其中 $H_i \leqslant G_i, 1 \leqslant i \leqslant n$.

习题5.6. 设 G_1 和 G_2 是两个非交换单群. 证明 $G_1 \times G_2$ 的非平凡正规子群只有 G_1 和 G_2.

习题5.7. 证明 $5 \cdot 7 \cdot 13$ 阶群一定是循环群.

习题5.8. (1) 求出圆的对称群.

(2) 求出球的对称群.

(3) 试求出圆柱体的对称群.

习题5.9. 给定两个水平平面, 在顶面有三个点, 它们在底面有正投影. 把顶面的三个点与底面的正投影分别用三根不相交的绳子连接起来, 且每根绳子与两平面之间的每一个水平面恰好相交一次, 这样的三根绳子称为一个 **3-辫子**. 给定两个 3-辫子 a, b, 将 b 放在 a 下面连接起来得到一个新的辫子, 称为 a 和 b 的乘法. 试证明所有的 3-辫子构成一个群, 并确定它的表现.

习题5.10. 设 G 由 n 个元素生成, 而 G 的子群 A 具有有限指数. 求证: A 可以由 $2n[G : A]$ 个元素生成.

习题5.11. 令 $G = G_1 \times G_2 \times \cdots \times G_n$, 且对任意 $i \neq j$, $|G_i|$ 和 $|G_j|$ 互素. 证明 G 的任意子群 H 都是它的子群 $H \cap G_i$ $(i = 1, 2, \cdots, n)$ 的直积.

§2.6 有限生成阿贝尔群的结构

§2.6.1 有限生成自由阿贝尔群

定义2.70. 群

$$\mathbb{Z}(S) = F(S)/F(S)' = \langle S \mid xy = yx,\ x, y \in S \rangle \tag{2.26}$$

称为由 S 生成的**自由阿贝尔群** (free abelian group).

如果 S 为有限集, 称 $\mathbb{Z}(S)$ 为**有限生成自由阿贝尔群** (finitely generated free abelian group).

定义2.71. 设 S 为集合, **直和** (direct sum) $\bigoplus\limits_{x\in S}\mathbb{Z}$ 定义为

$$\bigoplus_{x\in S}\mathbb{Z} = \{(a_x)_{x\in S} \mid a_x \in Z \text{ 且只有有限个 } a_x \neq 0\}.$$

由定义知 $\bigoplus\limits_{x\in S}\mathbb{Z}$ 在加法意义下构成阿贝尔群, 且当 S 为有限集时, $\bigoplus\limits_{x\in S}\mathbb{Z} \cong \mathbb{Z}^{|S|}$.

定理2.72. (1) $\mathbb{Z}(S) \cong \bigoplus\limits_{x\in S}\mathbb{Z}$.

(2) 如果 $m \neq n$, 则 $\mathbb{Z}^m$ 与 $\mathbb{Z}^n$ 不同构.

证明. 令

$$f : S \longrightarrow \bigoplus_{x\in S}\mathbb{Z}, \quad x \longmapsto a_x = (a_{x,y})_{y\in S}$$

为映射, 其中 $a_{x,x} = 1$ 且 $a_{x,y} = 0$ 如果 $x \neq y$. 由自由群的泛性质(定理 2.62), f 可以唯一扩充为满同态

$$\varphi : F(S) \longrightarrow \bigoplus_{x\in S}\mathbb{Z}.$$

再由于 $\bigoplus\limits_{x\in S}\mathbb{Z}$ 是阿贝尔群, 由命题 2.68, 我们得到满同态

$$\overline{\varphi} : \mathbb{Z}(S) \longrightarrow \bigoplus_{x\in S}\mathbb{Z}.$$

由 $\mathbb{Z}(S)$ 的定义, 任何 $\mathbb{Z}(S)$ 中的元素可以写成 $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ 的形式, 其中 $\alpha_i \in \mathbb{Z}, x_i$ 两两不同, 故

$$\overline{\varphi}(x_1^{\alpha_1}\cdots x_n^{\alpha_n}) = \alpha_1 a_{x_1} + \cdots + \alpha_n a_{x-n}.$$

$\overline{\varphi}(x_1^{\alpha_1}\cdots x_n^{\alpha_n}) = 0$ 等价于 $\alpha_1, \cdots, \alpha_n = 0$, 即 $x_1^{\alpha_1}\cdots x_n^{\alpha_n} = 1$, 故 $\overline{\varphi}$ 为单同态, 所以

$$\overline{\varphi} : \mathbb{Z}(S) \xrightarrow{\sim} \bigoplus_{x\in S} \mathbb{Z}.$$

(2) 如果 $m \neq n$, 且有同构 $\tau : \mathbb{Z}^m \to \mathbb{Z}^n$, 则 $\tau((k\mathbb{Z})^m) = (k\mathbb{Z})^n$ 对所有 $k \geqslant 2$ 成立, 故 τ 诱导同构

$$\mathbb{Z}^m/(k\mathbb{Z})^m \xrightarrow{\sim} \mathbb{Z}^n/(k\mathbb{Z})^n.$$

但上式左边元素个数等于 k^m, 右边元素个数等于 k^n, 矛盾! □

由定理 2.72, 立知

推论2.73. *有限生成自由阿贝尔群 $\mathbb{Z}(S)$ 同构于 $\mathbb{Z}^{|S|}$, 且在同构意义下, $\mathbb{Z}(S)$ 由 $|S|$ 唯一确定.*

定义2.74. 有限生成自由阿贝尔群 $\mathbb{Z}(S)$ 的生成元 S 称为 $\mathbb{Z}(S)$ 的一组**基** (basis), $|S|$ 称为 $\mathbb{Z}(S)$ 的**秩** (rank), 记为 $\operatorname{rank}\mathbb{Z}(S)$.

注记. 如果 $S = \{x_1, \cdots, x_n\}$, 则$\mathbb{Z}(S)$ 中任何元素均可唯一写成 $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$, $\alpha_i \in \mathbb{Z}$ 的形式, 故若 $\{y_1, \cdots, y_n\}$ 为 $\mathbb{Z}(S)$ 的另一组基, 则

$$y_j = x_1^{\alpha_{1j}} x_2^{\alpha_{2j}} \cdots x_n^{\alpha_{nj}} \ (\alpha_{ij} \in \mathbb{Z})$$

且

$$x_j = y_1^{\beta_{1j}} y_2^{\beta_{2j}} \cdots y_n^{\beta_{nj}} \ (\beta_{ij} \in \mathbb{Z}).$$

令矩阵 $A = (\alpha_{ij}), B = (\beta_{ij}) \in M_n(\mathbb{Z})$, 则 $AB = BA = I$, 即矩阵 A 在$M_n(\mathbb{Z})$ 中有乘法逆元 B.

§2.6.2 有限生成阿贝尔群的结构定理

我们假设 G 是有限生成阿贝尔群, 记 G 的运算为加法.

定理2.75. *设 G 是有限生成自由阿贝尔群, H 为 G 的非零子群, 则 H 也是有限生成自由阿贝尔群, 且 $\mathrm{rank}(H) \leqslant \mathrm{rank}(G)$. 更具体地说, 存在 G 的一组基 $\{x_1, \cdots, x_n\}$, 正整数 $r \leqslant n$, 正整数 $d_1 \mid d_2 \mid \cdots \mid d_r$, 使得 H 是以 $\{d_1x_1, \cdots, d_nx_n\}$ 为基的自由阿贝尔群.*

证明. 令集合

$$I = \{s \in \mathbb{Z} \mid \text{存在}G\text{的一组基}y_1, \cdots, y_n, \alpha \in H, \alpha = sy_1 + k_2y_2 + \cdots + k_ny_n\}.$$

我们注意到如果 $H \neq 0$, 则 $I \neq 0$ 且

- 如果 $s \in I$, $n \in \mathbb{Z}$, 则$ns \in I$. 从而 I 中有正整数.
- 由于 $\{y_2, y_1, \cdots, y_n\}$ 也是一组基, 故 $k_2 \in I$. 同理 $k_i \in I$.

由此, 令 d_1 为 I 中最小正整数, 则存在 $\alpha \in H$, 基 $\{y_1, y_2, \cdots, y_n\}$ 使得 $\alpha = d_1y_1 + k_2y_2 + \cdots + k_ny_n$. 令 $k_i = q_id_1 + r_i$ $(0 \leq r_i < d_1)$, 则

$$\alpha = d_1(y_1 + q_2y_2 + \cdots q_ny_n) + r_2y_2 + \cdots r_ny_n.$$

由于 $\{y_1 + q_2y_2 + \cdots q_ny_n, y_2, \cdots, y_n\}$ 还是一组基, 故 $r_i \in I$. 由 d_1 的最小性知 $r_i = 0$. 即存在 $\alpha \in H$, 基 $\{x_1, x_2, \cdots, x_n\}$ 使得 $\alpha = d_1x_1$.

我们现在对 G 的秩作归纳. 如果 $n = 1$, 定理显然成立. 假设对秩 $< n$ 时定理成立, 对 $H \leqslant G$, 令 $G_1 = \langle y_2, \cdots, y_n\rangle$, 我们断言

$$H = \langle\alpha\rangle \oplus (H \cap G_1).$$

事实上, 由于 $x_1, y_2, \cdots, y_n$ 为 G 的基, $\langle x_1\rangle \cap G_1 = \{0\}$, 故 $\langle\alpha\rangle \cap (H \cap G_1) = \{0\}$. 又若 $x \in H$,

$$x = k_1x_1 + k_2y_2 + \cdots + k_ny_n,$$

由于 $k_1, \cdots, k_n \in I, d_1 \mid k_1, x \in \langle\alpha\rangle + (H \cap G_1)$, 断言证毕.

现在如果 $G_1 \cap H = \{0\}$, 则 $H = \langle d_1x_1\rangle$, 定理成立. 如果$G_1 \cap H \neq \{0\}$, 则 $G_1 \cap H$ 是有限生成自由群 G_1 的子群. 由于 $\mathrm{rank}G_1 = n - 1$, 由归纳假设,

存在 G_1 的一组基 $\{x_2,\cdots,x_n\}, d_2 \mid d_3 \mid \cdots d_r$, 使得 $H=\langle d_2x_2,\cdots,d_rx_r\rangle$, 则 $\{x_1,\cdots,x_n\}$ 为 G 的一组基, 使得 $\{d_1x_1,\cdots,d_rx_r\}$ 为 H 的基, 且由 I 的性质, $d_1 \mid d_2$, 定理证毕. □

定理2.76. 有限生成阿贝尔群 A 均有如下结构

$$A \cong \mathbb{Z}^r \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z},$$

其中 $m_1 \mid m_2 \mid \cdots \mid m_s$ 为正整数.

证明. 设 $F(S) \to A$ 为满同态, 其中 S 为有限集. 则由 A 为阿贝尔群, φ 诱导满同态

$$\varphi : \mathbb{Z}(S) \to A.$$

则 $\ker\varphi$ 是 $\mathbb{Z}(S)$ 的子群. 由定理 2.75, 存在 $\mathbb{Z}(S)$ 的一组基 $\{x_1,\cdots,x_n\}$ 及正整数 $m_1 \mid m_2 \mid m_s$, 使得 $\{m_1x_1,\cdots,m_sx_s\}$ 是 $\ker\varphi$ 的基, 故

$$A = \mathbb{Z}(S)/\ker\varphi = \mathbb{Z}^{n-s} \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \mathbb{Z}/m_s\mathbb{Z}.$$

定理证毕. □

定义2.77. 设 A 是有限生成阿贝尔群, 定义它的**扭子群** (torsion subgroup)

$$A_t = \{a \in A \mid a\text{的阶有限}\}. \tag{2.27}$$

容易看出 A_t 的确是 A 的子群, 且对于群

$$\mathbb{Z}^r \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \mathbb{Z}/m_s\mathbb{Z},$$

其扭子群为 $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \mathbb{Z}/m_s\mathbb{Z} = T$. 由上述定理, 我们有

推论2.78. (1) $A = A_t \oplus A_f$, 其中 A_f 是有限生成自由阿贝尔群.

(2) $A \cong B$ 当且仅当 $A_t \cong B_t$ 且 $\mathrm{rank}A_f = \mathrm{rank}B_f$.

证明. 设 $\varphi : A \cong \mathbb{Z}^r \oplus T$, 令 $A_f = \varphi^{-1}(\mathbb{Z}^r), A_t = \varphi^{-1}(T)$, 则 A_t 为 A 的扭子群, 且 A_f 为秩为 r 的自由群.

(2) 由(1)立得. □

定理2.79. 设 $A \neq \{0\}$ 为有限阿贝尔群, 则

(1) $A \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \mathbb{Z}/m_s\mathbb{Z}$, 正整数 $m_1 \mid \cdots \mid m_s$ 由 A 唯一确定.

(2) $A \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \mathbb{Z}/p_t^{\alpha_t}\mathbb{Z}$, 其中 $p_1, \cdots, p_t$ 为素数, 且 $p_1^{\alpha_1}, \cdots, p_t^{\alpha_t}$ 由 A 唯一确定.

证明. 由于 A 有限, 则 $A = A_t$ 没有无限阶元, 故 A 有(1)的形式, 又由中国剩余定理, 如果 $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, 则

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \mathbb{Z}/p_s^{\alpha_s}\mathbb{Z}.$$

故 A 有(2)的形式. 我们需要证明唯一性.

首先我们证明(2)的唯一性. 由于 A 是阿贝尔群, 它的所有子群都是正规子群, 我们有

$$A = \bigoplus_p A_p = A_{p_1} \oplus \cdots \oplus A_{p_t}$$

的形式, 其中 A_p 是 A 的Sylow p 子群, 故不妨假设 A 本身是 p 群, 我们要证明

$$A \cong \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\alpha_r}\mathbb{Z} \ (\alpha_1 \leqslant \cdots \leqslant \alpha_r) \tag{2.28}$$

唯一. 如不然, 令

$$A \cong \mathbb{Z}/p^{\beta_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\beta_{r'}}\mathbb{Z} \ (\beta_1 \leqslant \cdots \leqslant \beta_{r'}). \tag{2.29}$$

考虑 A/pA, (2.28)说明 $|A/pA| = p^r$, (2.29)说明 $|A/pA| = p^{r'}$, 故 $r = r'$. 我们对 k 作归纳证明 $\alpha_k = \beta_k$. 如果 $\alpha_1 = \beta_1, \cdots, \alpha_{k-1} = \beta_{k-1}$ 但 $\alpha_k < \beta_k$, 则由(2.28), $|p^{\alpha_k}A/p^{\alpha_{k+1}}A| \leqslant p^{r-k}$, 但由(2.29), $|p^{\alpha_k}A/p^{\alpha_{k+1}}A| = p^{r-k+1}$, 矛盾. 故 $\alpha_k = \beta_k$, 即(2.28)与(2.29)形状一样, (2)的唯一性证毕.

对于(1)的唯一性, 对任何 p, 考虑 A 的Sylow p子群. 由(2)

$$A_p \cong \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\alpha_r}\mathbb{Z}, \ \alpha_1 \leqslant \cdots \leqslant \alpha_r.$$

由(1),

$$A_p = (\mathbb{Z}/m_1\mathbb{Z})_p \oplus \cdots \oplus (\mathbb{Z}/m_s\mathbb{Z})_p$$

由于 $m_1 \mid m_2 \mid \cdots \mid m_s$, 且 $(\mathbb{Z}/m\mathbb{Z})_p$ 为循环群, 故必有

$$(\mathbb{Z}/m_s\mathbb{Z})_p = \mathbb{Z}/p^{\alpha_r}\mathbb{Z}, \quad (\mathbb{Z}/m_{s-1}\mathbb{Z})_p = \mathbb{Z}/p^{\alpha_{r-1}}\mathbb{Z}, \quad \ldots.$$

由此, $m_s, m_{s-1}, \cdots$ 均唯一确定. □

定义2.80. 上述定理中 $\{p_1^{\alpha_1}, \cdots, p_t^{\alpha_t}\}$ 称为 A 的**初等因子组**, 其中元素称为**初等因子** (elementary divisors); $\{m_1, \cdots, m_s\}$ 称为 A 的**不变因子组**, 其中元素称为**不变因子** (invariant factors).

我们可以综合上述定理得到

定理2.81 (有限生成阿贝尔群的结构定理)**.** (1) 设 A 为有限生成阿贝尔群, 则

$$\begin{aligned} A &\cong \mathbb{Z}^r \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \mathbb{Z}/m_s\mathbb{Z} \\ &\cong \mathbb{Z}^r \oplus \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \mathbb{Z}/p_t^{\alpha_t}\mathbb{Z} \end{aligned}$$

其中

(i) r 称为 A 的秩, 由 A 唯一确定.

(ii) $1 < m_1 \mid m_2 \mid \cdots \mid m_s$ 由 A 唯一确定.

(iii) $\{p_1^{\alpha_1}, \cdots, p_t^{\alpha_t}\}$ 由 A 唯一确定.

(2) 有限生成阿贝尔群 A 与 B 同构当且仅当其秩相同, 且其初等因子或不变因子也相同.

例2.82. 我们来讨论一下8 阶群G 的结构.

(1) 阿贝尔群. 此时初等因子可能有3 种情况: $\{8\}$, $\{2,4\}$ 和$\{2,2,2\}$, 故共有3 种8 阶阿贝尔群: $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ 和$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

(2) 非阿贝尔群. 如果G中有8 阶元, 则G 是循环群; 如果其元素阶只为1 和2, 则G 为阿贝尔群(引理 *1.65*). 我们可以假设x 是G的一个4 阶元, 则$(G : \langle x\rangle) = 2$, $\langle x\rangle$ 是G 的正规子群(命题 *2.38*). 令$y \in G - \langle x\rangle$, 则$G = \{x^i, x^i y \mid i = 0, 1, 2, 3\}$.

考虑元素$y^{-1}xy \in \langle x\rangle$. 由于它与$x$ 同阶, 故$y^{-1}xy = x$ 或者x^3. 但由于x 与y 不交换, 故$y^{-1}xy = x^3 = x^-$. 如果y 的阶为2, 则

$$G = \langle x,\ y \mid x^4 = y^2 = 1,\ yxy = x^{-1}\rangle \cong D_4.$$

如果y 的阶为4, 则

$$G = \langle x,\ y \mid x^4 = y^4 = 1,\ y^{-1}xy = x^{-1}\rangle.$$

我们考虑4元数群

$$Q_8 := \left\{ \pm I,\ \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}. \tag{2.30}$$

则G 与Q_8 通过映射$x \mapsto \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$, $y \mapsto \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ 同构.

综上所述, 在同构意义下 8阶非阿贝尔群共有两个: D_4 和Q_8.

例2.83. 1500 阶阿贝尔群 A 的结构. 由$1500 = 2^2 \times 3 \times 5^3$, 它的初等因子组有如下可能: $\{2,2,3,5,5,5\}$, $\{4,3,5,5,5\}$, $\{2,2,3,5,25\}$, $\{4,3,5,25\}$, $\{2,2,3,125\}$, $\{4,3,125\}$, 故共有六种阿贝尔群, 其阶为 1500.

习　　题

习题6.1. 将 33 阶群分类. 将18 阶群分类.

习题6.2. 有限生成阿贝尔群 G 是自由阿贝尔群当且仅当 G 的每个非零元素都是无限阶元素.

习题6.3. (1) 正有理数乘法群 $\mathbb{Q}^+$ 是自由阿贝尔群, 全部素数是它的一组基.

(2) $\mathbb{Q}^+$ 不是有限生成的.

习题6.4. (1) $\mathbb{Q}$ 不是自由阿贝尔群.

(2) $\mathbb{Q}$ 的任意有限生成的子群都是循环群, 但 $\mathbb{Q}$ 不是循环群.

习题6.5. 设 G 是有限生成的自由阿贝尔群, $\mathrm{rank}(G) = r$. 如果 $g_1, g_2, \cdots, g_n$ 是 G 的一组生成元,则 $n \geq r$.

习题6.6. 设 A 为有限阿贝尔群, 对于 $|A|$ 的每个正因子 d, A 均有 d 阶子群和 d 阶商群.

习题6.7. 设 H 是有限阿贝尔群 A 的子群, 则有 A 的子群同构于 A/H.

习题6.8. 如果有限阿贝尔群 A 不是循环群, 则存在素数 p 使得 A 有子群同构于 $(\mathbb{Z}/p\mathbb{Z})^2$.

习题6.9. 求出 $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ 的不变因子和初等因子.

习题6.10. 求出 $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/35\mathbb{Z}$ 的不变因子和初等因子.

习题6.11. 设 n 为正整数, 问有多少个 n 阶阿贝尔群?

习题6.12. 设 p 是一个素数, 问 $\mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p^3\mathbb{Z}$ 有多少个 p^2 阶子群?

习题6.13. $\mathbb{C}^\times$ 的每个有限子群都是循环群. 由此求出 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}^\times$ 的所有群同态.

习题6.14. 设 G, A, B 均为有限阿贝尔群. 如果 $G \oplus A \cong G \oplus B$, 则 $A \cong B$.

习题6.15. 设有限生成阿贝尔群 G 的秩为 1, $f : G \to \mathbb{Z}$ 为满同态, 则 $A \cong \mathbb{Z} \oplus \ker f$, 即 $\ker f$ 是 G 的扭子群.

习题6.16. 有限生成自由阿贝尔群有什么样的泛性质?

习题6.17. 试证: 有限生成阿贝尔群 G 是自由阿贝尔群当且仅当 G 的每个非零元素都是无限阶元素.

习题6.18. 将 $\mathbb{F}_p$ 上的 n 维向量空间 $\mathbb{F}_p^n$ 作为加法群.

(1) 试求 $\mathbb{F}_p^n$ 中 p^{n-1} 阶子群的个数.

(2) 证明 $\mathbb{F}_p^n$ 中 p^k 阶子群的个数等于 p^{n-k} 阶子群的个数.

第三章　环和域

§3.1　环和域的定义

§3.1.1　环的概念的引入

在初等数论的学习中, 我们学习到两个集合:

(1) $\mathbb{Z}$: 所有整数构成的集合;

(2) $F[x]$: 域 F 上的多项式集合, 其中 $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 或 $\mathbb{F}_p$.

这两个集合均有加法和乘法运算, 且满足条件:

(i) 在加法运算下是阿贝尔群;

(ii) 乘法运算满足结合律, 且存在单位元 1;

(iii) 加法和乘法运算满足分配律.

同样, 在线性代数中, 域 F 上的 n 阶矩阵 $M_n(F)$ 在矩阵加法和乘法意义下也满足上述性质(i)-(iii).

令 $\alpha \in \mathbb{C}$, 我们考虑 $\mathbb{C}$ 上的子集合

$$\mathbb{Z}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_n\alpha^n \mid a_0, a_1, \ldots, a_n \in \mathbb{Z}\}.$$

同样, 我们有 $\mathbb{Z}[\alpha]$ 满足性质(i)-(iii), 此时有两种情况

(a) 存在多项式 $f(x) \in \mathbb{Z}[x], f(\alpha) = 0$. 例如 $\alpha = \sqrt{-1}$, 则 $\alpha^2 + 1 = 0$. 我们称 α 为**代数元** (algebraic element).

(b) 不存在多项式使得 α 为它的根, 我们称 α 为**超越元** (transcendental element).

这些例子, 均为环的例子.

§3.1.2　定义和例子

定义3.1. 集合 R 称为**(含幺)环**(ring with identity), 是指 R 上存在加法和乘法两种运算, 且

(1) R 关于加法为阿贝尔群, 我们记它的加法单位元为 0;

(2) R 关于乘法满足结合律且有单位元 1 (即 R 为乘法含幺半群);

(3) 加法和乘法运算满足**分配律**, 即对任意 $\lambda, a, b \in R$,

$$\lambda(a+b) = \lambda a + \lambda b, \quad (a+b)\lambda = a\lambda + b\lambda. \tag{3.1}$$

如果乘法满足交换律, 则称 R 为**交换环**(commutative ring). 如果$R-\{0\}$ 是乘法阿贝尔群, 称R 为**域** (field).

我们下面列举更多例子.

例3.2. 设$R=\{0\}$, 且其上加法和乘法为$0+0=0\cdot 0=0$, 则R 构成环, 称为**零环**, 记为0. 这是最简单的环.

例3.3. 我们在之前所讲的域 $\mathbb{Q},\mathbb{R},\mathbb{C}$ 或 $\mathbb{F}_p$, 均满足上述域的定义. 由于域中至少有2 个元素, 故$\mathbb{F}_2$ 是最简单的域.

例3.4. 设 R 为交换环, 则 R 上的 n 阶方阵集合 $M_n(R)$ 在矩阵加法和乘法意义下构成环. 如果 $n=1$, 则 $M_1(R)=R$. 如果 $n\geqslant 2, M_n(R)$ 为非交换环.

例3.5. 设

$$\mathbb{H}=\{a+bi+cj+dk \mid a,b,c,d\in\mathbb{R}\},$$

其中 $i^2=j^2=k^2=-1, ij=-ji=k, jk=-kj=i, ki=-ik=j$, 则 $\mathbb{H}$ 构成环, 称为 $\mathbb{R}$ 上的**四元数体** (*quaternion*). $\mathbb{H}$ 不是交换环. 它的子集合

$$\mathbb{H}(\mathbb{Q})=\{a+bi+cj+dk \mid a,b,c,d\in\mathbb{Q}\}$$

也是非交换环, 称为 $\mathbb{Q}$ **上的四元数体**.

对于四元数体 $\mathbb{H}$, 它的非零元均可逆(参见习题*1.2*), 但由于 $\mathbb{H}$ 不是交换环, 故 $\mathbb{H}$ 不是域. 我们称类似于$\mathbb{H}$ 的满足条件非零元均可逆的非交换环为**体** (*skew field*), 或谓**可除代数** (*division algebra*).

例3.6. 令

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

则 $\mathbb{H}'$ 在矩阵加法和乘法下构成非交换环. 它的子集合

$$\mathbb{H}'(\mathbb{Q})=\left\{\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix} \mid \alpha,\beta\in\mathbb{Q}(i)\right\}$$

也是非交换环.

图 3.1: 哈密尔顿纪念币

威廉 · 哈密尔顿爵士*(Sir William Hamilton, 1805*年*8*月*4*日 – *1865*年*9*月*2*日*)*, 爱尔兰数学家, 物理学家及天文学家. 哈密尔顿于*1843*年发现四元数, 这是体*(*可除环*)* 的第一个例子. 哈密尔顿用十多年时间, 尝试将复数*(*作为*2*维实平面*)* 推广到*3*维情形, 但未取得成功, 最终在四维情形他创造了四元数. 尽管四元数并未如哈密尔顿所预期那样享受与复数同等的荣光, 但四元数在基础数学研究还是有着很重要意义, 并被广泛应用在计算机图形学, 控制理论, 信号处理, 轨道力学, 主要用于表示旋转与方向. 附图*3.1*是*2003*年为纪念哈密尔顿诞生*200*周年爱尔兰政府发行的10 欧元纪念币.

命题3.7. 设 R 为环, 则

(1) 对任意的 $a \in R$, $0 \cdot a = a \cdot 0 = 0$.

(2) 对于 n 为正整数, $a \in R$, 记 na 为 n 个 a 之和, 记 $-na$ 为 na 的加法逆元. 则对 $n \in \mathbb{Z}$, $a, b \in R$, 我们有 $(na)b = a(nb) = nab$.

(3) 对于R 中元素a_i $(1 \leq i \leq m)$ 和b_j $(1 \leq j \leq n)$, 则

$$\sum_i a_i \sum_j b_j = \sum_i \sum_j a_i b_j.$$

证明. (1) 我们有 $0\cdot a=(0+0)\cdot a=0\cdot a+0\cdot a$, 故 $0\cdot a=0$. 同理 $a\cdot 0=0$.

(2) 首先 $n=0$ 的情形即(1). 其次, 由 $na=(n-1)a+a=(n+1)a-a$, 再对 n 做双向归纳即可.

(3) 当 i 的个数为 1 时, 对 j 做归纳, 要证等式即为右分配律. 对于一般情况的 i, 使用左分配律归结到 $i-1$ 的情况, 然后利用归纳假设. □

推论3.8. 如果 $1=0$, 则 $R=0$.

证明. 设 $a\in R$, 则 $a=a\cdot 1=a\cdot 0=0$. □

由上述命题, 我们立刻有

定理3.9 (牛顿二项式定理)**.** 设R 为交换环. 则对正整数 n 和元素$x,y\in R$, 总有

$$(x+y)^n=\sum_{k=0}^{n}C_n^kx^ky^{n-k}=\sum_{k=0}^{n}\binom{n}{k}x^ky^{n-k}. \tag{3.2}$$

证明. 由命题 3.7 (3) 做归纳, 我们有

$$\prod_{i=1}^{n}(a_{i1}+a_{i2})=\sum_{i_1=1}^{2}\sum_{i_2=1}^{2}\cdots\sum_{i_n=1}^{2}a_{1i_1}a_{2i_2}\cdots a_{ni_n}.$$

如令 $a_{11}=a_{21}=\cdots=a_{n1}=x$, $a_{12}=a_{22}=\cdots=a_{n2}=y$, 则 $a_{1i_1}a_{2i_2}\cdots a_{ni_n}=x^ky^{n-k}$ 当且仅当i_1, $\cdots$, i_n 恰好k 个为1, $n-k$ 个为2. 合并同类项即得(3.2). □

注记. 事实上只要$xy=yx$, 则式 (3.2) 总成立.

定义3.10. 如果 R 为环, a,b 为 R 中非零元且 $ab=0$, 称 a 为环 R 的**左零因子** (left zero divisor), b 为环 R 的**右零因子** (right zero divisor). 如果 a 既是左零因子又是右零因子, 称 a 为 R 的**零因子**(zero divisor).

注记. 如果 R 为交换环, 则左零因子, 右零因子和零因子是一个概念.

定义3.11. 如果 R 为环, a 称为**左可逆**(left invertible)的是指存在 $b\in R, ba=1$, 此时称 b 为 a 的**左逆** (left inverse). 同样, a 称为**右可逆** (right invertible)的, 是指存在 $c\in R, ac=1$, 此时称 c 为 a 的**右逆** (right inverse). 如果 a 既是左可逆的, 又是右可逆的, 称 a 为**可逆** (invertible)的, 也称 a 为 R 中的**单位** (unit).

引理3.12. (1) 如果 a 可逆, 则 a 的左逆等于右逆且唯一, 记为 a^{-1}.

(2) 环 R 中的单位集合构成一个群, 称为 R 的**单位群** (*group of units*), 记为 $U(R)$ 或 $R^\times$.

证明. (1) 如果 $ba = ac = 1$, 则 $b = b(ac) = (ba)c = c$.

(2) 由于 $1 \in U(R)$, 且如果 $a, b \in U(R)$, 则

$$abb^{-1}a^{-1} = b^{-1}a^{-1}ab = 1,$$

故 $ab \in U(R)$. 又易知 $a^{-1} \in U(R)$, 故 $U(R)$ 为群. □

例3.13. 域或者体F 的单位群$F^\times = F - \{0\}$, 它们的区别是前者是阿贝尔群, 而后者非交换.

例3.14. 设 R 为交换环, 则 n 阶矩阵环 $M_n(\mathbb{R})$ 的单位群称为R 上的n 阶一般线性群, 记为 $\mathrm{GL}_n(\mathbb{R})$.

定义3.15. 如果交换环 R 没有零因子, 称 R 为**整环**(integral domain).

由定义显然知域必为整环, 我们有包含关系:

$$\text{域} \subsetneq \text{整环} \subsetneq \text{交换环} \subsetneq \text{环}.$$

引理3.16. 交换环 R 为整环当且仅当**消去律**成立, 即若 $a \neq 0$, $ab = ac$, 则 $b = c$.

证明. 显然. 留给读者. □

例3.17. 环 $\mathbb{Z}/6\mathbb{Z}$ 中, $2 \cdot 3 = 4 \cdot 3 = 0$, 故 $2, 3, 4$ 为 $\mathbb{Z}/6\mathbb{Z}$ 的零因子. $\{1, 5\}$ 为 $\mathbb{Z}/6\mathbb{Z}$ 的单位群, $\mathbb{Z}/6\mathbb{Z}$ 不是整环.

例3.18. 对于$\alpha \in \mathbb{C}$, $\mathbb{Z}[\alpha]$ 是整环, 但不是域. 对于α 是超越元, 容易看出$\alpha^{-1} \notin \mathbb{Z}[\alpha]$, 故$\mathbb{Z}[\alpha]$ 不是域. 对于α 为代数元, 证明需要更深一步知识.

例3.19. 设 R 为交换环, 则对 $A \in M_n(R)$, 我们可以如线性代数中那样定义 A 的伴随矩阵 A^* 及 A 的行列式 $\det A$, 则如 $\det(A) \in U(R)$, 我们有

$$A \cdot \frac{1}{\det A} A^* = \frac{1}{\det A} A^* \cdot A = I.$$

反之, 若 A 可逆, 则 $\det A \cdot \det A^{-1} = 1 \in R$, 故 $\det A$ 可逆, 即我们有 $\alpha \in U(M_n(R))$ 当且仅当 $\det A \in U(R)$, 此时 $U(M_n(R)) = \mathrm{GL}_n(R)$. 当 $n \geqslant 2$ 时, $M_n(R)$ 不是交换环, 也不是整环(即使 R 为整环).

定义3.20. 环 R 的子集合 T 称为 R 的**子环** 是指 $T=0$ 或者 T 在 R 的加法和乘法意义下构成环.

同样, 域 F 的子集合 E 称为 F 的**子域** 是指 E 在 F 的加法和乘法意义下构成域.

由定义知, 如$T\neq 0$, 则集合 T 是 R 的子环当且仅当 T 是 R 的加法子群且在 R 的乘法意义下是含幺半群. 非空子集 E 是域 F 的子域当且仅当 E 是 F 的加法子群且 $E-\{0\}$ 是 $F^{\times}=F-\{0\}$ 的乘法子群.

例3.21. $\mathbb{H}(\mathbb{Q})$ 是 $\mathbb{H}$ 的子环.

引理3.22. (1) 如果 R_1, R_2 为 R 的子环, 则 $R_1\cap R_2$ 为 R 的子环;

(2) 同样, 如果 $(R_i)_{i\in I}$ 为 R 的子环, 则 $\bigcap\limits_{i\in I} R_i$ 也是 R 的子环. 我们称 $\bigcap\limits_{i\in I} R_i$ 为 $R_i(i\in I)$ 的交.

证明. 由定义立得. □

定义3.23. 设R_1, R_2 为环. 则 R_1 与 R_2 (作为集合的) 的笛卡尔积 $R=R_1\times R_2$ 在加法和乘法运算

$$(x_1,x_2)+(y_1,y_2)=(x_1+y_1,x_2+y_2),$$

$$(x_1,x_2)\cdot(y_1,y_2)=(x_1y_1,x_2y_2)$$

下构成群: 它的乘法单位元是 $1_R=(1_{R_1},1_{R_2})$, 零元$0_R=(0_{R_1},0_{R_2})$, 元素 (x_1,x_2) 的负元是 $(-x_1,-x_2)$. 环 R 称为 R_1 与 R_2 的**直积** , 或者称为**笛卡尔积**.

注记. 由于对于任何$x\in R_1$, $y\in R_2$, 均有

$$(x,1)\cdot(1,y)=0.$$

故两个非零环的直积一定不是整环. 特别地, 域的直积(作为环而言) 一定不是域.

习 题

习题1.1. 设 $n \geqslant 2$ 是正整数.

(1) 环 $\mathbb{Z}/n\mathbb{Z}$ 中元素 a 可逆的充要条件是 $(a,n)=1$.

(2) 若 p 为素数, 则 $\mathbb{Z}/p\mathbb{Z}$ 为域. 若 $n \geqslant 2$ 不为素数, 则 $\mathbb{Z}/n\mathbb{Z}$ 不是整环.

习题1.2. 证明$\mathbb{H}$ 中任何非零元均乘法可逆.

习题1.3. 设 $d \geqslant 1$ 为正整数. 利用 $R=\mathbb{Z}[\sqrt{-d}] \subseteq \mathbb{C}$ 说明 R 是整环并确定 R 的单位群.

习题1.4. 设 A 是阿贝尔群, $\mathrm{End}(A)$ 是群 A 的全部自同态构成的集合. 对于 $f,g \in \mathrm{End}(A)$, 定义

$$(f+g)(a)=f(a)+g(a), \quad (f\cdot g)(a)=f(g(a)) \ (a \in A).$$

证明 $\mathrm{End}(A)$ 对于上述运算是含幺环, 并求出它的单位群.

习题1.5. 设 G 是乘法群, R 为含幺环. 定义集合

$$R[G]=\{\sum_{g\in G} r_g g \mid r_g \in R, \text{并且只有有限多个 } r_g \neq 0\}.$$

在集合 $R[G]$ 上定义

$$\sum_{g\in G} r_g g+\sum_{g\in G} t_g g=\sum_{g\in G}(r_g+t_g)g, \quad (\sum_{g\in G} r_g g)(\sum_{g\in G} t_g g)=\sum_{g\in G}(\sum_{g'g''=g} r_{g'}t_{g''})g,$$

(1) 求证: 上面定义的加法和乘法是集合 $R[G]$ 中的二元运算, 并且 $R[G]$ 由此形成环, 称为群 G 在环 R 上的**群环**.

(2) $R[G]$ 是交换环当且仅当 R 是交换环且 G 是阿贝尔群.

(3) 如果环 R 的单位元为 1_R, 群 G 的单位元为 e, 则 $1_R e$ 是群环 $R[G]$ 的单位元.

(4) 可以将 R 自然地看成是 $R[G]$ 的子环.

(5) 试确定 $\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ 和$R[\mathbb{Z}]$ 的单位群, 其中 R 为整环.

习题1.6. 令 $R=\{a=(a_1,a_2,\ldots) \mid a_n \in \mathbb{Z},\ 0 \leqslant a_n \leqslant p^n-1, a_n \equiv a_{n+1} \bmod p^n\}$. 设 $a,b \in R$, 定义

$$a+b=c,\ 0 \leqslant c_n \leqslant p^n-1, c_n \equiv a_n+b_n \bmod p^n,$$

$$a+b=d,\ 0\leqslant d_n\leqslant p^n-1, d_n\equiv a_nb_n \bmod p^n.$$

(1) R 成为一个含幺交换环, 称为 p **进整数环**, 记为 $\mathbb{Z}_p$.

(2) $\mathbb{Z}$ 可自然看成是 $\mathbb{Z}_p$ 的子环.

(3) 试确定 $\mathbb{Z}_p$ 的单位群.

习题1.7. 设 $d\in\mathbb{Q}^\times-(\mathbb{Q}^\times)^2$. 证明 $\mathbb{Q}[\sqrt{d}]=\{a+b\sqrt{d}\mid a,b\in\mathbb{Q}\}$ 是 $\mathbb{C}$ 的子域. 并确定 $\mathbb{Q}[\sqrt{d}]$ 的全部子域.

习题1.8. 设 R 为环, $a\in R$. 求证 $\{r\in R\mid ra=ar\}$ 为 R 的子环.

习题1.9. 设 U 是一个集合. S 是 U 的全部子集构成的集族, 即 $S=\{V\mid V\subseteq U\}$. 对于 $A,B\in S$, 定义

$$A-B=\{c\in U\mid c\in A, c\notin B\},$$
$$A+B=(A-B)\cup(B-A),\quad A\cdot B=A\cap B.$$

求证 $(S,+,\cdot)$ 是含幺交换环.

习题1.10. 设 R 为环. 如果每个元素 $a\in R$ 均满足 $a^2=a$, 称 R 为**布尔** (***Boole***) **环**. 求证:

(1) 布尔环 R 必为交换环, 并且 $a+a=0_R$ (对每个 $a\in R$);

(2) 习题 *1.9* 中的环 S 是布尔环.

习题1.11. 非零有限整环必为域.

习题1.12. 环 R 中元素 a 叫做**幂零**的, 是指存在正整数 m, 使得 $a^m=0$.

(1) 证明当 R 是交换环时, 若 a 和 b 均为幂零元素, 则 $a+b$ 也是幂零元素.

(2) 如果 R 不为交换环时, (1) 中结论是否仍旧成立?

(3) 证明如果 x 幂零, 则 $1+x$ 是单位.

习题1.13. 设 a,b 是含幺环 R 中的元素, 则 $1-ab$ 可逆等价于 $1-ba$ 可逆.

习题1.14. 含幺环中某元素若有多于一个右逆, 则它必有无限多个右逆.

习题1.15. 令 $C(\mathbb{R})$ 表示全部连续实函数 $f:\mathbb{R}\to\mathbb{R}$ 组成的集合. 定义

$$(f+g)(a)=f(a)+g(a),\quad (fg)(a)=f(a)g(a),\ \forall f,g\in C(\mathbb{R}),a\in\mathbb{R}.$$

证明 $C(\mathbb{R})$ 由此成为含幺交换环. $C(\mathbb{R})$ 是否为整环? 是否含有幂零元? 单位群是什么?

习题1.16. 设 D 为有限体. 证明对任意 $a\in D$, $a^{|D|}=a$.

§3.2 环的同态与同构

§3.2.1 定义与简单例子

定义3.24. 设R_1, R_2 为环. 映射$f:R_1\to R_2$ 称为**环同态** 是指下列条件成立:

(1) $f(1)=1$, 即f 将乘法单位元映到单位元.

(2) 对任意 $g,h\in R_1$,

$$f(g+h)=f(g)+f(h),\quad f(gh)=f(g)f(h).$$

如 f 作为集合映射为单射, 称 f 为**单同态**, 也称为**嵌入**. 如 f 为满射, 称 f 为**满同态**. 如 f 为双射, 则称 f 为**同构**, 记为 $f:R_1\cong R_2$.

注记. 只有条件(2) 成立不能保证(1) 成立. 如映射

$$\mathbb{R}\longrightarrow M_2(\mathbb{R}),\quad x\longmapsto\begin{pmatrix}x&0\\0&0\end{pmatrix}$$

满足条件(2) 但不满足条件(1).

在一些文献中, 环不一定含幺, 此时环同态的定义中只假设(2). 可以证明, 如果 R_1,R_2 含幺, $f:R_1\to R_2$ 为满射, 且(2)成立, 则 $f(1)=1$.

由环同态定义, 我们立刻有

命题3.25. 设$f:R_1\to R_2$ 为环同态, 则$f(0)=0$, $f(-g)=-f(g)$ $(g\in R_1)$, 且$f(g^{-1})=f(g)^{-1}$ (如$g\in R_1^\times$ 可逆). 故环同态诱导单位群同态: $R_1^\times\to R_2^\times$.

例3.26. 在上节中, 我们定义了 四元数体$\mathbb{H}$ 与 $\mathbb{H}'$. 令

$$\begin{aligned} f : \mathbb{H} &\longrightarrow \mathbb{H}' \\ a+bi+cj+dk &\longmapsto \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \end{aligned}$$

其中 $\alpha = a+bi, \beta = c+di$, 则 f 是 $\mathbb{H}$ 到 $\mathbb{H}'$ 的同构. 今后我们将$\mathbb{H}$ 与 $\mathbb{H}'$ 等同看待. 注意到上述同构诱导了$\mathbb{H}(\mathbb{Q})$ 与$\mathbb{H}'(\mathbb{Q})$ 的同构.

例3.27. 设 m, n 为正整数, 设 R 为环, 则

$$\begin{aligned} f : M_m(R) \times M_n(R) &\longrightarrow M_{m+n}(R) \\ (A, B) &\longmapsto \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \end{aligned}$$

为环的单同态. 如果 R 为交换环, 则 f 诱导群的单同态

$$\mathrm{GL}_m(R) \times \mathrm{GL}_n(R) \longrightarrow \mathrm{GL}_{m+n}(R).$$

例3.28. 记 $\mathrm{Aut}(\mathbb{R})$ 为所有 $\mathbb{R}$ 到自身的同构, 即 $\mathbb{R}$ 的自同构的集合, 则 $\mathrm{Aut}(\mathbb{R})$ 在映射复合意义下构成群. 我们来确定 $\mathrm{Aut}(\mathbb{R})$. 设 $\varphi \in \mathrm{Aut}(\mathbb{R})$, 则

(i) $\varphi(1) = 1,\ \varphi(-1) = -1$;

(ii) $n\varphi(\frac{1}{n}) = \varphi(n \cdot \frac{1}{n}) = 1$, 故 $\varphi(\frac{1}{n}) = \frac{1}{n}$;

(iii) $\varphi(\frac{m}{n}) = m\varphi(\frac{1}{n}) = \frac{m}{n}$.

故 $\varphi\,|_{\mathbb{Q}} = \mathrm{id}$.

如果 $x - y > 0$, 则

$$\varphi(x-y) = \varphi(\sqrt{x-y})^2 > 0,$$

即 $\varphi(x) > \varphi(y)$, 故可得对任意 $x \in \mathbb{R}, \varphi(x) = x$, 即 $\varphi = \mathrm{id}$, 所以 $\mathrm{Aut}(\mathbb{R})$ 是平凡群.

注记. $\mathrm{Aut}(\mathbb{C})$ 不是平凡群, 比如说 $z \mapsto \bar{z}$ 是 $\mathbb{C}$ 的自同构. 事实上, $\mathrm{Aut}(\mathbb{C})$ 是无限群.

§3.2.2 环同态的核与理想

设 $\varphi : R_1 \to R_2$ 为环同态.

定义3.29. 同态 φ 的**核** (kernel)为集合

$$\ker\varphi = \{x \in R_1 \mid \varphi(x) = 0\}. \tag{3.3}$$

由于 $\varphi(0) = 0$, 故 $\ker\varphi$ 总包含元素0, 它不是空集. 我们容易验证 $\ker\varphi$ 满足下列两条性质:

(1) 对任意 $x, y \in \ker\varphi, x \pm y \in \ker\varphi$;

(2) 对任意 $x \in \ker\varphi, a \in R_1, ax$ 与 $xa \in \ker\varphi$.

特别地, $\ker\varphi$ 对于加法和乘法封闭. 如果 $1 \in \ker\varphi$, 则 $R_1 = \ker\varphi$, 即对所有 $a \in R_1, \varphi(a) = 0$. 再由于 $\varphi(1) = 1$, 即在 R_2 中, 我们有 $0 = 1$, 即 $R_2 = 0$, 也就是说

命题3.30. *如果 $\varphi : R_1 \to R_2$ 的核 $\ker\varphi = R_1$, 则 $R_2 = 0$.*

排除上述情况, 则 $\ker\varphi$ 是 R_1 的真子集.

定义3.31. 设非空集合 $I \subseteq R$ 满足性质

(1) 对任意 $x, y \in I, x \pm y \in I$;

(2) 对任意 $a \in R, x \in I$, 则 $ax, xa \in I$.

则称 I 为 R 的**理想** (ideal).

由于 I 非空, 设 $x \in I$, 则 $0 = x - x \in I$. 又显然 $\{0\}$ 与 R 均满足理想的定义, 我们称之为 R 的**平凡理想** (trivial ideal). 如果 $I \neq R$, 称 I 为 R 的**真理想** (proper ideal).

例3.32. *$\ker\varphi$ 是 R_1 中的理想, 且如果 $R_2 \neq 0$, $\ker\varphi$ 为 R 的真理想.*

例3.33. *设 F 为域. 如果 $I \neq 0$, 令 $x \in I$, 则 $1 = x^{-1}x \in I$. 由此可得, 对任意 $a \in F, a \cdot 1 \in I$, 即 $I = F$. 故域上的理想均是平凡理想.*

例3.34. *对于环 $\mathbb{Z}$, $n\mathbb{Z}$ 是它的理想. 更进一步地, 由于 0 和 $n\mathbb{Z}$ 是加法群 $\mathbb{Z}$ 的所有子群, 而根据理想的定义, I 必是 R 的加法子群, 故 $\mathbb{Z}$ 的所有理想为 0 和 $n\mathbb{Z}$.*

命题3.35. 同态 $\varphi : R_1 \to R_2$ 为单同态当且仅当 $\ker\varphi = 0$.

证明. 由于$0 \in \ker\varphi$ 对任意环同态成立, 故必要性显然. 另一方面, 如果 $\varphi(x) = \varphi(y)$ 且 $x \neq y$, 则 $0 \neq x - y \in \ker\varphi$, 即 $\ker\varphi \neq 0$. □

设 x 为环 R 中的元素, 若理想 I 包含 x, 由理想定义, 必有

$$Rx \subseteq I,\ xR \subseteq I,\ RxR \subseteq I,$$

即有 $Rx + xR + RxR \subseteq I$. 由于 $Rx + xR + RxR$ 本身就是一个理想, 我们称之为由x **生成的理想** (ideal generated by x).

定义3.36. 环 R 中由一个元素生成的理想称为**主理想** (principal ideal).

若 R 是交换环, 则 $Rx = xR = RxR = Rx + xR + RxR$, 我们记 $(x) = Rx$ 为 x 生成的主理想. 可以看出 $(0) = \{0\}, R = (1)$ 均是主理想. 如果 I 由 $x_1, \ldots, x_n$ 生成, 记 $I = (x_1, \ldots, x_n)$.

定义3.37. 如果整环 R 中的理想均是主理想, 则 R 称为**主理想整环** (principal ideal domain, 简称 PID).

例3.38. *整数环 $\mathbb{Z}$ 中所有理想均是主理想, 故 $\mathbb{Z}$ 是 PID.*

命题3.39. *设 F 为域, 则 $F[x]$ 为 PID.*

证明. 设 I 为 $F[x]$ 中的非零理想, 设 f 是 I 中非零多项式中次数最低的. 如果 $\deg f = 0$, 则 $f = a$ 为常数多项式, 故 $1 = a^{-1}a \in I$, 所以 $I = (1) = F[x]$.

如果 $\deg f > 0$, 对于任意 $g \in I$, 由带余除法有

$$g = fq + r, \quad r = 0 \text{ 或 } \deg r < \deg f.$$

由于 $g \in I, fq \in I, r = g - fq \in I$. 由 f 的次数最低性知 $r = 0$, 即 $g \in (f)$. 故 $I = (f)$ 为主理想. □

注记. 由证明可知, 多项式的带余除法起了关键作用. 此方法对于一般环上的多项式, 如 $\mathbb{Z}[x]$ 并不适用. 事实上, $(2, x)$ 不是 $\mathbb{Z}[x]$ 上的主理想, 即 $\mathbb{Z}[x]$ 不是主理想整环.

§3.2.3 环同态的更多典型例子

(I) $\mathbb{Z}$ 到 R 的典范同态.

设环 $R \neq 0$. 在 R 中, 如果整数 $n > 0$, 我们在本章第一节定义了 $nx = x + \cdots + x$ 为 n 个 x 相加; 如果 $n < 0$, 定义 $nx = -(-nx)$. 则

$$\varphi : \mathbb{Z} \to R, \quad n \mapsto n \cdot 1_R$$

为环的同态. 令 $\ker\varphi$ 为 φ 的核, 则 $\ker\varphi$ 为 $\mathbb{Z}$ 的理想, 我们有 $\ker\varphi = (0)$ 或 $n\mathbb{Z}$.

定义3.40. 如果 $\ker\varphi = (0)$, 则对于所有正整数 $k, k \cdot 1_R \neq 0$. 如果 $\ker\varphi = n\mathbb{Z}$, 则 n 为最小正整数, 使得 $n \cdot 1_R = 0$ ($n \geqslant 2$), 故 $nx = n1_R \cdot x = 0 \cdot x = 0$.

定义3.41. 如果 $\ker\varphi = (0)$, 称环 R 的**特征** (characteristic)为 0; 如果 $\ker\varphi = n\mathbb{Z}$ ($n \geqslant 2$), 称 R 的特征为 n,. 记 R 的特征为 $\mathrm{char}R$.

命题3.42. *如果 R 为整环, 则 $\mathrm{char}R = 0$ 或 p, 其中 p 为素数.*

证明. 如果 $\mathrm{char}R = n = n_1 \cdot n_2$ 为合数, 则 $n \cdot 1_R = n_1 1_R \cdot n_2 1_R = 0$, 故 $n_1 1_R = 0$ 或 $n_2 1_R = 0$, 与 n 的最小性矛盾. □

例3.43. *环 $\mathbb{Z}/n\mathbb{Z}$ ($n \geqslant 2$) 的特征为 n. 特别地, 如果 $n = p$ 为素数, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ 为域(自然是整环!), 特征为 p.*

(II) 多项式的赋值映射.

设 R 为交换环, $R[x]$ 为 R 上的多项式环, 则 R 是 $R[x]$ 的子环, 记i 为自然环同态 $R \to R[x]$. 另一方面, 我们有

命题3.44. *设 $\varphi : R \to R'$ 为环同态.*

(1) *对任意 $\alpha \in R'$, 存在唯一环同态 $\Phi : R[x] \to R'$, 使得 $\varphi = \Phi \circ i$, 且 $\Phi(x) = \alpha$.*

(2) *更进一步地, 对 $\alpha_1, \ldots, \alpha_n$, 存在唯一环同态*

$$\Phi : R[x_1, \ldots, x_n] \to R'$$

使得 $\varphi = \Phi \circ i$, 其中 i 为环同态 $R \to R[x_1, \ldots, x_n]$.

证明. 我们只证明(1), (2)的证明类似.

首先, 如果 $\varphi = \Phi \circ i$ 且 $\Phi(x) = \alpha$, 则

$$\Phi : \sum_n a_n x^n \mapsto \sum_n \varphi(a_n)\alpha^n$$

唯一确定. 我们只要证明上述映射为同态, 这个可以直接验证. □

注记. (1) 如果 $R' = R$, φ 为恒等映射, 则 $\Phi : R[x] \to R$ 为**赋值映射** $P(x) \mapsto P(\alpha)$.

(2) 设 $\varphi : R \to R_1$ 为环同态, 仍记 φ 为复合同态 $R \to R_1 \to R_1[x]$. 取 $\alpha = x$, 则我们有映射 $\Phi : R[x] \to R'[x]$, 其在 R 上的限制为 φ.

例3.45. 设 $R = \mathbb{Z}$, 取 $\varphi : \mathbb{Z} \to \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, 则我们得到同态 $\Phi : \mathbb{Z}[x] \to \mathbb{F}_p[x]$, $f(x) \mapsto f(x) \mod p$.

推论3.46. 设 $X = (X_1, \ldots, X_m), Y = (Y_1, \ldots, Y_n)$, 则

$$R[X, Y] \cong R[X][Y].$$

证明. 由同态 $\varphi : R \hookrightarrow R[X][Y]$ 及命题 3.44我们得到

$$\Phi : R[X, Y] \to R[X][Y], \text{ 其中 } \Phi(X_i) = X_i, \Phi(Y_j) = Y_j.$$

由同态 $\psi : R[x] \hookrightarrow R[X, Y]$, 令 $\alpha_i = Y_i$, 我们得到同态 $\Psi : R[X][Y] \to R[X, Y]$. 只需验证 $\Psi \circ \Phi = \mathrm{id}, \Phi \circ \Psi = \mathrm{id}$. □

例3.47. 令 $\alpha \in \mathbb{C}$, 则 $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Z}[\alpha]$ 是环的同态. 应用命题 *3.44*, 我们得到环同态 $\Phi : \mathbb{Z}[x] \to \mathbb{Z}[\alpha]$, $P(x) \mapsto P(\alpha)$.

首先 Φ 是满同态. 更进一步地, 如果 α 为超越元, 则 $\ker \Phi = 0$. 故 Φ 是单同态, 我们得到同构 $\mathbb{Z}[x] \cong \mathbb{Z}[\alpha]$.

如果 α 为代数元, 则 $\ker \Phi \neq 0$, Φ 不是单同态.

习 题

习题2.1. 证明整环 $\mathbb{Z}[\sqrt{d}]$ 的任何一个非零理想都包含一个非零整数.

习题2.2. 确定 $\mathrm{Aut}(\mathbb{Q}[\sqrt{d}])$, $d \in \mathbb{Q}^\times - (\mathbb{Q}^\times)^2$ 和 $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$.

习题2.3. 证明复数域 $\mathbb{C}$ 可嵌入到环 $M_2(\mathbb{R})$ 中.

习题2.4. 求下列环同态的核的生成元:

(1) $\mathbb{R}[x,y] \to \mathbb{R} : f(x,y) \mapsto f(0,0)$;

(2) $\mathbb{R}[x] \to \mathbb{C} : f(x) \mapsto f(2+i)$;

(3) $\mathbb{Z}[x] \to \mathbb{R} : f(x) \mapsto f(1+\sqrt{2})$;

(4) $\mathbb{C}[x,y,x] \to \mathbb{C}[t] : x \mapsto t, y \mapsto t^2, z \mapsto t^3$.

习题2.5. 求环同态 $\varphi : \mathbb{C}[x,y] \to \mathbb{C}[t];\ x \mapsto t+1,\ y \mapsto t^3-1$ 的核 K. 证明 $\mathbb{C}[x,y]$ 的每一个包含 K 的理想 I 都可以由2个元素生成.

习题2.6. 设 I, J 是环 R 的理想. 求证:

(1) $IJ = \{\sum_{k=1}^n a_k b_k \mid a_k \in I, b_k \in J\}$ 也是环 R 的理想, 且 $IJ \subseteq I \cap J$;

(2) $I+J$ 也是环 R 的理想, 并且它恰好是包含 I 和 J 的最小理想;

(3) 设 $I = n\mathbb{Z}, J = m\mathbb{Z}(n, m \geqslant 1)$ 是整数环 $\mathbb{Z}$ 的两个理想. 求$IJ, I+J, I \cap J$.

习题2.7. 设 I 是交换环 R 中的理想. 定义

$$\sqrt{I} = \{r \in R \mid \text{存在 } n \geqslant 1, \text{使得 } r^n \in I\}.$$

(1) $\sqrt{I}$ 是 R 的理想.

(2) $\sqrt{I} = R$ 当且仅当 $I = R$.

(3) $\sqrt{\sqrt{I}} = \sqrt{I}$.

(4) $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}, \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} = \sqrt{IJ}$.

习题2.8. 设 R 为含幺环. 集合 $C(R) = \{c \in R \mid \text{对于每个 } r \in R, rc = cr\}$ 叫做环 R 的**中心**.

(1) $C(R)$ 是 R的子环, 但不一定是 R 的理想.

(2) 如果 F 为域, 确定全矩阵环 $M_n(F)$ 的中心.

习题2.9. 证明只有有限个理想的整环 R 是域.

习题2.10. 设 $f : R \to S$ 是环同态. 如果 R 是体,求证 f 或者是零同态,或者是嵌入.

习题2.11. 设 $I_1, \cdots, I_n, \cdots$ 均是环R的理想, 并且 $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$. 求证集合$\bigcup\limits_{i=1}^{\infty} I_i$ 也是环 R 的理想.

习题2.12. (1) 设 R 为含幺交换环. 求证环 $M_n(R)$ 中每个理想均有形式 $M_n(I)$, 其中 I 是 R 的某个理想;

(2) 若 F 为域, 则 $M_n(F)$ 是单环, 即没有非平凡理想.

习题2.13. 求证 $T = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}$ 是环 $M_2(\mathbb{Z})$ 的子环. 试确定环 T 的所有理想.

习题2.14. 设 z 是复平面上一点, f 和 g 为在 z 点全纯的函数. 若 f 和 g 在 z 一个开邻域内相等, 称 f 和 g 等价. 令 O_z 为所有在 z 处全纯的函数的等价类, 则 O_z 关于函数加法和乘法成为一个环. 确定它的单位群和所有理想.

§3.3 环的同态基本定理

§3.3.1 理想与商环

设 R 为环, I 是 R 的一个理想, 由理想的性质知 I 是 R 的加法子群, 故 R/I 是加法商群. 如果 $a - b \in I$, 记 $a = b \bmod I$.

定理3.48. 令 I 是环 R 的理想, 则

(1) $\bar{R} = R/I$ 上存在唯一的环结构, 使得 $\pi : R \to \bar{R}, a \mapsto \bar{a} = a + I$ 是环的满同态.

(2) $\ker \pi = I$.

证明. 只需证明在 $\bar{R}$ 上的乘法 $\bar{a}\,\bar{b} = \overline{ab}$ 与 $\bar{a}, \bar{b}$ 的代表元 a, b 的选取无关, 其它易证.

如果 $\bar{a}_1 = \bar{a}, \bar{b}_1 = \bar{b}$, 则 $a - a_1 \in I, b - b_1 \in I$, 故 $ab - a_1b_1 = (a - a_1)b + a_1(b - b_1) \in I$, 即 $\overline{ab} = \overline{a_1b_1}$. □

注记. (1) 在商群 G/N 定义乘法时, 我们有 $aN \cdot bN = abN$ 为集合间的等式. 但 R/I 的乘法中, 作为集合 $(a + I)(b + I) \subseteq ab + I$, 但不一定相等.

(2) 设 S 为 R 的加法子群, R/S 为商群. 如果在 R/S 上定义乘法 $\bar{a}\,\bar{b} = \overline{ab}$, 使得 R/S 为环, 则 S 必为 R 上的理想. 事实上, 对任意 $a_1 = a \bmod S$, $b_1 = b \bmod S$, 则由 $\overline{a_1 b} = \overline{ab}$ 知 $(a_1 - a)b \in S$. 由 $\overline{ab} = \overline{ab_1}$ 知 $a(b - b_1) \in S$. 故 S 满足理想的条件.

§3.3.2 环同态基本定理

定理3.49. 设 $f : R \to R'$ 为环同态, 则

(1) $\ker f$ 是 R 的理想, $\mathrm{im} f$ 是 R' 的子环.

(2) 同态 $f = i \circ \bar{f} \circ \pi$, 即

$$f: \quad R \xrightarrow{\pi} R/\ker f \xrightarrow{\bar{f}} \mathrm{im} f \xrightarrow{i} R', \tag{3.4}$$

其中 π 为自然满同态, i 为自然单同态, 而

$$\bar{f}: \quad R/\ker f \longrightarrow \mathrm{im} f, \quad \bar{a} \longmapsto f(a) \tag{3.5}$$

为同构.

证明. 只需证明 $\bar{f} : R/\ker f \to \mathrm{im} f$ 为环同构. 首先, 由群的同态基本定理知 $\bar{f}$ 是定义良好的加法群的同构. 只需说明 $\bar{f}$ 满足 $\bar{f}(\bar{1}) = 1$ 及 $\bar{f}(\bar{a}\,\bar{b}) = \bar{f}(\bar{a})\bar{f}(\bar{b})$ 即可, 这些都是显然的. □

定理3.50. 设 J 为环 R 的理想, $\bar{R} = R/J$, π 为自然环同态 $R \to \bar{R}$, 则

(1) R 中包含 J 的理想集合与 $\bar{R}$ 中的理想集合以如下方式一一对应:

$$I \mapsto \pi(I), \quad \bar{I} \mapsto \pi^{-1}(\bar{I}).$$

(2) 如果 I 对应 $\bar{R}$ 中的理想 $\bar{I}$, 则 $R/I \cong \bar{R}/\bar{I}$.

证明. 对于(1), 只需证

(i) 如果 $I \supseteq J$ 是 R 中的理想, 则 $\pi(I)$ 是 $\bar{R}$ 中的理想.

(ii) 如果 $\bar{I}$ 是 $\bar{R}$ 中的理想, 则 $\pi^{-1}(\bar{I})$ 是 R 中的理想(自然包含 J!).

(iii) $\pi\pi^{-1}(\bar{I}) = \bar{I}, \pi^{-1}\pi(I) = I$.

(i)的证明是显然的. 对于(ii), 设 $\bar{I}$ 是 $\bar{R}$ 的理想. 考虑

$$R \xrightarrow{\pi} \bar{R} \xrightarrow{\varphi} \bar{R}/\bar{I}.$$

则 $\varphi \circ \pi$ 为满同态, 且

$$\ker(\varphi \circ \pi) = \{r \in R \mid \pi(r) \in \ker \varphi = \bar{I}\} = \pi^{-1}(\bar{I}),$$

故 $\pi^{-1}(\bar{I})$ 为 R 中理想, 且 $R/\pi^{-1}(\bar{I}) \cong \bar{R}/\bar{I}$, 即我们证明了(ii)及定理的(2).

(iii)由集合映射的性质, 我们首先有 $\pi^{-1}(\pi(I)) \supseteq I$ 且 $\pi(\pi^{-1}(\bar{I})) \subseteq I$. 再由 π 是满射, 知 $\pi(\pi^{-1}(\bar{I})) = \bar{I}$. 只需证明 $\pi^{-1}(\pi(I)) \subseteq I$.

设 $x \in \pi^{-1}(\pi(I))$, 则存在 $y \in I, \pi(x) = \pi(y)$, 故 $\pi(x-y) = 0$, 即 $x - y \in J \subseteq I$, 所以 $x = y + (x-y) \in I$, 即 $\pi^{-1}(\pi(I)) = I$. □

§3.3.3 同态基本定理的应用

例3.51. $\mathbb{Z}[i]/(1+3i)$ 同构于 $\mathbb{Z}/10\mathbb{Z}$.

事实上, 考虑映射 $\varphi : \mathbb{Z} \to R = \mathbb{Z}[i]/(1+3i)$, $1 \mapsto \bar{1}$. 我们证明 φ 是满射, 且 $\ker\varphi = 10\mathbb{Z}$. 由于在 R 中, $\overline{1+3i} = 0$, 即有 $\bar{i} = -\bar{3}$, 故 φ 是满射. 设 $\varphi(n) = \bar{n} = 0$, 则 $n = (1+3i)(x+yi)$, 比较系数知 $n = x - 3y$ 且 $3x + y = 0$, 故 $n = 10x$, 即 $\ker\varphi = 10\mathbb{Z}$.

例3.52. 设整环 R 的特征为素数 p, 则 $\varphi : \mathbb{Z} \to R$ 诱导 $\mathbb{F}_p \subseteq R$ 且对所有 $x \in R$, $px = 0$. 如果 R 的特征为 0, 则有 $\mathbb{Z} \subseteq R$, 如果 R 为域, 则有 $\mathbb{Q} \subseteq R$.

对于特征 p 的整环, 我们有

命题3.53. 对任意 $x, y \in R, (x+y)^p = x^p + y^p$.

证明. 由牛顿二项式定理

$$(x+y)^p = x^p + y^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i}.$$

又由于 $p \mid \binom{p}{i}$ 对 $1 \leqslant i \leqslant p-1$ 成立, 故命题得证. □

推论3.54. 设 R 为特征 p 的整环, 则 $\sigma : R \to R$, $x \mapsto x^p$ 为环 R 的自同态, 且 σ 为单同态.

注记. σ 称为 R 的(绝对) **Frobenius映射** (Frobenius map).

例3.55. $\mathbb{C}[x,y]/(xy) \cong I$, 其中

$$I = \{(p(x), q(y)) \mid p(0) = q(0)\} \subseteq \mathbb{C}[x] \times \mathbb{C}[y].$$

我们来证明这一事实. 赋值映射 $\mathbb{C}[x,y] \to \mathbb{C}[x]$, $f(x,y) \mapsto f(x,0)$ 为满射, 其核为 (x), 即我们有 $\mathbb{C}[x,y]/(x) \cong \mathbb{C}[x]$, 同理, $\mathbb{C}[x,y]/(y) \cong \mathbb{C}[y]$, 故同态

$$\begin{aligned} \mathbb{C}[x,y] &\longrightarrow \mathbb{C}[x] \times \mathbb{C}[y] \\ f(x,y) &\longmapsto (f(x,0), f(0,y)) \end{aligned}$$

的核为 (xy), 其像即 I.

§3.3.4 中国剩余定理

定理3.56. 设 R 为环, $I_1, \ldots, I_n$ 为 R 的理想, 且当 $i \neq j$ 时, $I_i + I_j = R$, 则

$$R/I_1 \cap \cdots \cap I_n \cong \prod_{i=1}^{n} R/I_i.$$

证明. 我们首先证明

$$I_1 + I_2 \cdots I_n = R.$$

由 $I_1 + I_2 = R$ 及 $I_1 + I_3 = R$, 则

$$R = (I_1 + I_2)(I_1 + I_3) = (I_1 + I_2)I_1 + I_1 I_3 + I_2 I_3 = I_1 + I_2 I_3.$$

由归纳知 $I_1 + I_2 I_3 \cdots I_n = R$.

取 $1 \in R$, 则存在 $a \in I_1, b \in I_2 I_3 \cdots I_n, a + b = 1$, 故

$$b = 1 \mod I_1,\ b = 0 \mod I_2,\ \ldots,\ b = 0 \mod I_n.$$

同理, 对任意 i, 我们有 $x_i \in R$, 且

$$x_i = 0 \mod I_i,\ x_i = 0 \mod I_j (\text{如果 } j \neq i).$$

现在考虑同态

$$\begin{aligned} \varphi : R &\longrightarrow \prod_i R/I_i \\ x &\longmapsto (x \mod I_1, \ldots, x \mod I_n). \end{aligned}$$

则 $\ker\varphi = I_1 \cap \cdots \cap I_n$. 对于 $(\bar{a}_1, \ldots, \bar{a}_n) \in \prod_i R/I_i$, 则令 $x = a_1x_1 + a_2x_2 + \cdots + a_nx_n$, 则 $\varphi(x) = (\bar{a}_1, \ldots, \bar{a}_n)$, 故 φ 是满同态. 由同态基本定理, 定理得证. □

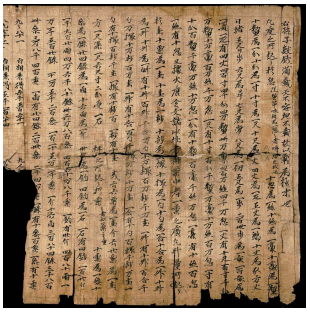


图 3.2: 《孙子算经》唐代抄本

图 3.3: 《算法统宗》明代原本

注记. 中国剩余定理(Chinese Remainder Theorem)是中国人对数学研究的杰出贡献, 又称为孙子定理, 源自中国古代数学名著《孙子算经》(公元四、五世纪)卷下第26题: “今有物不知其数, 三三数之剩二, 五五数之剩三, 七七数之剩二, 问物几何? ” 用代数的语言, 即求正整数 x, 使得

$$x \equiv 2 \mod 3, \quad x \equiv 3 \mod 5, \quad x \equiv 2 \mod 7.$$

由上述定理的证明, 只要先求出 x_1, x_2, x_3 使得

$$x_1 \equiv 1 \mod 3, \quad x_1 \equiv 0 \mod 5, \quad x_1 \equiv 0 \mod 7,$$

$$x_2 \equiv 0 \mod 3, \quad x_2 \equiv 1 \mod 5, \quad x_2 \equiv 0 \mod 7,$$

$$x_3 \equiv 0 \mod 3, \quad x_3 \equiv 0 \mod 5, \quad x_3 \equiv 1 \mod 7,$$

我们可取 $x_1 = 70, x_2 = 21, x_3 = 15$, 则

$$x \equiv 2x_1 + 3x_2 + 2x_3 \mod (3 \times 5 \times 7) \equiv 23 \mod 105.$$

此解法即明朝数学家程大位在《算法统宗》(1593年)所言:

三人同行七十稀,
五树梅花廿一枝,
七子团圆整半月,
除百零五便得知.

习　　题

习题3.1. 证明交换环 R 中全部幂零元素组成的集合 $N=\mathrm{Nil}(R)$ 是环 R 的理想, 并且商环 R/N 中只有零元素是幂零理想.

习题3.2. 设 I 是含幺交换环 R 中的理想. 求证有环同构:

$$M_n(R)/M_n(I)\cong M_n(R/I).$$

习题3.3. 设 $f:R\to S$ 是环的同态. I 和 J 是环 R 和 S 的理想, 并且 $f(I)\subseteq J$, 按如下方式作商环之间的映射:

$$\bar{f}:R/I\to S/J,\quad a\mapsto [f(a)],$$

其中对于 $a\in R,\bar{a}=a+I$ 为 R/I 中的元素, 而 $[f(a)]=f(a)+J$ 为 S/J 中元素.

(1) 证明上述映射 $\bar{f}$ 是良好定义的, 并且是环同态;

(2) 证明 $\bar{f}$ 是环同构当且仅当 $f(R)+J=S$ 并且 $I=f^{-1}(J)$.

习题3.4. 设 $(R,+,\cdot)$ 是含幺环. 对于 $a,b\in R$, 定义

$$a\oplus b=a+b+1,\quad a\odot b=ab+a+b.$$

证明 $(R,\oplus,\odot)$ 也是含幺环, 并且与环 $(R,+,\cdot)$ 同构.

习题3.5. (1) 主理想环的每个同态像也是主理想环.

(2) 求证 $\mathbb{Z}/m\mathbb{Z}(m\geqslant 1)$ 是主理想环.

习题3.6. 设S, $R_i(i\in I)$ 均为环, $R=\prod\limits_{i\in I}R_i$ 是R_i 的笛卡尔积.

(1) 令 $\pi_i:R\to R_i$, $(a_j)_{j\in I}\mapsto a_i$, 证明 π_i 为环同态. 这样的环同态称为**正则投射**.

(2) 设对于每个 $i\in I$, $\varphi_i:S\to R_i$ 均为环同态. 求证存在唯一的环同态 $\varphi:S\to R$, 使得对于每个$i\in I$, 均有$\pi_i\circ\varphi=\varphi_i$.

习题3.7. 设 D 为整环, m 和 n 为互素的正整数. $a,b\in D$, 如果 $a^m=b^m$, $a^n=b^n$, 证明 $a=b$.

习题3.8. 设 $I_1,\dots,I_n$ 是环 R 的理想且

(1) $I_1+\cdots+I_n=R$;

(2) 对于每个 $i(1\leqslant i\leqslant n)$, $I_i\cap(I_1+\cdots+I_{i-1}+I_{i+1}+\cdots+I_n)=(0)$.

证明 $R\cong\prod\limits_{i=1}^{n}I_i$.

习题3.9. 环 R 中元素 e 叫做**幂等元素**, 是指 $e^2=e$. 如果 e 又属于环 R 的中心, 则称 e 为**中心幂等元素**. 设 R 是含幺环, e 为 R 的中心幂等元素. 证明

(1) $1-e$ 也是中心幂等元素.

(2) eR 和 $(1-e)R$ 均是 R 的理想, 并且 $R\cong eR\times(1-e)R$.

习题3.10. 设I, J 是环 R 的理想,满足 $I+J=R$, 及 $IJ=0$.

(1) 证明: $R\cong R/I\times R/J$;

(2) 描述对应于这个直积分解的幂等元.

习题3.11. 环 R 中幂等元集合 $\{e_1,\dots,e_n\}$ 叫做**正交的**, 是指当 $i\neq j$ 时, $e_ie_j=0$. 设 $R,R_1,\dots,R_n$ 都是含幺环. 则下列两个条件等价:

(1) $R\cong R_1\times\cdots\times R_n$;

(2) R 具有正交的中心幂等元集合 $\{e_1,\cdots,e_n\}$, 使得 $e_1+\cdots+e_n=1_R$, 并且 $e_iR\cong R_i(1\leqslant i\leqslant n)$.

§3.4 整环与域

在环论研究中, 最好处理的研究对象自然是域. 由此可以得到数学中两大基础学科之一的线性代数理论. 因此如何构造域是环论中一个重要问题.

退而求其次, 由于域是特殊的整环, 我们首先可以考虑如何从交换环得到整环, 即对于交换环 R, 我们考虑理想 I, 使得 R/I 是整环. 我们其次再考虑如何由整环得到域.

§3.4.1 素理想与极大理想

我们首先考虑 $\mathbb{Z}$ 上的素数 p, 它对应于理想 $p\mathbb{Z}$, 且其商环 $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ 是域. 由初等数论可知, p 满足如下性质:

(i) (欧几里得引理) 如果 $p \mid ab$, 则 $p \mid a$ 或 $p \mid b$.

(ii) 如果理想 $p\mathbb{Z} \subseteq I \subseteq \mathbb{Z}$, 则 $I = \mathbb{Z}$ 或 $I = p\mathbb{Z}$.

此两个性质, 即对应于素理想和极大理想的定义.

定义3.57. 交换环 R 上的真理想 $\mathfrak{p}$ 称为 R 的**素理想**, 如果对于 $a, b \in R, ab \in \mathfrak{p}$, 则 $a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$.

环 R 上所有素理想的集合记为 Spec$R$, 称为 R 的**素谱**.

定义3.58. 交换环 R 上的真理想 $\mathfrak{m}$ 称为 R 的**极大理想**, 是指如果理想 $J \supsetneqq \mathfrak{m}$, 则 $J = R$.

环 R 上所有极大理想的集合记为 Max$R$, 称为 R 的**极大谱**.

注记. Spec$R$ (与 Max$R$)是仿射代数几何中最重要的概念, 在今后的数学研究中会经常遇到.

命题3.59. *设R 为交换环, 则下列条件等价:*

(1) $\mathfrak{p}$ *是* R *的素理想;*

(2) *如果理想* $I_1 I_2 \subseteq \mathfrak{p}$, *则* $I_1 \subseteq \mathfrak{p}$ *或* $I_2 \subseteq \mathfrak{p}$;

(3) $R/\mathfrak{p}$ *是整环.*

证明. (1) $\Longrightarrow$ (2). 如果 $I_1 \nsubseteq \mathfrak{p}, I_2 \nsubseteq \mathfrak{p}$, 则存在 $a \in I_1 \backslash \mathfrak{p}, b \in I_2 \backslash \mathfrak{p}$, 且 $ab \in I_1 I_2 \subseteq \mathfrak{p}$, 与 $\mathfrak{p}$ 是素理想矛盾.

(2) $\Longrightarrow$ (3). 如果 $\bar{a} \cdot \bar{b} = 0 \in R/\mathfrak{p}$, 则 $ab \in \mathfrak{p}$, 即 $(a)(b) \subseteq \mathfrak{p}$, 故 $(a) \subseteq \mathfrak{p}$ 或 $(b) \subseteq \mathfrak{p}$. 所以 $\bar{a} = 0$ 或 $\bar{b} = 0$, 即 $R/\mathfrak{p}$ 中没有零因子.

(3) $\Longrightarrow$ (1). 如果 $ab \in \mathfrak{p}$, 则 $\overline{ab} = 0 \in R/\mathfrak{p}$, 故 $\bar{a} = 0$ 或 $\bar{b} = 0$, 即 $a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$. □

命题3.60. *设R 为交换环, 则下列条件等价*

(1) $\mathfrak{m}$ *是* R *的极大理想.*

(2) $R/\mathfrak{m}$ *是域.*

证明. (1) $\Longrightarrow$ (2). 我们首先证明如果 0 是 R 的极大理想, 则 R 为域. 事实上, 对任意 $x \in R, x \neq 0, 0 \subsetneqq (x)$, 故 $(x) = R$, 即存在 $y \in R, xy = 1$, 所以 x 可逆, R 为域.

对于一般情况, 由于 $R/\mathfrak{m}$ 中的理想与 R 中包含 $\mathfrak{m}$ 的理想一一对应(定理 3.50), 故若 $\mathfrak{m}$ 为极大理想, (0) 是 $R/\mathfrak{m}$ 中的极大理想, 所以 $R/\mathfrak{m}$ 是域.

(2) $\Longrightarrow$ (1). 如果 $R/\mathfrak{m}$ 为域, 则 0 是 $R/\mathfrak{m}$ 的极大理想, 故 $\mathfrak{m}$ 是 R 中的极大理想. □

推论3.61. *极大理想都是素理想, 即* $\mathrm{Spec}R \supseteq \mathrm{Max}R$.

例3.62. *对于整数环* $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ *是整环当且仅当* n *为素数, 此时* $\mathbb{Z}/n\mathbb{Z}$ *为域, 故*

$$\mathrm{Spec}\ \mathbb{Z} = \{0\} \cup \mathrm{Max}\mathbb{Z} = \{0, p\mathbb{Z} \mid p\text{为素数}\}.$$

例3.63. *设* F *为域,* $R = F[x]$. *由命题 3.39 可知*R *上的理想为*0 *或者*$(f(x))$.

由于 R *为整环但不是域(*x *不可逆),* 0 *为* R *的素理想但不是极大理想. 而*$R/(f(x))$ *是整环当且仅当* $f(x)$ *为不可约多项式, 此时* $R/(f(x))$ *是域. 事实上, 设* $0 \neq \bar{u}(x) \in R/(f(x))$, *则* $(u(x), f(x)) = 1$, *故存在* $v(x), g(x)$, *使得*$u(x)v(x) + f(x)g(x) = 1$, *所以* $\bar{u}(x) \cdot \bar{v}(x) = \bar{1}, \bar{u}(x)$ *可逆, 故*

$$\mathrm{Spec}\ F[x] = \{0\} \cup \mathrm{Max}F[x] = \{0, (f(x)) \mid f(x)\text{为}F[x]\text{上首一不可约多项式}\}.$$

特别地, 取 $F = \mathbb{C}$, *由代数学基本定理(我们将在*§*5.3 证明),* $f(x)$ *必有* $x - \alpha$, $\alpha \in \mathbb{C}$ *的形式, 即*

$$\mathrm{Spec}\ \mathbb{C}[x] = \{0\} \cup \{(x - \alpha) \mid \alpha \in \mathbb{C}\}.$$

例3.64. *设* $R = \mathbb{Z}[x]$, *则* $\mathfrak{p} = (2)$ *是* R *上的素理想但不是极大理想. 事实上,* $(2) \subsetneqq (2, x) \subsetneqq R$, $(2, x)$ *是* R *上的极大理想.*

对于一般交换环 R, 是否一定存在极大理想呢? 这个问题的回答, 需要用到集合论中的**选择公理**, 或者其等价形式**Zorn 引理**.

引理3.65 (Zorn 引理)**.** *在任何一非空的偏序集中, 若任何全序子集都有上界, 则此偏序集内必然存在极大元素.*

命题3.66. 设 $\mathfrak{a} \neq R$ 是交换环 R 中的任意理想, 则 $\mathfrak{a}$ 包含在 R 中某极大理想 $\mathfrak{m}$ 中.

证明. 设 X 为 R 中所有包含 $\mathfrak{a}$ 且不等于 R 的理想的集合. 则根据包含关系, X 是一个偏序集. 如果 $\{\mathfrak{b}_i\}$ 是其中一个全序集, 则 $1 \notin \mathfrak{b}_i$ 对所有 i 成立, 故 $1 \notin \mathfrak{b} = \bigcup \mathfrak{b}_i$, 即 $\mathfrak{b}$ 是所有$\mathfrak{b}_i$ 的上界. 由Zorn引理, X 中存在极大元 $\mathfrak{m} \neq R$, 它一定是极大理想. □

§3.4.2 整环的局部化

整环的局部化, 即是由整环 D 得到一个域 F, 使得 D 为 F 的子环. 我们可以类比由整数环 $\mathbb{Z}$ 得到有理数域 $\mathbb{Q}$ 的过程.

(i) 我们需要 $m \in \mathbb{Z}\backslash\{0\}$ 可逆, 故得到 $\frac{1}{m}$.

(ii) 对 $\frac{1}{m}$ 迭加, 得到分数 $\frac{n}{m}$.

(iii) 两个分数可能相等, 即 $\frac{n}{m} = \frac{n_1}{m_1}$ 如果 $m_1 n = m n_1$.

(iv) 分数的加法与乘法.

由此即得到域 $\mathbb{Q}$, 且由映射 $n \mapsto \frac{n}{1}$, $\mathbb{Z}$ 视为 $\mathbb{Q}$ 的子环.

对于整环 D, 我们有同样过程. 考虑集合

$$D \times (D - \{0\}) = \{(r, s) \mid r \in D, s \in D - \{0\}\}.$$

我们在其上定义关系

$$(r, s) \sim (r', s') \quad \text{如果} \quad r's = rs'.$$

容易验证 $\sim$ 是等价关系. 令 $\frac{r}{s}$ 表示 (r, s) 所在的等价类(分数), 令

$$K = \left\{ \frac{r}{s} \;\middle|\; r \in D, s \in D - \{0\} \right\} \tag{3.6}$$

为所有等价类的集合.

定理3.67. 集合 K 在运算

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}, \quad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'} \tag{3.7}$$

下构成域, 它的零元 $0 = \frac{0}{1}$, 单位元 $1 = \frac{1}{1}$, 且

(1) $f : D \to K, a \mapsto \frac{a}{1}$ 是单同态*(*嵌入*)*.

(2) 设 φ 是环 D 到域 F 的嵌入, 则存在唯一的域的嵌入 $\psi : K \to F$ 使得 $\varphi = \psi \circ f$.

注记. 由(1), 可以将 D 看成 K 的子环, 而由(2)可以认为 K 是包含 D 的最小子域.

定义3.68. 域 K 称为整环 D 的**商域** (quotient field).

定理的证明. 首先需要证明 K 上的加法运算与乘法运算与代表元的选取无关. 我们对加法证明. 如果

$$\frac{r_1}{s_1}=\frac{r_2}{s_2},\quad \frac{r_1'}{s_1'}=\frac{r_2'}{s_2'},$$

即

$$r_1s_2=r_2s_1,\quad r_1's_2'=r_2's_1'.$$

则

$$\frac{r_1}{s_1}+\frac{r_1'}{s_1'}=\frac{r_1s_1'+r_1's_1}{s_1s_1'},\quad \frac{r_2}{s_2}+\frac{r_2'}{s_2'}=\frac{r_2s_2'+r_2's_2}{s_2s_2'}.$$

由于

$$\begin{aligned}&(r_1s_1'+r_1's_1)s_2s_2'=r_1s_2s_1's_2'+r_1's_2's_1s_2\\ =&r_2s_1s_1's_2'+r_2's_1's_1s_2=s_1s_1'(r_2s_2'+r_2's_2),\end{aligned}$$

故加法的定义与代表元选取无关.

验证 K 是域的其他条件类似. 下面证明(1)和(2).

(1)的证明: 易验证 f 是同态, 且

$$\ker f=\left\{r\in D\;\middle|\;\frac{r}{1}=\frac{0}{1}\right\}=\{0\},$$

故 f 是单同态.

(2)的证明: 令 $\psi:K\to F,\psi(\frac{r}{s})=\varphi(r)\varphi(s)^{-1}$, 则 ψ 与代表元选取无关, 且是环(从而是域)的同态. 由于 ψ 不是零同态, 故 $\ker\psi=0$, 因此 ψ 是域的嵌入. 容易验证 $\psi=\varphi\circ f$.

我们证明 ψ 的唯一性. 首先 $\psi(\frac{r}{1})=\varphi(r)$, 其次 $\psi(\frac{s}{1}\cdot\frac{1}{s})=\varphi(s)\cdot\psi(\frac{1}{s})$, 故 $\psi(\frac{r}{s})=\varphi(r)\varphi(s)^{-1}$. □

以上由整环得到其商域的方法, 称为**局部化** (localization) 方法. 事实上, 对于集合 $S\subseteq D\backslash\{0\}$, 若它满足条件(i) $1\in S$, (ii) 如果 $a\in S,b\in S$, 则 $ab\in S$(即 S 为 $D\backslash\{0\}$ 上乘法含幺半群), 则我们同样可以构造整环

$$S^{-1}D=\{\frac{r}{s}\;\big|\;r\in D,s\in S\},$$

使得 D 是 $S^{-1}D$ 的整环. 这样的集合S 称为**乘法集**. 在未来的代数学习和研究中, 局部化方法将起到很重要的作用.

习　　题

习题4.1. 设 R 是含幺交换环, $\mathfrak{p}_1,\ldots,\mathfrak{p}_m$ 为 R 的素理想而 A 为 R 的理想. 如果 $A\subseteq\mathfrak{p}_1\cup\cdots\cup\mathfrak{p}_m$, 则必存在某个 $i(1\leqslant i\leqslant m)$, 使得 $A\subseteq\mathfrak{p}_i$.

习题4.2. 含幺交换有限环的素理想必是极大理想.

习题4.3. 交换环 R 中所有素理想均包含 $\mathrm{Nil}(R)$.

习题4.4. 设 $\mathfrak{p}$ 是含幺交换环 R 的素理想, $I_1,\ldots,I_n$ 是 R 的理想. 如果 $\mathfrak{p}=\bigcap_{i=1}^n I_i$, 则 $\mathfrak{p}$ 必等于某个 I_i.

习题4.5. 设 $f:R\to S$ 是环的满同态, $K=\ker f$.

(1) 若 $\mathfrak{p}$ 是 R 的素理想并且 $\mathfrak{p}\supseteq K$, 则 $f(\mathfrak{p})$ 也是 S 的素理想;

(2) 若 $\mathfrak{q}$ 是 S 的素理想, 则 $f^{-1}(\mathfrak{q})$ 也是 R 的素理想;

(3) S 中的素理想和 R 中包含 K 的素理想是一一对应的. 将"素理想"改成"极大理想"则此论断也成立.

习题4.6. 设 I 是环 R 的理想, 求证 R/I 中素理想均可写成形式 $\mathfrak{p}/I$, 其中 $\mathfrak{p}$ 是 R 中素理想并且包含 I. 由此证明交换环 R 的素谱 $\mathrm{Spec}R$ 与 $R/\mathrm{Nil}(R)$ 的素谱 $\mathrm{Spec}R/\mathrm{Nil}(R)$ 一一对应.

习题4.7. 设 $m\geqslant 2$. 确定 $\mathrm{Spec}(\mathbb{Z}/m\mathbb{Z})$, $\mathrm{Max}(\mathbb{Z}/m\mathbb{Z})$.

习题4.8. 确定环 $\mathbb{Z}[x]/(x^2+3,p)$ 的结构, 其中 $p=3,5$.

习题4.9. 确定下面每个环的极大理想:

(1) $\mathbb{R}\times\mathbb{R}$; (2) $\mathbb{R}[x]/(x^2)$; (3) $\mathbb{R}[x]/(x^2-3x+2)$; (4) $\mathbb{R}[x]/(x^2+x+1)$.

习题4.10. 描述环 $\mathbb{Z}[x]/(x^2-3,2x+4)$ 和 $\mathbb{Z}[i]/(2+i)$.

习题4.11. 证明 $\mathbb{Z}_p$ 是 *PID*, 且只有唯一的极大理想 $p\mathbb{Z}_p$.

习题4.12. 设R 是环, $\mathfrak{m}$ 是 R 的一个理想. 假设 R 的每个不属于 $\mathfrak{m}$ 的元素是 R 中的单位. 证明 $\mathfrak{m}$ 是 R 的唯一极大理想.

习题4.13. 设 D 为整环, K 是 D 的商域. 设集合 $S \subseteq D$ 为乘法集, 即满足条件

(i) $0 \notin S$, $1 \in S$;

(ii) 对 $x, y \in S$, 则 $xy \in S$.

定义

$$S^{-1}D = \left\{ \frac{m}{n} \mid m \in D,\ n \in S \right\} \subseteq K.$$

证明:

(1) $S^{-1}D$ 是 K 中包含 D 的子环.

(2) $S^{-1}D$ 中的素理想必有 $S^{-1}\mathfrak{p} = \{\frac{m}{n} \mid m \in \mathfrak{p},\ n \in S\}$ 的形式, 其中 $\mathfrak{p}$ 是 D 的素理想.

(3) $\mathrm{Spec}S^{-1}D$ 与集合 $\{\mathfrak{p} \in \mathrm{Spec}D \mid \mathfrak{p} \cap S = \emptyset\}$ 一一对应.

(4) 设 $D = \mathbb{Z}$, $\mathfrak{p} = p\mathbb{Z}$, $S = \mathbb{Z} - \mathfrak{p}$, 则 $\mathbb{Z}/\mathfrak{p} = \mathbb{Z}/p\mathbb{Z}$ 同构于 $S^{-1}\mathbb{Z}/S^{-1}\mathfrak{p}$.

(5) 设 $\mathfrak{p}$ 是 D 的素理想, $S = \mathbb{Z} - \mathfrak{p}$. 问何时 $D/\mathfrak{p}$ 同构于 $S^{-1}D/S^{-1}\mathfrak{p}$?

习题4.14. 设 R 是分式域为 F 的整环, $\mathfrak{p}$ 是 R 的素理想. R 在$\mathfrak{p}$ 处的局部化 $R_{\mathfrak{p}}$ 是指 F 的子环$(R-\mathfrak{p})^{-1}R = \{\frac{a}{d} \mid a, d \in R, d \notin \mathfrak{p}\}$. 试确定 $R_{\mathfrak{p}}$ 的所有极大理想.

第四章　因式分解

§4.1　唯一因式分解环

在本章, 我们假设 R 是(含幺)交换环.

本节的目的是将 $\mathbb{Z}$ 上的因子概念拓展到 R 上, 并探讨其中元素的因式分解.

§4.1.1　因子, 素元与不可约元

定义4.1. 设 $a,b\in R$. 如果 $b=ax$, 称 a 是 b 的**因子** (divisor 或factor), 而 b 是 a 的**倍元** (multiple), 记为 $a\mid b$.

如果 $a\mid b$ 且 $b\mid a$, 称 a 与 b **相伴** (associate), 记为 $a\sim b$.

如果 $b=ax$ 且 x 不是单位, 称 a 是 b 的**真因子** (proper divisor).

命题4.2. 设 $a,b\in R,u\in U(R)=R^\times$, 则

(1) $a\mid b$ 当且仅当 $(b)\subseteq(a)$, $a\sim b$ 当且仅当 $(b)=(a)$.

(2) $u\sim 1$ 是所有 $r\in R$ 的因子. 如果 r 不是单位, 则 u 是 r 的真因子.

(3) 如果 $a=bu$, 则 $a\sim b$. 如果 R 为整环, 则反之亦然.

(4) 若 R 为整环, a 为 b 的真因子, 则 $(b)\subsetneq(a)$. 反之亦然.

证明. (1)-(2) 由定义立知.

(3) 如果 $a=bu$, 则 $b=au^{-1}$, 所以 $a\mid b$ 且 $b\mid a, a\sim b$. 若 R 为整环, $a\sim b$, 则 $a=bx, b=ay$, 所以 $axy=a$. 若 $a=0$, 则 $b=0, a=b\cdot 1$. 如果 $a\neq 0$, 则 $xy=1, x\in U(R)$.

(4) 如果 $b=ax, x$ 不为单位, 则 $a\notin(b)$. 否则 $a=by$, 故 $xy=1$ (由于 $a\neq 0$, 否则 $a=b=0$), x 为单位.

反之, 若 $(b)\subsetneq(a)$, 令 $b=ax$, 则 x 不为单位, 否则 $a\sim b, (b)=(a)$. 由于 $u\in U(R)$ 是所有元素的因子, 我们称其为**平凡因子** (trivial divisor). □

定义4.3. (1) 设 $p\notin U(R), p\neq 0$, 如果 $p\mid ab$, 则 $p\mid a$ 或 $p\mid b$, 则称 p 为**素元** (prime element).

(2) 设 $a\notin U(R), a\neq 0$, 如果 a 没有非平凡真因子, 则称 a 为**极大元** (maximal element).

例4.4. *在环 $\mathbb{Z}$ 中, 素元 = 极大元 = $\{\pm p \mid p$ 为素数$\}$.*

命题4.5. *设 R 为整环, 则*

(1) *p 为素元当且仅当 (p) 为素理想.*

(2) *a 为不可约元当且仅当理想 (a) 为 R 中主理想集合中的极大元.*

(3) *素元必是不可约元.*

(4) *如果 R 为 PID, 则不可约元也是素元.*

证明. (1) 若 p 为素元, 若 $ab \subseteq (p)$, 则 $ab = px, p \mid ab$, 故 $p \mid a$ 或 $p \mid b$, 所以 $(a) \subseteq (p)$ 或 $(b) \subseteq (p)$, 故 (p) 为素理想. 反之, 若 (p) 为素理想, 若 $p \mid ab$, 则 $(ab) \subseteq (p)$, 故 $(a) \subseteq (p)$ 或 $(b) \subseteq (p)$, 故 $p \mid a$ 或 $p \mid b$, 即 p 为素元.

(2) 设 a 为不可约元. 若 $(a) \subsetneqq (b)$, 则 b 为 s 的真因子, 但 a 没有非平凡真因子, 故 $b \in U(R)$, (a) 为极大元.

反之, 若 (a) 为极大元. 如果 s 为不可约元, 若存在 $a = bx$, b 为 a 的真因子, 则 $(a) \subsetneqq (b)$. 故 $(b) = R$, $b \in U(R)$ 为平凡真因子.

(3) 由(2), 只需证 (p) 为极大元. 若 $(p) \subsetneqq (b)$, 则 $p = bx$, 故 $p \mid b$ 或 $p \mid a$. 若 $p \mid b$, 则 $(b) \subsetneqq (p)$, 则 $(b) = (p)$ 不可能. 故 $x = py$, $p = pby$. 由 r 为整环, 故 $by = 1$, b 为单位, 因此 (p) 为极大元.

(4) 如果 R 为 PID, 则 R 中所有理想均是主理想, 即说明极大元 a 生成的理想 (a) 为极大理想, 故 (a) 为素理想. 由(1)知 (a) 为素元. □

§4.1.2 唯一因式分解环

定义4.6. 设 R 为整环, 且满足如下两条件

(1) (因式分解存在) 对任意 $a \in R, a$ 不是单位, 则 $a = c_1 c_2 \cdots c_n$, 其中 c_i 为不可约元.

(2) (因式分解唯一) 如果 $a = c_1 c_2 \cdots c_n = d_1 d_2 \cdots d_m$, 其中 c_i, d_j 为不可约元, 则 $m = n$, 且经过恰当排序后 $c_i \sim d_i$, 即 $(c_i) = (d_i)$.

则称 R 为**唯一因式分解环**(uniquely factorization domain, 简称 UFD).

我们首先给出两个不是 UFD 的整环的例子.

例4.7. 令 F 为域, $R = F[x_1, x_2, \ldots]$, 其中 $x_{n+1}^2 = x_n$, 则

$$x_1 = x_2^2 = x_3^4 = \cdots .$$

因式分解不存在.

例4.8. 设 $R = \mathbb{Z}[\sqrt{-5}]$, 则 $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. 我们来说明 2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$ 均是 R 中的不可约元.

设 $N : R \to \mathbb{N}$, $N(a+b\sqrt{-5}) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2$, 则

(i) $N(x) = 0$ 当且仅当 $x = 0$. $N(1) = 1$.

(ii) $N(xy) = N(x)N(y)$.

(iii) $N(x) = 1$ 当且仅当 $x \in U(R)$. 的确, 如果 $xy = 1$, 则 $N(xy) = 1$, 故 $N(x) = 1$. 反之, 若 $N(x) = 1$, 则$x = a+b\sqrt{-5}$ 的逆为$a - b\sqrt{-5} \in R$.

注意到 $N(2) = 4$, 如果 $2 = xy$, 则 $N(x)N(y) = 4$. 如果 x, y 均不是单位, 则必有 $N(x) = N(y) = 2$, 即 $x = a+b\sqrt{-5}$ 满足 $a^2+5b^2 = 2$. 但此方程没有整数解, 故 2 是不可约元. 同理可得 $3, 1+\sqrt{-5}, 1-\sqrt{-5}$ 是不可约元.

由此即知 R 不是 *UFD*.

由于 $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$, 但 2 不整除 $1 \pm \sqrt{-5}$, 故 2 不是素元. 我们也得到了不可约元不是素元的例子.

定义4.9. 设 R 为交换环, $a, b \in R$. 如果存在 $d \in R$ 满足

(1) d 是 a 与 b 的公因子, 即 $d \mid a$ 且 $d \mid b$.

(2) 如果 d' 是 a 与 b 的公因子, 则 $d' \mid d$.

则称 d 是 a, b 的**最大公因子** (greatest common divisor), 记为 (a, b).

注意到如果 a, b 的最大公因子 d 存在, 则 ud 也是 a, b 的最大公因子, 即 d 不是唯一决定的, 但理想 (d) 是唯一确定, 即相伴意义下 d 唯一.

引理4.10. 设在整环 R 中最大公因子存在. 设 $a, b, c \in R$.

(1) $c(a, b) \sim (ca, cb)$.

(2) 如果 $(a, b) \sim 1, (a, c) \sim 1$, 则 $(a, bc) \sim 1$.

证明. (1) 令 $(a,b)\sim d$, 则 $cd\mid ca, cd\mid cb$, 故 $cd\mid (ca,cb)$. 反过来, 由于 $c\mid ca, c\mid cb$, 故 $c\mid (ca,cb)$.令 $(ca,cb)\sim cd'$, 故由 $cd'\mid ca$, 我们有 $d'\mid a$, 同理有 $d'\mid b$, 故 $d'\mid d$, 故 $cd'\mid cd$. 所以 $c(a,b)\sim (ca,cb)$.

(2) 由 $(a,b)\sim 1$, 故 $(ac,bc)\sim c$. 又 $(a,ac)\sim a$, 故

$$(a,bc)\sim ((a,ac),bc)\sim (a,(ac,bc))\sim (a,c)\sim 1.$$

引理证毕. □

定理4.11. *设 R 为 UFD, 则 R 满足性质*

(1) (*诺特性质*) *R 上的主理想列 $(a_1)\subseteq (a_2)\subseteq\cdots\subseteq (a_n)\subseteq\cdots$ 必稳定, 即存在 $N,(a_N)=(a_{N+1})=\cdots=(a_n)$, 对所有 $n\geqslant N$ 成立.*

(2) *R 上的不可约元均是素元.*

(3) *对于 R 上任何非零元 a, b, 存在最大公因子.*

证明. (1) 注意到若 $(a)\subsetneqq (b)$, 如将 a 写成 r 个不可约因子之积, 则 b 要么是单位, 要么 b 写成不可约因子之积时, 不可约因子个数小于 r. 由此可知, 若 a_1 是 r 个不可约因子之积, 则以 (a_1) 开始的主理想列最多有 r 个 i 满足 $(a_i)\subsetneqq (a_{i+1})$, 即主理想列必然稳定.

(2) 设 p 是 R 中的不可约元且 $p\mid ab$, 记 $ab=px$, 记

$$a=c_1\cdots c_m,\quad b=d_1\cdots d_n,$$

其中 c_i,d_j 为不可约元, 则由因式分解的唯一性, $p\sim c_i$ 或 d_j 对某个 i,j 成立, 故 $p\mid a$ 或 $p\mid b$, 因此 p 是素元.

(3) 若 a 或 b 为单位, 则显然 $(a,b)\sim 1$. 否则将 a 和 b 做因子分解

$$a=up_1^{e_1}\cdots p_r^{e_r},\quad b=vp_1^{f_1}\cdots p_r^{f_r},$$

其中 $u,v\in U(R), e_i,f_j\geqslant 0, p_1,\cdots,p_r$ 是 R 中彼此不相伴的不可约元. 令 $g_i=\min\{e_i,f_i\}$. 令 $d=p_1^{g_1}\cdots p_r^{g_r}$. 我们证明 d 是 a 和 b 的一个最大公因子.

首先, 不难看出 d 是 a 与 b 的公因子. 若 d' 是 a 与 b 的公因子. 若不可约元 $p\mid d'$, 则 p 必与某个 p_i 相伴, 故 d' 可以写为 $d=wp_1^{t_1}\cdots p_r^{t_r}$. 记 $a=d'x$, 即

$$wp_1^{t_1}\cdots p_r^{t_r}\cdot x=up_1^{e_1}\cdots p_r^{e_r}.$$

由分解唯一性 $t_i \leqslant e_i$. 同理 $t_i \leqslant f_i$, 故 $t_i \leqslant g_i$, 所以 $d' \mid d$, 即 d 为 a 与 b 的最大公因子. □

定理4.12. *若 R 为整环, 则下列条件等价*

(1) *R 为 UFD.*

(2) *定理 4.11 中 (1) 和 (3)成立.*

(3) *定理 4.11 中 (1) 和 (2)成立.*

证明. (1) $\Longrightarrow$ (2). 由上述定理已证.

(2) $\Longrightarrow$ (3). 设 p 为不可约元. 如果 $p \nmid a$, 则 $(p, a) \sim 1$. 同理如果 $p \nmid b$, 则 $(p, b) \sim 1$. 故 $(p, ab) \sim 1$, 所以 $p \nmid ab$, 即 p 为素元.

(3) $\Longrightarrow$ (1). 首先证明断言: R 中每个元素 $a \notin U(R)$ 均可分解为有限多个不可约元之积. 如果 a 不可约, 断言自然成立, 否则 $a = a_1 b_1$, a_1, b_1 为 a 的非平凡真因子. 如果 a_1, b_1 均不可约, 则断言成立. 否则 a_1 或 b_1 有非平凡真因子 a_2, 我们可以得到主理想列

$$(a) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq \cdots .$$

由诺特性质, 这个过程不能无限继续. 故 a 可以分解成有限个不可约元之积.

现在若 $a = p_1 \cdots p_s = q_1 \cdots q_t$. 由 p_1 是素元, $p_1 \mid a$, 则 p_1 整除某个 q_i. 不妨设 $q_1 = p_1 x$, 由 q_1 不可约, 则 x 必是单位, 故 $p_1 \sim q_1$, 不妨设 $p_1 = q_1$, 所以 $p_2 \cdots p_s = q_2 \cdots q_t$. 由此归纳可得分解的唯一性. □

定理4.13. *每个 PID 都是 UFD.*

证明. 我们只需证明诺特性质, 即若

$$(a_0) \subseteq (a_1) \subseteq \cdots \subseteq (a_n) \subseteq \cdots ,$$

则存在 N, 使得 $(a_n) = (a_N)$ 对所有 $n \geqslant N$ 成立.

令 $I = \bigcup\limits_{n \in \mathbb{N}} (a_n)$, 则 I 是 R 中的理想. 令 $I = (a)$, 故 $(a) = \bigcup\limits_{n \in \mathbb{N}} (a_n)$. 设 $a \in (a_N)$, 则 $(a) \subseteq (a_N)$. 但显然 $(a_N) \subseteq (a)$, 故

$$(a_N) = (a) = (a_{N+1}) = \cdots = (a_n).$$

定理证毕. □

注记. 设 R 为 UFD. 若 $(a,b)\sim 1$, 则并不一定存在 u,v 使得 $ua+vb=1$. 例如 $\mathbb{Z}[x]$ 是 UFD. 但 2 与 x 的最大公因子是 1, 但并不存在 $u,v\in\mathbb{Z}[x], 2u+xv=1$.

更进一步地, 如果 R 是 UFD, 且满足条件: 对任意 $a,b\in R$, 存在 $u,v\in R$, 使得 $ua+vb=d=(a,b)$, 即 $(d)=(a,b)$. 则 R 中所有有限生成的理想都是主理想. 我们称 R 为 **Bezout 环** (Bezout ring).

§4.1.3 欧几里得环

设 $R=\mathbb{Z}$ 或 $F[x]$, 其中 F 为域, 则 R 为主理想整环. 回顾一下在证明 R 为PID 时, 我们对 R 中的元素赋予了大小: 在 $R=\mathbb{Z}$ 时是绝对值, 在 $R=F[x]$ 时是多项式的次数. 我们接着证明对任意 $f,g\neq 0$, 存在带余除法 $f=gq+r$, 使得 $r=0$ 或者 r 严格比 g 小. 由此我们证明了 R 为 PID.

将这个概念推广, 我们就得到如下定义.

定义4.14. 设 R 为整环. 如果存在函数

$$\varphi: R-\{0\}\to\mathbb{N}_+,$$

对任意 $a,b\in R$ 且 $a\neq 0$, 存在$q,r\in R$ 使得 $b=aq+r$ 且或者 $r=0$ 或者 $\varphi(r)<\varphi(a)$, 则称 R 为**欧几里得整环** (Euclidean domain, 简称 ED).

欧几里得*(Euclid,* 公元前*300*年左右*)* 编写的《几何原本》是科学史上最重要的著作之一, 直到*100*年前还是学习几何学的标准教材, 它是基于严格逻辑推理思想构建起来的西方科学体系的源泉. 中国科学之所以没有发展出来一套严格逻辑体系, 很大程度上与中国古代缺乏这种逻辑思维训练有密切关系. 《几何原本》不仅仅建构了欧几里得几何学, 欧几里得还在其中给出了最古老且至今十分有效的算法: 最大公因式的欧几里得算法, 证明了素数的无限性和欧几里得引理, 从而在本质上给出了算术基本定理和整数环是欧几里得环的证明. 早在*1607*年, 《几何原本》就由徐光启和利玛窦翻译成中文, 康熙皇帝还曾经仔细学习过《几何原本》, 但清朝上位者显然并未想到用之来开启民智. 图 *4.1* 是牛津大学自然史博物馆中陈列的欧几里得雕像, 图 *4.2* 是徐光启和利玛窦*1607*年翻译出版的第一个中文译本《几何原本》首页.

图 4.1: 欧几里得雕像

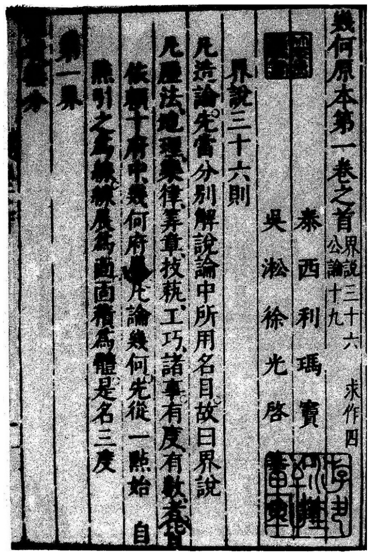


图 4.2: 徐光启, 利玛窦译《几何原本》首页

命题4.15. *ED 都是 PID, 故为 UFD.*

证明. 设 $I \neq 0$ 是欧几里得整环 R 的理想. 设 $a \neq 0, a \in I$ 且 $\varphi(a)$ 最小. 我们证明 $I = (a)$. 实际上, 如果 $b \in I$, 则 $b = aq + r, \varphi(r) < \varphi(a)$ 或 $r = 0$. 由于 $r = b - aq \in I$, 由 a 的最小性, $r = 0, b = aq \in (a)$, 故 $I = (a)$. □

例4.16. $\mathbb{Z}[\sqrt{-1}]$ 是欧几里得整环.

事实上, 令

$$\varphi : \mathbb{Z}[\sqrt{-1}] \longrightarrow \mathbb{N}$$
$$a + b\sqrt{-1} \longmapsto a^2 + b^2 = (a + b\sqrt{-1})(a - b\sqrt{-1}).$$

若 $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$, 令 $\frac{\alpha}{\beta} = x + y\sqrt{-1} \in \mathbb{Q}[\sqrt{-1}]$. 令 $x_0, y_0 \in \mathbb{Z}$, 使得 $|x - x_0| \leqslant \frac{1}{2}, |y - y_0| \leqslant \frac{1}{2}$, 则

$$\alpha = (x_0 + y_0\sqrt{-1})\beta + ((x - x_0) + (y - y_0)\sqrt{-1})\beta = q\beta + r.$$

$$\varphi(\gamma) = \varphi(\beta)((x - x_0)^2 + (y - y_0)^2) \leqslant \frac{1}{2}\varphi(\beta) < \varphi(\beta).$$

故 $\mathbb{Z}[\sqrt{-1}]$ 是 ED.

习 题

习题1.1. 设 R 为 *UFD* , a,b,c 为 R 中非零元素. 证明*:*

(1) $ab \sim (a,b)[a,b]$*;*

(2) 若 $a \mid bc$, $(a,b)=1$, 则 $a \mid c$.

习题1.2. 设 R 为 *PID*. 证明*:*

(1) $(a)\cap(b)=([a,b])$, 并且 $(a)\cap(b)=(a)(b)$ 当且仅当 $(a,b)=1$*;*

(2) 方程 $ax+by=c$ 在 R 中有解 (x,y) 的充要条件是 $(a,b)\mid c$.

习题1.3. 设 D 是整环但不是域, 则 $D[x]$ 不是 *PID*.

习题1.4. 设 R为整环, $a,b\in R-0$, $a\sim b$. 求证*:*

(1) 若 a 为不可约元, 则 b 也为不可约元*;*

(2) 若 a 为素元, 则 b 也为素元.

习题1.5. 设 a 为主理想整环 D 中非零元. 求证*:* 若 a 为素元,则 $D/(a)$ 为域*;* 若 a 不是素元, 则 $D/(a)$ 不是整环.

习题1.6. 下列哪些环是 *PID?* 哪些环是 *ED?*

(1) $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{-3}]$.

(2) $\mathbb{R}[x,y]$.

(3) $\mathbb{Z}[\omega]$, 其中 $\omega=\frac{-1+\sqrt{-3}}{2}$.

习题1.7. 设 D 是 *PID*, E 是整环, 并且 D 是 E 的子环, $a,b\in D-\{0\}$. 如果 d 是 a 和 b 在 D 中的最大公因子, 证明 d 也是 a 和 b 在 E 中的最大公因子.

§4.2 高斯整数与二平方和问题

定义4.17. 整环 $\mathbb{Z}[\sqrt{-1}]$ 称为**高斯整数环** (domain of Gauss integers), 其中元素称为**高斯整数** (Gauss integer), 其素元称为**高斯素数** (Gauss prime).

由上节可知高斯整数环 $\mathbb{Z}[\sqrt{-1}]$ 是 ED, 故为 PID. 在本节中, 我们记

$$\begin{aligned}\varphi:\mathbb{Z}[\sqrt{-1}] &\longrightarrow \mathbb{N}\\ a+b\sqrt{-1} &\longmapsto a^2+b^2.\end{aligned}$$

引理4.18. 高斯整数环的单位群 $U(\mathbb{Z}[\sqrt{-1}]) = \{\pm 1, \pm\sqrt{-1}\}$.

证明. 元素 $x \in U(\mathbb{Z}[\sqrt{-1}])$ 当且仅当 $\varphi(x) = 1$, 故 $x = a + b\sqrt{-1}$ 为单位当且仅当 $a^2 + b^2 = 1$, 即 $a = \pm 1$, $b = 0$ 或 $a = 0$, $b = \pm 1$. □

定理4.19. (1) 设 p 为素数, 则 p 或为高斯素数或为两个共轭的高斯素数之积, 即 $p = \pi\bar{\pi}$.

(2) 设 π 为高斯素数, 则 $\pi\bar{\pi}$ 或为素数, 或为素数的平方.

(3) 素数 p 为高斯素数当且仅当 $p \equiv 3 \bmod 4$.

(4) 设 p 为素数, 则下列条件等价:

(i) p 为两个共轭的高斯素数之积.

(ii) $p = a^2 + b^2, a, b \in \mathbb{Z}$.

(iii) $x^2 \equiv -1 \bmod p$ 有整数解, 即 $(\frac{-1}{p}) = 1$.

(iv) $p \equiv 1 \bmod 4$ 或 $p = 2$.

证明. (1) 若 $p = \pi_1 \cdots \pi_n$ 为高斯素数之积, 则 $p^2 = \varphi(p) = \varphi(\pi) \cdots \varphi(\pi_n)$. 由于 $\varphi(\pi_i) > 1$, 故 $\varphi(\pi_i) = p$ 或 p^2. 我们有 $n = 1$ 或 2. 若 $n = 1$, p 是高斯素数. 若 $n = 2$, 则 $\varphi(\pi_1) = \varphi(\pi_2) = p$, 故 $p = \varphi(\pi_1) = \pi_1\bar{\pi}_1$.

(2) 设 $p \mid \varphi(\pi) = \pi\bar{\pi}$. 若 p 是高斯素数, 则 $p \mid \pi$ 或 $p \mid \bar{\pi}$, 但在后一种情况 $\bar{p} = p \mid \pi$, 故 $p^2 \mid \pi\bar{\pi}$. 但 p^2 是两个素元之积, $\pi\bar{\pi}$ 亦然. 由因式分解唯一性, $p^2 = \pi\bar{\pi} \cdot \varepsilon, \varepsilon$ 为单位. 但 $p^2 > 0, \pi\bar{\pi} > 0$, 故 $\varepsilon = 1$, $p^2 = \pi\bar{\pi} = \varphi(\pi)$.

若 p 不是高斯素数. 由(1), $p = \pi_1\bar{\pi}_1 \mid \pi\bar{\pi}$, 同样由分解唯一性, $\pi_1\bar{\pi}_1 = \pi\bar{\pi} = p$.

(3) 我们只要证如果 $p \equiv 3 \bmod 4$, 则 p 是高斯素数, 另一方面的证明由(4)即知. 如果 p 不是高斯素数, 则

$$p = \pi\bar{\pi} = \varphi(\pi) = a^2 + b^2, \quad \pi = a + b\sqrt{-1},$$

则 $p \equiv 0, 1, 2 \bmod 4$, 即 $p \not\equiv 3 \bmod 4$.

(4) (i) $\Longleftrightarrow$ (ii). 显然.

(ii) $\Longrightarrow$ (iii). 如果 $p = a^2 + b^2$, 则 $0 < b^2 < p$. 取 $\bar{c} = \bar{b}^{-1} \in \mathbb{F}_p$, 则 $a^2c^2 \equiv -1 \bmod p$.

(iii) $\Longleftrightarrow$ (iv). 如果 p 为奇素数, 则 $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, $(\frac{-1}{2}) = 1$, 故 $(\frac{-1}{p}) = 1$ 等价于 $p \equiv 1 \bmod 4$ 或 $p = 2$.

(iii) $\Longrightarrow$ (i). 由 $p \mid x^2+1=(x+\sqrt{-1})(x-\sqrt{-1})$, 但是 $p \nmid x+\sqrt{-1}$, $p \nmid x-\sqrt{-1}$, 我们知 p 不是素元. 由(1), p 必是共轭高斯素数之积. □

定理4.20. 设 $n \geqslant 2$ 的素分解是 $2^{\alpha}p_1^{\beta_1}\cdots p_s^{\beta_s}q_1^{\gamma_1}\cdots q_t^{\gamma_t}$, 其中 $p_1,\ldots,p_s \equiv 1 \bmod 4, q_1,\ldots,q_t \equiv 3 \bmod 4$. 则 n 是两个整数的平方和当且仅当 $\gamma_1,\ldots,\gamma_t$ 全为偶数, 此时共有 $4(\beta_1+1)\cdots(\beta_s+1)$ 对整数 (x,y) 满足 $n=x^2+y^2$.

证明. $n=x^2+y^2$ 当且仅当 $n=a\bar{a}$, 其中 $a=x+iy \in \mathbb{Z}[\sqrt{-1}]$. 将 n 写成高斯素元之积, 我们有

$$n=\varepsilon(1+i)^{2\alpha}\pi_1^{\beta_1}\bar{\pi}_1^{\beta_1}\cdots\pi_s^{\beta_s}\bar{\pi}_s^{\beta_s}\cdot q_1^{\gamma_1}\cdots q_t^{\gamma_t},$$

其中 ε 为单位. 将 a 写成高斯素数之积, 则有

$$a=\varepsilon_1(1+i)^{\alpha'}\pi_1^{\beta_{11}}\bar{\pi}_1^{\beta_{12}}\cdots\pi_s^{\beta_{s1}}\bar{\pi}_s^{\beta_{s2}}\cdot q_1^{\gamma_1'}\cdots q_t^{\gamma_t'},$$

$$\bar{a}=\bar{\varepsilon}_1(1-i)^{\alpha'}\pi_1^{\beta_{12}}\bar{\pi}_1^{\beta_{11}}\cdots\pi_s^{\beta_{s2}}\bar{\pi}_s^{\beta_{s1}}\cdot q_1^{\gamma_1'}\cdots q_t^{\gamma_t'},$$

其中 ε_1 为单位. 由因式分解的唯一性, $n=a\bar{a}$ 当且仅当

$$2\alpha'=2\alpha,\quad \beta_{11}+\beta_{12}=\beta_1,\quad \cdots,\quad \beta_{s1}+\beta_{s2}=\beta_s,$$

$$2\gamma_1'=\gamma_1,\quad \cdots,\quad 2\gamma_t'=\gamma_t,$$

即 $\gamma_1,\cdots,\gamma_t$ 为偶数. 此时 β_{11}(及β_{21})有 β_1+1 种可能选择, ..., β_{s1}(及β_{s2})有 β_s+1 种可能选择, ε_1 有 4 种选择, 即解的个数为 $4(\beta_1+1)\cdots(\beta_s+1)$. □

习 题

习题2.1. 设 p 是奇素数, $p \equiv 1 \pmod 4$. 如果 (a,b) 是不定方程 $x^2+y^2=p$ 的一组整数解, 则它的全部整数解为 $(x,y)=(\pm a,\pm b),\ (\pm b,\pm a)$.

习题2.2. 将 60 和 $81+8\sqrt{-1}$ 在环 $\mathbb{Z}[\sqrt{-1}]$ 中分解成不可约元之积.

习题2.3. 试求方程 $x^2+y^2=585$ 的所有整数解.

习题2.4. 利用正文的方法研究如下问题:

(1) 对于正整数 n, $x^2+2y^2=n$ 何时有整数解? 有多少组整数解?

(2) 对于正整数 n, $x^2+xy+y^2=n$ 何时有整数解? 有多少组整数解?

§4.3 多项式环与 Gauss 引理

§4.3.1 环上的多项式环

我们假设 R 为交换环, $R[x]$ 为其多项式环. 设多项式 $f(x) \in R[x]$. 若 $f \neq 0$, 记 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ ($a_n \neq 0$), 我们称 f 的**次数** (degree)为 n, 并记为 $\deg f$, 称 a_n 为 $f(x)$ 的**首项系数** (leading coefficient). 若 f 的首项系数为 1, 称 f 为**首一多项式**. 若 $f = 0$ 为零多项式, 记 $\deg f = -\infty$.

环 R 中元素 a 在 $R[x]$ 中的像称为**常值多项式**. 注意到 $f(x)$ 为常值多项式当且仅当 $\deg f \leq 0$.

命题4.21. *设 $f(x), g(x) \in R[x]$, 则*

(1) $\deg(f+g) \leqslant \max\{\deg f, \deg g\}$.

(2) $\deg(fg) \leqslant \deg f + \deg g$, *且如果 $f(x)$ 或 $g(x)$ 的首项系数不为零因子, 则等号成立. 特别地, 若 R 为整环, 则等式恒成立.*

证明. 显然. 留作练习. □

命题4.22. *若 D 为整环, 则 $D[x]$ 也是整环, 且 $U(D[x]) = U(D)$, 即二者的单位群相同.*

证明. 若 $f(x), g(x) \in D[x]$ 且均不为 0, 则 $f(x) \cdot g(x)$ 的首项系数即 $f(x)$ 与 $g(x)$ 的首项系数之积, 也不为0, 所以 $f(x)g(x) \neq 0$. 若 $f(x) \in U(D[x])$. 令 $f(x)g(x) = 1$, 则 $\deg f = \deg g = 0$, 即 $f(x) = a_0$, $g(x) = b_0$ 为非零常值函数, 且 $a_0 b_0 = 1$, 故 $U(D[x]) \subseteq U(D)$. 另一方面, $U(D) \subseteq U(D[x])$ 显然. □

我们知道如果 F 为域, 则对于多项式 $f(x), g(x) \in F[x]$ 且$g(x) \neq 0$, 存在唯一的多项式 $q(x), r(x) \in F[x]$, 使得 $\deg r < \deg g$, 且

$$f = qg + r,$$

即带余除法成立. 由带余除法我们可以推得 $F[x]$ 是欧几里得整环, 故也是 PID 和 UFD. 对于环的多项式情形, 我们有如下命题, 其证明与域上的情形一致.

命题4.23. *若 $f(x), g(x) \in R[x]$, 且 $g(x)$ 的首项系数在 R 的单位群中, 则存在唯一的多项式 $q(x), r(x)$ 满足条件*

$$f(x) = q(x)g(x) + r(x), \quad \deg r(x) < \deg g(x). \tag{4.1}$$

推论4.24 (余数定理)**.** *设 $f(x) \in R[x]$, $c \in R$, 则存在唯一的多项式 $q(x)$, 使得*

$$f(x) = q(x)(x - c) + f(c). \tag{4.2}$$

故 c 为 $f(x)$ 的根当且仅当 $(x - c) \mid f(x)$.

证明. 此时 $g(x) = x - c$, 故 $\deg r(x) < 1$, $r(x)$ 只能为常值多项式, 故 $r(x) = r(c) = f(c) - q(c)(c - c) = f(c)$. □

推论4.25 (拉格朗日)**.** *设 D, E 为整环, 且 $D \subseteq E$. 则 $D[x]$ 上的非零多项式 $f(x)$ 在 E 中至多有 $\deg f$ 个不同根.*

证明. 若 $c_1, \ldots, c_r$ 为 $f(x)$ 在 E 上的根, 则 $f(x) = (x - c_1)q_1(x)$. 由 $(c_2 - c_1)q_1(c_2) = f(c_2) = 0$ 知 $q_1(c_2) = 0$, 故 $q_1(x) = (x - c_2)q_2(x)$. 由此递推知

$$f(x) = (x - c_1)(x - c_2) \cdots (x - c_r)q_r(x).$$

由于 $\deg q_r \geqslant 0$, $\deg f(x) = r + \deg q_r(x)$, 所以 $r \leqslant \deg f$. □

注记. E 的交换性条件必不可少. 例如在四元数体 $\mathbb{H}$ 中, $x^2 + 1$ 有无数多个根 $ai + bj + ck$ $(a^2 + b^2 + c^2 = 1)$.

命题4.26. *设 D 为 UFD, F 为其商域, $f(x) = \sum_{i=0}^{n} a_i x^i$ $(a_n \neq 0)$ 为 D 上的非零多项式. 若 $u = \frac{c}{d} \in F$(其中$c, d \in D$ 且$(c, d) = 1$) 为 $f(x)$ 的根, 则 $c \mid a_0$ 且 $d \mid a_n$.*

证明. 由 $f(u) = 0$ 知

$$\sum_{i=0}^{n} a_i c^i d^{n-i} = 0.$$

所以 $c \mid a_0 d^n$ 且 $d \mid a_n c^n$. 但由 $(c, d) = 1$ 知 $c \mid a_0$ 且 $d \mid a_n$. □

设 D, E 为整环, $D \subseteq E$. 设 $f(x) = a_n x^n + \cdots + a_0 \in D[x]$. 我们记

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1, \tag{4.3}$$

称为 $f(x)$ 的**形式微商** (formal derivative). 对于 $c \in E$, c 称为 $f(x)$ 的n**重根** (root of multiplicity n), 是指

$$f(x) = (x-c)^n g(x) \quad \text{且} \, g(c) \neq 0. \tag{4.4}$$

定理4.27. *设 D, E 为整环, $D \subseteq E$. 设 $f(x) \in D[x]$, $c \in E$.*

(1) 若 c 为 $f(x)$ 的 n 重根, 则 $f(c) = \cdots = f^{(n-1)}(c) = 0$, 且 $f^{(n)}(c) \neq 0$. 若 D 为特征零的整环, 则反之也成立.

(2) 如果 D 为域, 且 $(f, f') = 1$, 则 $f(x)$ 在 E 上无重根.

证明. (1) 由形式微商的定义, 我们知

(a) 若 $f(x) \in D[x] \subseteq E[x]$, $f(x)$ 作为 E 上多项式的形式微商等于 $f(x)$ 作为 D 上多项式的形式微商.

(b) $(f+g)' = f' + g'$, $(fg)' = f'g + fg'$.

若 c 为 $f(x)$ 的 n 重根, 则 $f(x) = (x-c)^n g(x)$, 故

$$\begin{aligned} f'(x) &= n(x-c)^{n-1}g(x) + (x-c)^n g'(x) \\ &= (x-c)^{n-1}(ng(x) + (x-c)g'(x)), \end{aligned}$$

可知 c 是 $f'(x)$ 的 $n-1$ 重根. 由归纳假设知

$$f(c) = \cdots = f^{(n-1)}(c) = 0, \quad f^{(n)}(c) \neq 0.$$

反之, 若 $f(c) = \cdots = f^{(n-1)}(c) = 0$, $f^{(n)}(c) \neq 0$, 将 $f(x)$ 写成 $x - c$ 的多项式

$$f(x) = b_0 + b_1(x-c) + b_2(x-c)^2 + \cdots + b_m(x-c)^m,$$

则

$$f(c) = b_0, f'(c) = b_1, \ldots, \frac{f^{(m)}(c)}{m!} = b_m,$$

所以 $b_0 = \cdots = b_{n-1} = 0$, $b_n \neq 0$,

$$f(x) = (x-c)^n(b_n + b_{n+1}(x-c) + \cdots + b_m(x-c)^{m-n}) = (x-c)^n g(x)$$

且 $g(c) = b_n \neq 0$.

(2) 由(1)立得. □

§4.3.2 Gauss 引理

设 D 为 UFD, $f(x)=\sum\limits_{i=0}^{n}a_ix^i$ $(a_n\neq 0)$ 是 D 上非零多项式.

定义4.28. 系数 $a_0,a_1,\ldots,a_n$ 的最大公因子称为 f 的**容积** (content), 记为 $c(f)$. 若 $c(f)\sim 1$, 称 f 为**本原多项式** (primitive polynomial).

由定义可知

$$f=c(f)\cdot f_1,\quad \text{其中 } f_1 \text{ 为本原多项式.} \tag{4.5}$$

且在相伴意义下, 上式唯一, 即如 $f=c\cdot g$ 且 g 为本原多项式, 则 $c\sim c(f)$.

命题4.29 (Gauss 引理)**.** *设 D 为 UFD. 设 $f(x),g(x)\in D[x]$ 且非零, 则*

$$c(fg)=c(f)\cdot c(g). \tag{4.6}$$

特别地, 本原多项式的乘积为本原多项式.

证明. 由 $fg=c(f)c(g)f_1g_1$ 知 $c(fg)=c(f)c(g)c(f_1g_1)$, 我们只需证明 $c(f_1g_1)=1$, 即本原多项式的乘积为本原多项式. 设

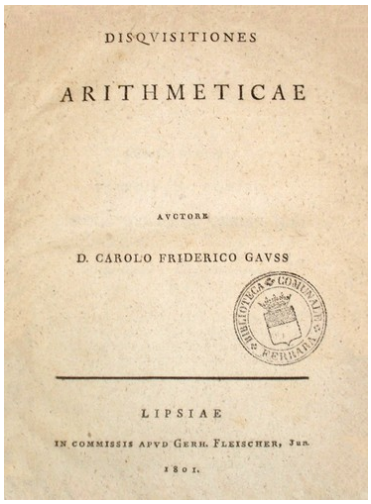
$$f_1=\sum_{i=1}^{n}a_ix^i,\quad g_1=\sum_{i=1}^{m}b_jx^j,$$

则 $f_1g_1=\sum\limits_{k}c_kx^k$, 其中 $c_k=\sum\limits_{i+j=k}a_ib_j$. 对于 D 上素元 p, 由 $p\nmid c(f_1)$, 故存在 s, 使得 $p\mid a_i$ 对 $i<s$ 成立但 $p\nmid a_s$. 同样存在 t, $p\mid b_j$ 对于 $j<t$ 成立但 $p\nmid b_t$. 故对于

$$c_{s+t}=a_0b_{s+t}=\cdots+a_{s-1}b_{s+1}+a_sb_t=a_{s+1}b_{t-1}+\cdots+a_{s+t}b_0,$$

由 $p\nmid a_sb_t$ 得 $p\nmid c_{s+t}$. 故 c_k 的最大公因子为 1, 即 $c(f_1g_1)=1$. □

图 4.3: 德国邮票上的高斯


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

图 4.4: 《算术研究》封面

> 卡尔·弗里德里希·高斯*(Carl Friedrich Gauss, 1777*年*4*月*30*日*–1855*年*2*月*23*日*)* 被称为*"*数学王子*"*, 被普遍认为是数学史上最伟大的数学家, 在数学的每个领域都有开创性的贡献. *1801*年出版的《算术研究》*(Disquisitiones Arithmeticae)* 是数学史上最重要的著作之一, 它标志着现代数论的开端. 我们学习过的初等数论知识和本书环的理论部分*(*唯一因式分解环, 高斯整数环*)* 的很多知识都出于该书. 高斯在不到*18*岁时证明正p边形可以通过直尺和圆规构造当且仅当p是费马素数*(*即形如$2^{2^n}+1$ 的素数*)*, 这也促使他选择数学作为研究方向. 而伽罗瓦理论给出了尺规作图问题的完美解答, 两大数学天才的思想在此交汇. 但遗憾的是, 尽管高斯是当时最伟大的科学家, 但年轻的阿贝尔和伽罗瓦的工作并没有得到他的重视. 图 *4.3* 是纪念高斯诞生*200*周年时民主德国发行的邮票. 图 *4.4* 是《算术研究》的封面.

由 Gauss 引理, 我们立刻有如下结果.

引理4.30. 设 D 为 *UFD*, F 为 D 的商域, $f,g\in D[x]$ 为本原多项式, 则 f 与 g 在 $D[x]$ 相伴当且仅当 f 与 g 在 $F[x]$ 上相伴.

证明. 若 $f=\alpha g,\alpha\in F^\times$, 令 $\alpha=\frac{a}{b}$, $a,b\in D$ 互素, 则 $bf=ag$, 故

$b = c(bf) \sim a = c(ag)$, 即 $\alpha \in D^\times$. □

引理4.31. *设 D 为 UFD, F 为 D 的商域, 则 $f(x)$ 在 $D[x]$ 中为不可约元当且仅当 $f(x)$ 满足下列两条件之一:*

(1) *$f(x) = p$ 为 D 上的不可约元.*

(2) *$f(x)$ 本原且在 $F[x]$ 中不可约.*

证明. 若 $\deg f = 0$, 则 $f(x)$ 不可约等价于 $f(x) = p$ 在 D 上不可约. 现在设 $\deg f \geqslant 1$.

若 $f(x)$ 在 $F[x]$ 中不可约且为本原多项式. 设 $f(x) = g(x)h(x) \in D[x]$, 则 $g(x)$ 或 $h(x)$ 在 $F[x]$ 中可逆, 不妨设为 $g(x)$, 则 $g(x) \in F^\times$. 又 $g(x) \in D[x]$, 故 $g(x) \in D - \{0\}$. 由 $c(f) = g \cdot c(h)$, 故 $g(x) \in U(D) = D^\times$.

反之, 若 $f(x) \in D[x]$ 不可约, 由 $f(x) = c(f) \cdot f_1(x)$ 知 $c(f) = 1$, $f(x)$ 为本原多项式. 若 $f(x) = g(x)h(x) \in F[x]$, 令

$$g(x) = \frac{a}{b}g'(x), \quad h(x) = \frac{c}{d}h'(x),$$

其中 $a, b, c, d \in D, g'(x), h'(x) \in D[x]$ 本原, 则 $bdf(x) = acg'(x)h'(x)$, 故在 D 中 $bd \sim ac$, 即 $f(x) \sim g'h'$. □

定理4.32 (Gauss)**.** *如果 D 为 UFD, 则 $D[x]$ 也是 UFD. 从而 n 元多项式环 $D[x_1, \ldots, x_n]$ 均为 UFD.*

证明. 我们先证因子分解的存在性, 后证唯一性.

存在性: 设 $f(x) \in D[x]$. 我们对 $f(x)$ 的次数作归纳证明 $f(x)$ 为 $D[x]$ 中不可约元的乘积.

若 $\deg f = 0$, 则 $f(x) \in D$. 由 D 为 UFD 知 $f(x)$ 可以写为不可约元之积. 若 $\deg f \geqslant 1$, 由 $f(x) = c(f) \cdot f_1(x)$. 我们可以假设 $f(x)$ 本原, 则当 $\deg f = 1$ 时 $f(x)$ 为不可约元, 则由引理 4.31, $f(x)$ 为 $D[x]$ 上不可约元, 否则 $f(x) = g(x)h(x)$ 在 $F[x]$ 上可约. 同样由引理 4.31, $f(x) = g'(x)h'(x)$ 在 $D[x]$ 上可约. 由 $c(f) = 1$ 可知 $g'(x), h'(x)$ 为本原多项式. 由归纳假设知 $f(x)$ 为 $D[x]$ 中不可约之积.

唯一性: 若

$$f(x) = c_1 \cdots c_r g_1(x) \cdots g_s(x) = d_1 \cdots d_{r'} g'_1(x) \cdots g'_{s'}(x)$$

为 $f(x)$ 的不可约因式分解, 其中 $c_1,\dots,c_r,d_1,\dots,d_{r'}\in D$ 不可约, $g_1(x),\dots,g_s(x)$, $g'_1(x),\dots,g'_{s'}(x)$ 为 $D[x]$ 上次数$\geqslant 1$的不可约多项式, 则由

$$c(f)=c_1\cdots c_r=d_1\cdots d_{r'}$$

知 $r=r'$ 且经调换次序后 $c_1\sim d_1$, …, $c_r\sim d_r$, 故 $g_1(x)\cdots g_s(x)\sim g'_1(x)\cdots g'_{s'}(x)$. 故由引理 4.30, 它们在 $F[x]$ 中也相伴. 由 $F[x]$ 中因式分解的唯一性知 $s=s'$, 且经调换次序后 $g_i(x)$ 与 $g'_i(x)$ 在 $F[x]$ 中相伴, 再由引理 4.30, 它们在 $D[x]$ 中也相伴. □

下面我们给出 $D[x]$ 中多项式为不可约多项式的一种判别方法.

定理4.33 (Eisenstein 判别法)**.** *设 D 为UFD, 设*

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in D[x].$$

若存在 D 上不可约元 p, 使得 $p\mid a_i$ $(0\leqslant i\leqslant n-1)$, 但 $p^2\nmid a_0$, 则 $f(x)$ 为 $D[x]$ 中不可约多项式.

证明. 若 $f(x)=g(x)h(x)$, 其中 $g(x)=\sum\limits_{i=1}^{m}b_ix^i$, $h(x)=\sum\limits_{j=0}^{l}c_jx^j$. 比较首项系数, 知 $m+l=n$ 且 $b_mc_l=1$, 即 b_m,c_l 为 D 中单位, 故不妨设 $g(x)$ 与 $h(x)$ 首一. 比较常数项系数, 我们有 $p\mid b_0c_0$ 且 $p^2\nmid b_0c_0$. 不妨设 $p\mid b_i$ 对所有 $i<k$ 成立, 则

$$a_k=b_kc_0+b_{k-1}c_1+\cdots+b_0c_k.$$

若 $m<n$, 则 $k<n$. 由定理条件, 我们有 $p\mid a_k$. 另一方面 $p\nmid b_kc_0$ 但 $p\mid b_ic_j(i<k)$, 故 $p\nmid a_k$, 得到矛盾. 故 $m=n$, 即 $f(x)$ 不可约. □

注记. 同样的证明适应于 $f(x)=a_nx^n+\cdots+a_1x+a_0$, $p\nmid a_n$, $p\mid a_i(0\leqslant i\leqslant n-1)$ 但 $p^2\nmid a_0$ 的情形.

例4.34. *设 p 为素数, $f(x)=\frac{x^p-1}{x-1}=1+x+\cdots+x^{p-1}$, 则*

$$g(x)=f(x+1)=\frac{(x+1)^p-1}{x}=x^{p-1}+\sum_{k=1}^{p-1}\binom{p}{k}x^{p-k-1}$$

满足 Eisenstein 判别法的条件, 故$g(x)$ 是不可约多项式, 从而 $f(x)$ 也是 $\mathbb{Z}[x]$ 上的不可约多项式.

令 $D=\mathbb{Z}, F=\mathbb{Q}$, 则Gauss 引理有如下实际应用

定理4.35. *整系数多项式 $f(x)$ 不可约当且仅当它作为有理系数多项式不可约, 且其系数的最大公约数为 1. 换言之, 设 $f(x)\in\mathbb{Z}[x]$, 则 $f(x)=g(x)h(x)$, 其中 $g(x),h(x)\in\mathbb{Z}[x]$ 且次数 $\geqslant 1$ 当且仅当 $f(x)=g'(x)h'(x)$, 其中 $g'(x),h'(x)\in\mathbb{Q}[x]$ 且次数 $\geqslant 1$.*

习 题

习题3.1. *证明命题 4.21.*

习题3.2. *设 R 是环, $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$. 证明:*

(1) *$f(x)$ 可逆当且仅当 $a_0\in U(R)$, 且 $a_1,\ldots,a_n\in \mathrm{Nil}(R)$.*

(2) *$f(x)$ 幂零当且仅当 $a_0,a_1,\ldots,a_n$ 均可逆.*

(3) *$f(x)$ 是零因子当且仅当存在 $0\neq a\in R$, 使得 $af(x)=0$.*

习题3.3. *设 D 为 UFD, F 为 D 的商域. $f(x)$ 为 $D[x]$ 中首一多项式. 证明: $f(x)$ 在 $F[x]$ 中的每个首一多项式因子必属于 $D[x]$.*

习题3.4. *将 x^n-1 $(3\leqslant n\leqslant 10)$ 在 $\mathbb{Z}[x]$ 中作素因子分解.*

习题3.5. *设 F 为域, $d:\ F[x]\to F[x]$ 为线性映射, 若对于任意的 $f,g\in F[x]$, $d(fg)=(df)g+f(dg)$, 则称 d 为$F[x]$ 上的一个**线性导子**. 请找出 $F[x]$ 上所有线性导子.*

习题3.6. *设 D 是整环但不是域, 求证 $D[x]$ 不是主理想整环.*

习题3.7. *设 $f(x)$ 是 $\mathbb{Q}[x]$ 中奇次不可约多项式, α 和 β 是 $f(x)$ 在 $\mathbb{Q}$ 的某个扩域中两个不同的根, 求证 $\alpha+\beta\notin\mathbb{Q}$.*

习题3.8. *设 R 是含幺环. 定义集合*

$$R[[x]]=\{\sum_{n=0}^{+\infty}a_nx^n\mid a_n\in R(n=0,1,2,\ldots)\},$$

每个元素 $\sum\limits_{n=0}^{+\infty} a_n x^n$ 叫做 R 上关于 x 的**形式幂级数**. 定义

$$\sum a_n x^n + \sum b_n x^n = \sum (a_n + b_n) x^n,$$
$$(\sum a_n x^n)(\sum b_n x^n) = \sum (\sum_{i+j=n} a_i b_j) x^n.$$

(1) $R[[x]]$ 对于上述加法和乘法形成含幺环, 叫做环 R 上关于 x 的**形式幂级数环**;

(2) 若 R 为交换环, 则 $R[[x]]$ 也是交换环;

(3) 多项式环 $R[x]$ 可自然看成是 $R[[x]]$ 的子环;

(4) 设 R 是含幺交换环, $f(x) = \sum\limits_{i=1}^{\infty} a_i x^i \in R[[x]]$, 则 $f(x)$ 可逆当且仅当 $a_0 \mathbb{R}\times$.

(5) 若 R 为域, 则 $R[[x]]$ 是 *PID* 且只有唯一的极大理想 $\mathfrak{m}$. 求出 $R[[x]]$ 的所有理想.

习题3.9. 试确定 $\mathbb{R}[x]$ 和 $\mathbb{Z}[x]$ 的所有素理想和极大理想.

习题3.10. 试确定环 $\mathbb{Z}[x]$ 和环 $\mathbb{Q}[x]$ 的自同构群.

习题3.11. 设 $c_0, \ldots, c_n$ 是整环 D 中两两相异的 $n+1$ 个元素, $d_0, \ldots, d_n$ 是 D 中任意 $n+1$ 个元素. 证明:

(1) 在 $D[x]$ 中至多存在一个次数 $\leqslant n$ 的多项式 $f(x)$, 使得 $f(c_i) = d_i$ $(0 \leqslant i \leqslant n)$;

(2) 如果D 为域, 则(1) 中所述的多项式是存在的.

习题3.12. 判断下列元素是否为 $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}[[x]]$ 中的可逆元? 是否为不可约元?

(1) $2x+2$; (2) x^2+1; (3) $x+1$; (4) x^2+3x+2.

习题3.13. 设 $f = \sum u_i x^i \in \mathbb{Z}[x]$ 为首 1 多项式, p 为素数, 以 $\overline{a}$ 表示 $a \in \mathbb{Z}$ 在环的自然同态$\mathbb{Z} \to \mathbb{F}_p$ 之下的像, 而令 $\overline{f}(x) = \sum \overline{a}_i x^i \in Z_p[x]$.

(1) 求证: 若对某个素数p, $\overline{f}(x)$ 在$\mathbb{F}_p[x]$ 中不可约, 则 $f(x)$ 在$\mathbb{Z}[x]$ 中不可约.

(2) 若 $f(x)$ 不是 $\mathbb{Z}[x]$ 中首 1 多项式, 问(1) 中结论是否成立?

习题3.14. 设 F 为域, $a, b \in F$ 且 $a \neq 0$. 证明 $f(x)$ 在 $F[x]$ 中不可约当且仅当 $f(ax+b)$ 在 $F[x]$ 中不可约.

习题3.15. 证明两个整多项式在$\mathbb{Q}[x]$ 中互素当且仅当它们在$\mathbb{Z}[x]$ 中生成的理想含有一个整数.

习题3.16. 设 $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, $\deg f = n$. 若存在素数 p 和整数 k $(0 < k < n)$, 使得:

$$p \nmid a_n, \quad p \nmid a_k, \quad p \mid a_i \ (0 \leq i \leq k-1), \quad p^2 \nmid a_0.$$

求证 $f(x)$ 在 $\mathbb{Z}[x]$ 中必存在次数 $\geq k$ 的不可约因子.

习题3.17. 设 D 是整环, $0 \neq f(x) = a_0 + a_1 x + \cdots + a_n x^n \in D[x]$. 若 $(a_0, a_1, \cdots, a_n) = 1$, 则 $f(x)$ 在 $D[x]$ 中不可约分解若存在则必唯一.

第五章　域扩张理论

§5.1　域扩张基本理论

§5.1.1　常见的域的例子

我们回顾一下域 F 是一类特别的环, 即 F 是整环且其单位群 $F^\times = F - \{0\}$, 即其非零元均可逆.

例5.1. *若域 F 的特征为0, 则同态 $\mathbb{Z} \to F, 1 \mapsto 1_F$ 可以扩充为域的单同态 $\mathbb{Q} \hookrightarrow F$, 即 $\mathbb{Q}$ 可以视为 F 的子域. 若 $F \subseteq \mathbb{C}$, 我们称 F 为* **数域** *(number field). 例如实数域 $\mathbb{R}$ 即为数域的一个例子.*

例5.2. *如果域 F 的特征为 p, 则同态 $\mathbb{Z} \to F$ 诱导域的单同态 $\mathbb{F}_p \hookrightarrow F$. 特别地, 如果 F 的元素个数有限, 称 F 为* **有限域** *(finite field).*

例5.3. *设 F 为域, x 为未定元. F 上的* **有理函数域** *(rational function field) $F(x)$ 即 F 上多项式环 $F[x]$ 的商域, 它的元素可以记为 $\frac{f(x)}{g(x)}$, 其中 $f(x), g(x) \in F[x]$ 且 $g(x) \neq 0$.*

上述三个例子在域的理论中起着重要作用, 我们将经常使用到它们.

§5.1.2　代数扩张与超越扩张

在引进概念前, 我们首先看一个例子. 令 $F = \mathbb{Q}, K = \mathbb{C}$. 对于 $\alpha \in \mathbb{C}$, 有两种情况: (i) $\alpha = e$ 或 π 及类似情形. 此时对所有非零多项式 $f(x) \in \mathbb{Q}[x]$, $f(\alpha) \neq 0$; (ii) $\alpha = \sqrt{2}$ 或 ζ_n 及类似情形. 此时存在非零多项式 $f(x) \in \mathbb{Q}[x]$, $f(\alpha) = 0$. 这两种情况说明了域扩张中两种元素: **超越元**与**代数元** (见第三章§3.1.1).

定义5.4. 如果域 F 是域 K 的子域, 称 K 是 F 的**扩张** (extension), 记为 K/F.

如果 K/F 为域扩张, $\alpha \in K$, 记 $F(\alpha)$ 为 K 中包含 F 与 α 的最小子域. 更进一步地, $S \subset K$ 生成的子域记为$F(S)$.

域的理论从本质上而言是研究域扩张的理论. 设 K/F 为域扩张, $\alpha \in K$. 考虑环同态

$$\varphi : F[x] \to K, \quad g(x) \mapsto g(\alpha).$$

由于 K 是域, 自然也是整环, 故 $\ker\varphi$ 是 $F[x]$ 上的素理想. 这有两种情形:

(i) 或者 $\ker\varphi = (0)$;

(ii) 或者 $\ker\varphi = (f(x))$, $f(x)$ 是 $F[x]$ 中首一不可约多项式.

在情形(i), φ 诱导域的单同态

$$\varphi : F(x) \to K, \quad \frac{g(x)}{h(x)} \mapsto \frac{g(\alpha)}{h(\alpha)}.$$

由 $\mathrm{im}\varphi = F(\alpha)$, 故 $F(x) \xrightarrow{\sim} F(\alpha)$. 在情形(ii), φ 诱导域同构

$$F[x]/(f(x)) \xrightarrow{\sim} F(\alpha), \quad x \mapsto \alpha.$$

此时

$$F(\alpha) = F[\alpha] = \{g(\alpha) \mid g(x) \in F[x]\}.$$

定义5.5. 设 α 为 F 某扩域中元素. 如果对所有 $0 \neq f(x) \in F[x], f(\alpha) \neq 0$, 称 α 为 F 上的**超越元** (transcendental element), 或谓 α 在 F 上**超越** (transcendental). 如果存在 $0 \neq f(x) \in F[x], f(\alpha) = 0$, 称 α 为 F 上的**代数元** (algebraic element), 或谓 α 在 F 上**代数** (algebraic).

由上述分析, 我们立刻有

命题5.6. *如果 α 在 F 上超越, 则 $F(\alpha) \xrightarrow{\sim} F(x)$. 如果 α 在 F 上代数, 则存在 $F[x]$ 上首一不可约多项式 $f(x)$,*

$$F[x]/(f(x)) \xrightarrow{\sim} F(\alpha) = F[\alpha].$$

注记. 上述 $f(x)$ 称为 α 在 F 上的**最小多项式** (minimal polynomial), 或谓**不可约多项式** (irreducible polynomial). 如果$g(x) \in F[x]$ 且$g(\alpha) = 0$, 则称$g(x)$ 为 α 在 F 上的**化零多项式**.

注意到最小多项式必然是化零多项式的因子. 事实上, 由带余除法可得 $g(x) = q(x)f(x) + r(x)$, 其中$\deg r(x) < \deg f(x)$. 则 $r(x)$ 也是 α 在 F 上的化零多项式. 如 $r(x) \neq 0$, 由 $f(x)$ 的不可约性, $(f(x), r(x)) = 1$ 也是 α 的化零多项式, 这不可能.

定义5.7. 设 K/F 为域扩张. 如果存在 $\alpha \in K$ 在 F 上超越, 称 K/F 为**超越扩张** (transcendental extension). 如果对所有 $\alpha \in K$, α 在 F 上代数, 称 K/F 为**代数扩张** (algebraic extension).

如果 $K = F(\alpha_1, \ldots, \alpha_n)$, 称 K/F 为**有限生成扩张** (finitely generated extension). 特别地, 如果 $K = F(\alpha)$, 称 K/F 为**单扩张** (simple extension).

§5.1.3 代数扩张的性质

设 K/F 为域扩张, 则在域的加法和与 F 的乘法意义下, K 是 F 上的线性空间.

定义5.8. 域扩张 K/F 的**扩张次数** (degree of extension), 记为 $[K : F]$, 是指 K 作为 F-线性空间的维数 $\dim_F K$.

如果 K/F 的扩张次数有限, 称 K/F 为**有限扩张** (finite extension), 否则称 K/F 为**无限扩张** (infinite extension).

由线性代数理论, 我们立刻有

命题5.9. *如果 $K = F(\alpha)$ 是 F 上的单代数扩张, $f(x)$ 为 α 的最小多项式. 则*

$$[K : F] = \deg f = n.$$

此时 $\{1, \alpha, \ldots, \alpha^{n-1}\}$ 是 K/F 的一组基. 反之, 若 $[F(\alpha) : F] < +\infty$, 则 α 在 F 上代数.

定理5.10 (次数公式)**.** *设 $K \supseteq M \supseteq F$ 为域扩张, 则*

$$[K : F] = [K : M] \cdot [M : F]. \tag{5.1}$$

证明. 若 K/M 或 M/F 为无限扩张, 则等号显然成立. 否则设 $[K : M] = m$, $[M : F] = n$. 令 $\{\alpha_1, \ldots, \alpha_m\}$ 为 K 作为 M-线性空间的基, $\{\beta_1, \ldots, \beta_n\}$ 为 M 作为 F-线性空间的基, 则对任意 $x \in K$,

$$\begin{aligned} x &= \sum_{i=1}^{m} a_i \alpha_i = \sum_{i=1}^{m} (\sum_{j=1}^{n} a_{ij} \beta_j) \alpha_i \\ &= \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} \alpha_i \beta_j, \quad a_i \in M, a_{ij} \in F, \end{aligned}$$

故 x 为 $\{\alpha_i\beta_j \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$ 的 F-线性组合. 另一方面, 如果

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\alpha_i\beta_j = 0,$$

则 $\sum\limits_{i=1}^{m}(\sum\limits_{j=1}^{n} a_{ij}\beta_j)\alpha_i = 0$. 由 $\{\alpha_1, \ldots, \alpha_m\}$ 线性无关知对所有的 i, $\sum\limits_{j=1}^{n} a_{ij}\beta_j = 0$. 由 $\{\beta_1, \ldots, \beta_n\}$ F-线性无关知 $a_{ij} = 0$.

综上所述 $\{\alpha_i\beta_j \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$ 是 K 作为 F-线性空间的基, 故 $[K : F] = mn = [K : M] \cdot [M : F]$. □

次数公式 (5.1) 有很多应用.

推论5.11. *设 $[K : F] = n$, $\alpha \in K$, 则 $[F(\alpha) : F] \mid n$, 即 α 在 F 上的最小多项式的次数被 n 整除.*

推论5.12. *如果 p 为素数, $[K : F] = p$, $\alpha \in K, \alpha \notin F$, 则 $K = F(\alpha)$.*

命题5.13. *有限扩张即为有限生成代数扩张.*

证明. 如果 K/F 为代数扩张. 令 $\{\alpha_1, \ldots, \alpha_n\}$ 为 K 的一组 F-基, 则 $K = F(\alpha_1, \ldots, \alpha_n)$. 由于 $\{1, \alpha_i, \ldots, \alpha_i^n\}$ 线性相关, 故 α_i 在 F 上代数, 故 K/F 是有限生成的代数扩张.

反之, 如果 $K = F(\alpha_1, \ldots, \alpha_n)$, 且 $\alpha_1, \ldots, \alpha_n$ 在 F 上代数, 则由定理 5.10,

$$[K : F] = [F(\alpha_1, \ldots, \alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})] \cdot \cdots \cdot [F(\alpha_1) : F] < +\infty.$$

命题证毕. □

定理5.14. *设 K 是 F 的扩域, 则 K 中 F-代数元集合构成 K 的子域.*

证明. 设 $\alpha, \beta \in K$, α, β 在 F 上代数, 则 $[F(\alpha, \beta) : F] < +\infty$, 故对于 $\gamma = \alpha \pm \beta$, $\alpha\beta$ 或 $\alpha\beta^{-1}$, $F(\gamma) \subseteq F(\alpha, \beta)$, 故 $[F(\gamma) : F] < +\infty$, 因此 γ 在 F 上代数. □

定理5.15. *如果域 K 在 M 上代数, M 在 F 上代数, 则 K 在 F 上代数.*

证明. 设 $\alpha \in K$, 则 α 在 M 上代数, 则存在

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0, \quad a_i \in M.$$

即 α 在 $F(a_0, a_1, \ldots, a_{n-1})$ 上代数. 由于 $a_0, \ldots, a_{n-1}$ 在 F 上代数, 故

$$[F(\alpha, a_0, a_1, \ldots, a_{n-1}) : F] < +\infty,$$

即 α 在 F 上的代数. □

§5.1.4 域的同态与同构

定义5.16. 设 K, K' 为 F 的扩域. 域同构 $\varphi : K \to K'$ 称为 **F-同构** (F-isomorphism), 是指 φ 在 F 上的限制为恒等映射. 如果 $K = K'$, 称 φ 为域 K 的 **F-自同构** (F-automorphism).

命题5.17. *设 $\varphi : K \to K$ 为 F-自同构, $f(x) \in F[x]$. 若 $\alpha \in K$, $f(\alpha) = 0$, 即 $\alpha \in K$ 是 f 的根, 则 $f(\varphi(\alpha)) = 0$, 即 $\varphi(\alpha) \in K'$ 是 f 的根.*

证明. 令 $f(x) = \sum_{i=1}^{n} a_i x^i$, $a_i \in F$. 则

$$0 = \varphi(f(\alpha)) = \sum_{i=1}^{n} \varphi(a_i\alpha^i) = \sum_{i=1}^{n} a_i\varphi(\alpha)^i = f(\varphi(\alpha)).$$

命题证毕. □

命题5.18. *如果 $\varphi : F(\alpha) \xrightarrow{\sim} F(\beta)$, 其中$\varphi(\alpha) = \beta$ 且 $\varphi|_F = \mathrm{id}$, 则 α 与 β 在F上有相同的不可约多项式.*

证明. 设 $f(x)$ 是 α 的最小多项式, $g(x)$ 是 β 的最小多项式. 考虑 $\varphi : F(\alpha) \to F(\beta)$, 由命题 5.17知 $f(\beta) = 0$, 即 $g(x) \mid f(x)$. 再考虑 $\varphi^{-1} : F(\beta) \to F(\alpha)$ 知 $f(x) \mid g(x)$, 故$f(x) = g(x)$. □

注记. 若仅有 $F(\alpha) = F(\beta)$, α 与 β 的不可约多项式可以相差很大, 但它们的次数必须相等(参见命题 5.9).

§5.1.5 代数闭包与代数封闭域

定义5.19. 域 F 称为**代数封闭域** (algebraically closed field), 是指 $F[x]$ 上的不可约因子均是一次因子; 换言之, 是指若 $f(x) \in F[x]$, 且 $\deg f > 0$, 则存在 $\alpha \in F$, $f(\alpha) = 0$.

如果 K/F 为代数扩张且 K 是代数封闭域, 则称 K 为 F 的**代数闭包** (algebraic closure),

定理5.20. *对给定的域 F, F 的代数闭包存在且 (在同构意义下) 唯一.*

证明. 先证唯一性. 设 K_1, K_2 为 F 的两个代数闭包. 设 L 为 K_1 中的最大子域使得存在域嵌入 $\varphi : L \to K_2$ 且 $\sigma|_F = \mathrm{id}$. 我们证明 $L = K_1$. 若不然, 取 $\alpha \in K_1 \backslash L$, 则 α 在 F 上代数, 故也在 L 上代数. 令 $f(x)$ 为 α 在 F 上的最小多项式, $g(x)$ 为 α 在 L 上的最小多项式, 则 $g(x) \mid f(x)$. 由于 $\varphi(f(x)) = f(x)$ 为 K_2 上一次因式的乘积, 则 $\varphi(g(x))$ 在 K_2 上分解为一次因式之积. 令 β 为 $\varphi(g)(x)$ 的一个根, 则

$$\varphi : L(\alpha) \to \varphi(L)(\beta) \hookrightarrow K_2, \quad \alpha \mapsto \beta$$

是域的嵌入, 这与 L 的最大性矛盾, 故 $L = K_1$. 由于 $\varphi(K_1) \subseteq K_2$ 且 F 上所有次数 $\geqslant 1$ 的多项式在 $\varphi(K_1)$ 中有根. 故 $\varphi(K_1) = K_2$, 即 φ 为同构.

存在性的证明: 我们首先假设下述定理 5.21 成立. 由此, 可以构造一串域

$$E_1 \subset E_2 \subset \cdots \subset E_n \cdots$$

使得$E_n[x]$ 中任何次数大于0 的多项式在E_{n+1} 中都有根. 令E 为所有E_n 的并, 则E 自然是一个域: 如果$x, y \in E$, 则存在n 使得$x, y \in E_n$, 故$x + y, xy \in E_n$. 我们如此定义x 与y 的加法和乘法, 显然这与n 的选择无关, 由此给出了E 的域结构. $E[x]$ 中任何次数大于0 的多项式的系数总在某个E_n 中, 因此在E_{n+1} 中有根, 从而在E 中有根, 故E 是代数封闭域. □

定理5.21. *对于任意域 F, 存在域扩张 E/F, 使得 F 上任何次数 $\geqslant 1$ 的多项式在 E 上均有根.*

为证明定理 5.21, 我们首先有如下引理:

引理5.22. 设 F 为域. 对任意次数 $\geqslant 1$ 的多项式 $f(x) \in F[x]$, 存在 F 的扩域 L, 使得 $f(x)$ 在 L 上有根.

证明. 不妨设 $f(x)$ 首一不可约, 则 $L = F[x]/(f(x))$ 为域. 映射 $\sigma : F \to L$, $a \mapsto a$ 是域的嵌入, 且 $f(x)$ 在 L 上有根 $x \mod f(x)$. □

定理 *5.21* 的证明. 对于 $F[x]$ 上每一个次数 $\geqslant 1$ 的多项式 $f(x)$, 我们对应一未定元 X_f. 令 S 为所有 X_f 构成的集合, 因此 S 与 $F[x]$ 中次数 $\geqslant 1$ 的多项式集合一一对应. 令 $F[S]$ 为F 上由 S 生成的多项式环. 令 I 为 $F[S]$ 中所有 $f(X_f)$ 生成的理想. 我们证明 $I \neq (1)$. 否则存在 $g_1, \ldots, g_n \in F[S]$,

$$g_1 f_1(X_{f_1}) + g_2 f_2(X_{f_2}) + \cdots + g_n f_n(X_{f_n}) = 1.$$

为简单起见, 记 $X_i = X_{f_i}$. 由于 $g_1, \ldots, g_n$ 最多为有限多变量多项式. 不妨记为 $X_1, \ldots, X_N (N \geqslant n)$, 则我们有

$$\sum_{i=1}^{n} g_i(X_1, \ldots, X_N) f_i(X_i) = 1.$$

设 L 为 F 的有限扩张, 其中 $f_1, \ldots, f_n$ 在 F 上有根. 不妨设 α_i 是 f_i 的根. 对于 $i > n$, 令 $\alpha_i = 0$, 则将 $\alpha_1, \ldots, \alpha_N$ 代入上式, 我们得到 $0 = 1$, 不可能! 故 I 不是 $F[S]$.

令 $\mathfrak{m}$ 为 $F[S]$ 中包含 I 的一个极大理想, 则 $E = F[S]/\mathfrak{m}$ 为域, $F \hookrightarrow E$, 且 $F[x]$ 中每个次数 $\geqslant 1$ 的多项式在 E 中均有根. □

习　　题

习题1.1. 设 F/K 为域的扩张, $u \in F$ 是 K 上的奇次代数元素. 求证 $K(u) = K(u^2)$.

习题1.2. 设 p 为素数, 求扩张 $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ 和 $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ 的次数, 其中 $\zeta_n = e^{\frac{2\pi i}{n}}$ 为 n 次本原单位根. 对一般的 n, 扩张 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 的次数是多少?

习题1.3. 求元素 $\sqrt{2} + \sqrt{3}$ 在域 K 上的极小多项式, 其中

(1) $K = \mathbb{Q}$;　　(2) $K = \mathbb{Q}(\sqrt{2})$;　　(3) $K = \mathbb{Q}(\sqrt{6})$.

习题1.4. 证明 $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

习题1.5. 设 F/K 为域的代数扩张, D 为整环且 $K\subseteq D\subseteq F$. 求证 D 为域.

习题1.6. 设 u 属于域 F 的某个扩域, 并且 u 在 F 上代数. 如果 $f(x)$ 为 u 在 F 上的极小多项式, 则 $f(x)$ 必为 $F[x]$ 中不可约元. 反之, 若 $f(x)$ 是 $F[x]$ 中首 1 不可约多项式, 并且 $f(u)=0$, 则 $f(x)$ 为 u 在 F 上的极小多项式.

习题1.7. 设 K/F 为域扩张, $a\in K$. 若 $a\in F(a^m)$, $m>1$, 则 a 在 F 上代数.

习题1.8. 设 $K(x_1,\ldots,x_n)$ 是n 元多项式环$K[x_1,\ldots,x_n]$ 的商域. 若 $u\in K(x_1,\ldots,x_n)$, $u\notin K$, 则 u 在 K 上超越.

习题1.9. 设 K 为域, $u\in K(x)$, $u\notin K$. 证明 x 在 $K(u)$ 上代数.

习题1.10. 令 $K=\mathbb{Q}(\alpha)$ 其中 α 是方程 $x^3-x-1=0$ 的一个根. 求 $\gamma=1+\alpha^2$ 在 $\mathbb{Q}$ 的极小多项式.

习题1.11. 设 a 是正有理数且不是 $\mathbb{Q}$ 中数的平方. 证明$[\mathbb{Q}(\sqrt[4]{a}):\mathbb{Q}]=4$.

习题1.12. 设 u 是多项式 x^3-6x^2+9x+3 的一个根.

(1) 求证 $[\mathbb{Q}(u):\mathbb{Q}]=3$.

(2) 试将 $u^4,(u+1)^{-1},(u^2-6u+8)^{-1}$ 表示成 $1,u,u^2$ 的 $\mathbb{Q}$-线性组合.

习题1.13. 设 x 是$\mathbb{Q}$ 上的超越元且 $u=x^3/(x+1)$, 求 $[\mathbb{Q}(x):\mathbb{Q}(u)]$.

习题1.14. 试写出二元域 $\mathbb{F}_p$ 的一个 2 次不可约多项式 $f(x)$. 设 u 是 $f(x)$ 的一个根, 写出 $\mathbb{F}_2(u)$ 的全部元素以及它们的加法表和乘法表.

习题1.15. 设 M/K 为域的扩张, M 中元素 u,v 分别是 K 上的 m 次和 n 次代数元素. $F=K(u)$, $E=K(v)$.

(1) 求证 $[FE:K]\leqslant mn$.

(2) 如果 $(m,n)=1$, 则 $[FE:K]=mn$.

习题1.16. 设 F 为特征 p 域, p 为素数. $c \in F$.

(1) 证明 $x^p - x - c$ 在 $F[x]$ 中不可约当且仅当 $x^p - x - c$ 在 F 中无根.

(2) 若$\mathrm{char}F = 0$ 时, 试问(1) 中结论是否仍然成立?

习题1.17. 设F 为特征不为 2 的域, 证明 F 的每个二次扩张均有形式 $F(\sqrt{a}), a \in F$. 如果 $\mathrm{char}F = 2$, 则结论是否成立?

习题1.18. 设 $K = \mathbb{Q}(\alpha)$ 为 $\mathbb{Q}$ 的单扩张, 其中 α 在 $\mathbb{Q}$ 上代数. 证明 $|\mathrm{Aut}(K)| \leqslant [K : \mathbb{Q}]$.

§5.2 尺规作图问题

在本节, 我们应用域扩张知识来回答古典几何中的尺规作图问题. 用规范语言来说:

定义5.23. 给定复平面上点的集合, 它包括原点以及点 $(1, 0)$, 则经下面方法得到的点、直线和圆称为**可构造** (constructible)的点、直线和圆:

(i) 连接两可构造点作直线.

(ii) 以一可构造点为圆心过另一可构造点作圆.

(iii) 可构造直线之间、圆之间或直线与圆的交点为新可构造点.

如果 $(a, 0)$ 为可构造点, 称 $a \in \mathbb{R}$ 为**可构造数** (constructible number).

引理5.24. 经过可构造点 A 可作直线与已知可构造直线 l 垂直.

证明. 分两种情况:

(i) $A \in l$. 令 B 为 l 上另一可构造点, 以 A 为圆心过 B 作圆交 l 于点 C. 以 B, C 为圆心分别过 C, B 作圆交于点 D, 则直线 AD 与 l 垂直(图 5.1).

(ii) $A \notin l$. 以 A 为圆心, 可构造长度为半径作圆交 l 于 B, C, 以 B, C 为圆心分别过 C, B 作圆交于点 D, 则直线 AD 与 l 垂直(图 5.2). □

引理5.25. 如果 $A \notin l$, 则可过点 A 作直线 l'与 l 平行.

证明. 过 A 作 l 的垂线 l_0, 过 A 作 l_0 的垂线 l', 则 l' 与 l 平行. □

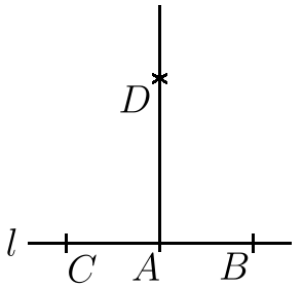


图 5.1: 过直线上一点作垂线

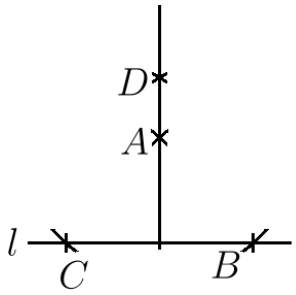


图 5.2: 过直线外一点作垂线

引理5.26. *给定 B 及过 B 的直线 l. 对于复平面上任两可构造点 O, A, 可在 l 上构造点 C, 使得 $|BC| = |OA|$.*

证明. 如果 OA 不在 l 上, 则如图 5.3 所示, 过 A, B 分别作直线平行于 OB, OA, 交于点 D, 以 B 为圆心过 D 作圆交 l 于 C, 则 $|BC| = |BD| = |OA|$. 如果 OA 在 l 上, 我们可以另找一条直线 l', 经两次作图即可. □

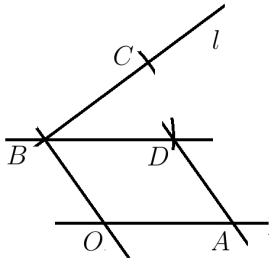


图 5.3: 构造定长线段

引理5.27. *如果 (a, b) 为可构造点, 则 a, b 为可构造数.*

证明. 由于 x 轴为可构造直线, 过 (a, b) 作 x 轴的垂线即得 $(a, 0)$, 再由引理 5.26 即得点 $(b, 0)$. □

命题5.28. *可构造数的集合 F 构成 $\mathbb{R}$ 的子域.*

证明. 由引理 5.26 知 F 即为所有可构造点两两间的距离和相反数.

首先由 $(0, 0), (1, 0)$ 为可构造点, 得到 $0 \in F$ 且 $1 \in F$.

若 $\alpha, \beta \in F$, 则 $-\alpha \in F$ 显然成立, $\alpha + \beta$ 由引理 5.26 也显然成立, 故只要证明 $\alpha\beta \in F$ 且 $\alpha^{-1} \in F$. 我们不妨设 $\alpha, \beta > 0$, 则证明如图 5.4 所示.

□

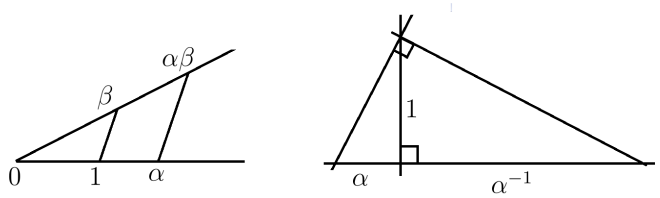


图 5.4: 乘积和逆

引理5.29. *如果正实数 $\alpha \in F$, 则 $\sqrt{\alpha} \in F$.*

证明. 如图 5.5. □

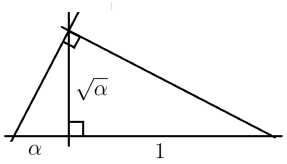


图 5.5: 求平方根

引理5.30. *设 $A_i = (a_i, b_i)$ $(i = 1, 2, 3, 4)$ 是复平面4点且其坐标在域 K 中. 则通过它们作直线与圆得到的交点坐标要么在 K 中, 要么在 $K(\sqrt{r})$ 中, 其中 $r \in K$.*

证明. 过 A_i 与 A_j 的直线为

$$(a_i - a_j)(y - b_j) = (b_i - b_j)(x - a_j).$$

以 A_i 为圆心过 A_j 的圆为

$$(x - a_i)^2 + (y - b_i)^2 = (a_j - a_i)^2 + (b_j - b_i)^2.$$

讨论它们的交点即得引理. □

定理5.31. *设 $a_1, \ldots, a_m$ 为可构造实数, 则存在域扩张链*

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = K,$$

其中

(1) $K \subseteq \mathbb{R}$.

(2) $a_1, \ldots, a_m \in K$.

(3) $F_{i+1} = F_i(\sqrt{r_i}), r_i \in F_i \backslash F_i^2$.

反之, 若 $\mathbb{Q} \subseteq F_1 \subseteq \cdots \subseteq F_n = K$, 且(3) 成立, 则 K 中元素可构造.

证明. 由上面所列出的引理及构造的规则即得. □

推论5.32. 如果 $a \in \mathbb{R}$ 可构造, 则 a 在 $\mathbb{Q}$ 上代数且存在整数 $r \geq 0$,

$$[\mathbb{Q}(a) : \mathbb{Q}] = 2^r. \tag{5.2}$$

推论5.33. 不可能用尺规作图来任意三等分角.

证明. 我们只需证明 60° 不可尺规三等分即可. 首先容易看出 60° 可以尺规作出, 这是因为 $\cos 60^\circ = \frac{1}{2}$ 为可构造数. 但是对于 $\theta = 20^\circ = \frac{\pi}{9}$, $\cos 3\theta = \frac{1}{2}$, 于是 $\cos\theta$ 的最小多项式为 $4x^3 - 3x + \frac{1}{2}$, $[\mathbb{Q}(\cos\theta) : \mathbb{Q}] = 3$ 不是 2 的幂. □

推论5.34. 设 p 为素数. 若正 p 边形可以用直尺圆规构造, 则 $p = 2^{2^n} + 1$ 为 ***Fermat* 素数** (*Fermat prime*).

注记. 逆命题也成立, 它是 Galois 理论的推论(命题 6.38).

证明. 令 $\zeta_p = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$, $\zeta_p + \zeta_p^{-1} = 2\cos\frac{2\pi}{p}$, 则

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p + \zeta_p^{-1})] = 2.$$

而 $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, 故 $[\mathbb{Q}(\cos\frac{2\pi}{p}) : \mathbb{Q}] = \frac{p-1}{2}$. 由推论 5.32, 正 p 边形可构造等价于 $p - 1 = 2^m$, 即 $p = 2^m + 1$. 若 m 有奇因子 m_0, $m = m_0 r$, 则 $2^r + 1 \mid p$, 即 p 不为素数. 故 $p = 2^{2^n} + 1$ 为 Fermat 素数. □

习 题

习题2.1. 下列哪些量可以尺规作出?

(1) $\sqrt[4]{3 + 5\sqrt{8}}$; (2) $\frac{3\sqrt{5}}{\sqrt{7}-4}$; (3) $2 + \sqrt[5]{7}$; (4) $x^5 - 3x^2 + 6$ 的根.

习题2.2. 证明可以尺规三等分 45° 和 54° 度角.

习题2.3. 解决古代"难"题—倍方问题.

习题2.4. 设 $3 \leqslant n \leqslant 10$ 为正整数, 则正 n 边形是否可尺规作出?

§5.3 代数基本定理

在本节, 我们证明如下的定理, 即所谓**代数基本定理**.

定理5.35 (代数基本定理)**.** *设 $f(x) \in \mathbb{C}[x]$ 为次数 $\geqslant 1$ 的多项式, 则存在 $x_0 \in \mathbb{C}$ 使得 $f(x_0) = 0$.*

证明. 定理等价于证明存在 $x_0 \in \mathbb{C}$, $|f(x_0)| = 0$. 我们只需证明如下两个引理. □

引理5.36. *如果 $x_0 \in \mathbb{C}$, $f(x_0) \neq 0$, 则 $|f(x_0)|$ 不是 $|f(x)|$ 的最小值.*

引理5.37. *如果 $f(x)$ 是复多项式, 则 $|f(x)|$ 在 $\mathbb{C}$ 上某点 x_0 处达到最小值.*

引理 *5.36* 的证明. 首先, 对于任意 $c \in \mathbb{C}$, 即 $c = re^{i\theta}$, 则 $\alpha = \sqrt[k]{r}e^{\frac{i\theta}{k}}$ 是多项式 $x^k - c$ 的根.

将 x 用 $x + x_0$ 代替, 故不妨假设 $x_0 = 0$. 将 $f(x)$ 乘以 $f(0)^{-1}$, 故不妨设 $f(0) = 1$. 我们要证明 1 不是 $|f(x)|$ 的最小值. 记

$$f(x) = 1 + ax^k + x^{k+1}g(x), \quad a \neq 0.$$

设 $\alpha^k = -a$, 将 x 用 αx 代替, 则

$$f(x) = 1 - x^k + x^{k+1}g(x).$$

所以当 x 足够小时,

$$\begin{aligned} |f(x)| &\leqslant |1 - x^k| + |x^{k+1}g(x)| \\ &= 1 - x^k + x^{k+1}|g(x)| \\ &= 1 - x^k(1 - x|g(x)|) < 1, \end{aligned}$$

引理得证. □

引理 *5.37* 的证明. 若 $f(x) = a_n x^n + \cdots + a_0$,

$$\lim_{|x|\to+\infty} \frac{|f(x)|}{|x|^n} = \lim_{|x|\to+\infty} |a_n + \frac{a_{n-1}}{x} + \cdots + \frac{a_0}{x^n}| = |a_n|,$$

故当 $|x| \to +\infty$ 时, $|f(x)| \to +\infty$, 取 $R > 0$, 使得当 $|x| \geqslant R$ 时, $|f(x)| > |f(0)|$. 则

$$\min_{x\in\mathbb{C}} |f(x)| = \min_{|x|\leqslant R} |f(x)|,$$

而后者是可以达到的(由于有界闭区域上的连续函数有最大最小值). □

习 题

习题3.1. 证明 $\mathbb{C}[x]$ 的极大理想与复平面上的点一一对应. $\mathbb{R}[x]$ 的极大理想可以自然地对应到复平面上的什么?

§5.4 有限域的理论

所谓**有限域**, 即元素个数有限的域. 此时称有限域元素个数为**有限域的阶** (order of finite field). 若 K 为有限域, 则 K 的特征必然是某个素数 p, 故有 $\mathbb{F}_p \hookrightarrow K$ 为 K 的子域. 设 $[K : \mathbb{F}_p] = n$, 则 K 是 $\mathbb{F}_p$ 上的 n 维向量空间, $|K| = p^n$. 故我们有如下引理:

引理5.38. 有限域的阶均为素数方幂.

例5.39. 设 α 为 $\mathbb{F}_2$ 上不可约多项式 $x^2 + x + 1$ 的根, 则 $\mathbb{F}_2(\alpha)$ 是 4 阶有限域, 它的 4 个元素为 $0, 1, \alpha, 1 + \alpha$. 由于 $\mathbb{F}_2[x]$ 上的二次不可约多项式只有一个, 故 $\mathbb{F}_2(\alpha) = \mathbb{F}_4$ 为唯一的 4 元域.

下述定理是有限域理论的基本定理.

定理5.40. 设 p 是素数, $q = p^r, r \geqslant 1$.

(1) 存在阶为 q 的有限域.

(2) 在 $\mathbb{F}_p$ 的代数闭包 $\overline{\mathbb{F}}_p$ 中只有唯一的 q 元域 $\{x \in \overline{\mathbb{F}}_p \mid x^q = x\}$, 且所有 q 元域均同构于它.

(3) 如果 K 的阶为 q, 则 $K^\times$ 是 $q - 1$ 阶循环群.

(4) 对于任何 q 元域 K 中元素 α, $\alpha^q = \alpha$ 且

$$x^q - x = \prod_{\alpha\in K} (x - \alpha). \tag{5.3}$$

(5) $\mathbb{F}_p$ 上的 r 次不可约多项式均是 x^q-x 的因子, 且

$$x^q-x=\prod_{d\mid r}\prod_{\substack{f\text{首一不可约}\\ \deg f=d}} f(x). \tag{5.4}$$

(6) 若 K,K' 均为有限域, 且都在 $\mathbb{F}_p$ 某给定的代数闭包中, 且 $|K|=p^r$, $|K'|=p^k$, 则 $K\supseteq K'$ 当且仅当 $k\mid r$.

(7) $\mathrm{Aut}(\mathbb{F}_q)$ 是由 $\sigma:\mathbb{F}_q\to\mathbb{F}_q,\ x\mapsto x^p$ 生成的 r 元循环群.

注记. $\sigma:x\mapsto x^p$ 称为 K 的**绝对 Frobenius** (absolute Frobenius). 对于任意特征 p 域, $\sigma:K\to K, x\mapsto x^p$ 均为域同态, 它将 K 同构于 $K^{(p)}=\{x^p\mid x\in K\}\hookrightarrow K$.

证明. (1) 我们证明 $X=\{x\in\overline{\mathbb{F}}_p\mid x^q=x\}$ 为 q 元域.

首先, 由于 $f(x)=x^q-x$ 在 $\overline{\mathbb{F}}_p$ 上无重根, 故 $|X|=\deg f=q$. 其次, 若 $\alpha,\beta\in X$, $(\alpha\pm\beta)^q=\alpha^q\pm\beta^q=\alpha\pm\beta$, 所以 $\alpha\pm\beta\in X$. $(\alpha\cdot\beta)^q=\alpha^q\beta^q=\alpha\beta$, 所以 $\alpha\beta\in X$. 若 $\alpha\in X,\alpha\neq 0$, 则 $(\alpha^{-1})^q=(\alpha^q)^{-1}=\alpha^{-1}$, 所以 $\alpha^{-1}\in X$. 由上可知 X 构成域.

(3) 我们证明如下定理.

定理5.41. 域上的有限乘法群均是循环群.

证明. 设 G 是域 F 上的 n 阶有限乘法群. 由于 $|G|=n$, 对任意 $x\in G, x^n=1$. 但域中多项式 x^n-1 最多有 n 个根, 故 $G=\{x\in F\mid x^n=1\}$. 由于 G 是有限阿贝尔群, 由结构定理

$$G\cong\mathbb{Z}/n_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/n_k\mathbb{Z},\quad n_1\mid n_2\mid\cdots\mid n_k,$$

则 G 中所有元素均要满足 $x^{n_k}=1$. 但 F 中这样的元素最多有 n_k 个, 所以 $n\leqslant n_k$, 故 $n=n_k$, $G\cong\mathbb{Z}/n\mathbb{Z}$ 为循环群. □

(2) 唯一性由(3)立得.

(4) 由于 $K^\times$ 是 $q-1$ 阶循环群, 对于 $\alpha\in K,\alpha^q=\alpha$. 由于 x^q-x 最多有 q 个根, $\alpha\in K$ 为其所有根, 故 $x^q-x=\prod\limits_{\alpha\in K}(x-\alpha)$.

(5) 设 $f(x)\in\mathbb{F}_p[x]$, $\deg f=r$, f 首一不可约, 则 $\mathbb{F}_p(\alpha)=\mathbb{F}_p[x]/f(x)$ 为 q 阶有限域. 我们有 α 是 x^q-x 的根, 故 $f(x)\mid x^q-x$. 同样可证, 对于 $\deg f=d\mid r$, f 首一不可约, $f(x)\mid x^q-x$, 故有

$$\prod_{d\mid r}\prod_{\substack{f\text{首一不可约}\\ \deg f=d}} f(x)\ \Big|\ x^q-x.$$

反之, 若 $g(x)\mid x^q-x$, α 为 $g(x)$ 的根, 则 $\alpha^q-\alpha=0$, 即 $\mathbb{F}_p(\alpha)=\mathbb{F}_p[x]/(g(x))=\mathbb{F}_{p^{\deg g}}\subseteq\mathbb{F}_q$, 所以 $\mathbb{F}_p(\alpha)^\times$ 是 $\mathbb{F}_q^\times$ 的子群, 即 $p^{\deg g}-1\mid p^r-1$. 由 $(p^m-1,p^n-1)=p^{(m,n)}-1$ 知 $\deg g\mid r$.

综上可知 x^q-x 的所有首一不可约因子为 $f(x),\deg f=d\mid r, f$ 首一不可约. 由于 x^q-x 无重根, 它的所有不可约因子也无重根. 所以

$$x^q-x=\prod_{d\mid r}\prod_{\substack{f\text{首一不可约}\\ \deg f=d}} f(x).$$

(6) 如果 $K\supseteq K'$, 则 $K'^\times$ 是 $K^\times$ 的子群, 故 $p^k-1\mid p^r-1$. 由 $(p^m-1,p^n-1)=p^{(m,n)}-1$ 知 $k\mid r$.

反之, 若 $k\mid r$, 则

$$K'=\{x\in\overline{\mathbb{F}}_p\mid x^{p^k}=x\}\subseteq K=\{x\in\overline{\mathbb{F}}_p\mid x^{p^r}=x\}.$$

(7) 首先 $\sigma:\mathbb{F}_q\to\mathbb{F}_q, x\mapsto x^p$ 为域 $\mathbb{F}_q$ 的自同构. 其次, 若 $\varphi:\mathbb{F}_q\to\mathbb{F}_q$ 为自同构, 由 $\varphi(0)=0,\varphi(1)=1$, 我们知 $\varphi|_{\mathbb{F}_p}=\mathrm{id}$. 令 $\mathbb{F}_q=\mathbb{F}_p(\alpha)$, 其中 α 为 $\mathbb{F}_q^\times$ 的生成元. 令 $f(x)$ 为 α 的最小多项式, 故 $\deg f=r$, 且

$$\varphi(f(\alpha))=f(\varphi(\alpha))=0,$$

即 $\varphi(\alpha)$ 也是 $f(x)$ 的根. 又由于 $\sigma\in\mathrm{Aut}(\mathbb{F}_q),\sigma(\alpha)=\alpha^p,\dots,\sigma^{r-1}(\alpha)=\alpha^{p^{r-1}}$ 也是 $f(x)$ 的根. 由于 $f(x)\mid x^q-x$ 无重根, $\alpha,\alpha^p,\dots,\alpha^{p^{r-1}}$ 为 $f(x)$ 的所有根, 即

$$f(x)=(x-\alpha)(x-\alpha^p)\cdots(x-\alpha^{p^{r-1}}).$$

所以 $\varphi(\alpha)=\alpha^{p^k}=\sigma^k(\alpha)$, 故 $\varphi=\sigma^k$. □

注记. (1) 由上面定理的证明, 我们知道如果 $f(x)$ 为 $\mathbb{F}_p$ 上首一 d 次不可约多项式, α 为 $f(x)$ 的根, 则

$$f(x) = (x-\alpha)(x-\alpha^p)\cdots(x-\alpha^{p^{r-1}}). \tag{5.5}$$

(2) 若 $\overline{\mathbb{F}}_p$ 为 $\mathbb{F}_p$ 的代数闭包, 则

$$\overline{\mathbb{F}}_p = \bigcup_{r\in\mathbb{N}} \mathbb{F}_{p^r}$$

且 $\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^m}$ 当且仅当 $r \mid m$.

例5.42. 设 α, β 为 $\mathbb{F}_p[x]$ 中 x^2-2, x^2-3 的根. 试求当 $p = 5, 7$ 时, $\alpha+\beta$ 满足的最小多项式.

解. 当 $p=5$ 时, x^2-2 和 x^2-3 均是不可约多项式, 故 $\mathbb{F}_5(\alpha) = \mathbb{F}_{5^2} = \mathbb{F}_5(\beta) = \mathbb{F}_5(\alpha,\beta)$. 若 $\alpha^2 = 2$, 则 $(2\alpha)^2 = 3$, 故 $\beta = \pm 2\alpha$. 所以 $\alpha+\beta = 3\alpha$ 或 $-\alpha$, 其最小多项式为 x^2-3 或 x^2-2.

当 $p=7$ 时, $3^2 = 2$, 故 $\alpha = \pm 3$, $\alpha+\beta = \pm 3+\beta$, 其不可约多项式为 $(x\mp 3)^2 - 3 = x^2 \pm x - 1$. □

在实际应用中, 常常需要判定 $\mathbb{Z}[x]$ 上多项式是否可约, 此时我们有下面简单事实.

命题5.43. 若本原多项式 $f(x) \in \mathbb{Z}[x]$ 可约, 则 $\bar{f}(x) = f(x) \mod p \in \mathbb{F}_p[x]$ 可约. 故若 $\bar{f}(x)$ 为 $\mathbb{F}_p[x]$ 上不可约多项式, 则 $f(x)$ 为 $\mathbb{Z}[x]$ 上不可约多项式.

我们重新证明一下 Eisenstein 判别法.

命题5.44 (Eisenstein 判别法)**.** 如果 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $p \nmid a_n$, $p \mid a_i (0 \leqslant i < n)$ 且 $p^2 \nmid a_0$. 则 $f(x)$ 不可约.

证明. 考虑 $\overline{f(x)} = \bar{f}(x) \mod p$, 则 $\bar{f}(x) = \bar{a}_n x^n$. 若 $f(x) = g(x)h(x)$ 可约, 则 $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$, 故 $\bar{g}(x) = \bar{b}_k x^k, \bar{h}(x) = \bar{c}_l x^l$, 所以

$$g(x) = b_k x^k + \cdots + b_1 x + b_0, \quad h(x) = c_l x^l + \cdots + c_1 x + c_0.$$

由 $p \mid b_0$ 及 $p \mid c_0$ 知 $p^2 \mid b_0 c_0 = a_0$, 与已知矛盾. □

命题5.45. 如果 $f(x) \in K[x]$ 的次数为 2 次或 3 次, 则 $f(x)$ 在 $K[x]$ 上可约当且仅当存在 $\alpha \in K, f(\alpha) = 0$.

证明. 若多项式 $f(x)$ 可约, 则 $f(x) = g(x)h(x)$, 且 $g(x), h(x)$ 的次数均大于或等于 1. 由于 $\deg f = 2$ 或 3, 故 $g(x)$ 与 $h(x)$ 必有一次数为 1. 故存在 $\alpha \in K$, $f(\alpha) = 0$. 反之显然. □

习 题

习题4.1. 构造一个 8 元域并写出它的加法表和乘法表.

习题4.2. 列出 $\mathbb{F}_2$ 上全部次数 $\leqslant 4$ 的不可约多项式, 列出 $\mathbb{F}_3$ 上全部 2 次不可约多项式.

习题4.3. 设 p, l 为素数, n 为正整数, 试求 $F_p[x]$ 中 l^n 次首一不可约多项式的个数.

习题4.4. 设 $\alpha_1^2 = 2$, $\alpha_2^2 = 3$. 求 $\alpha_1 + \alpha_2$ 在 $\mathbb{Q}, \mathbb{F}_5, \mathbb{F}_7$ 上的不可约多项式.

习题4.5. 设 $f(x)$ 是 $\mathbb{F}_p[x]$ 中首一不可约多项式.

(1) 若 u 为 $f(x)$ 的一个根, 则 $f(x)$ 共有彼此不同的 n 个根, 并且它们为 $u, u^p, u^{p^2}, \ldots, u^{p^{n-1}}$;

(2) 若 $f(x)$ 的一个根 u 为域 $F = \mathbb{F}_p(u)$ 的乘法循环群 $F^\times$ 的生成元, 则 $f(x)$ 每个根也都是$\mathbb{F}^\times$ 的生成元. 这样的多项式称为 $\mathbb{F}_p[x]$ 中的 n 次**本原多项式**.

(3) 证明 $\mathbb{F}_p[x]$ 中 n 次本原多项式共有 $\varphi(p^n - 1)/n$ 个, 其中 φ 是欧拉函数.

习题4.6. 当 $n \geqslant 3$ 时, $x^{2^n} + x + 1$ 是 $\mathbb{F}_2[x]$ 中可约多项式.

习题4.7. (1) 证明 $x^4 + x + 1$ 为 $\mathbb{F}_2[x]$ 中本原多项式;

(2) 列出 16 元域 $\mathbb{F}_{16} = \mathbb{F}_2[u]$ 中唯一的 4 元子域的全部元素, 这里 u 是 $x^4 + x + 1 \in \mathbb{F}_2[x]$ 的一个根;

(3) 求出 u 在 $\mathbb{F}_4$ 上的极小多项式.

习题4.8. (1) 证明 $x^4+x^3+x^2+x+1$ 为 $\mathbb{F}_2[x]$ 中不可约多项式但不是本原多项式.

(2) 令 u 为 $x^4+x^3+x^2+x+1\in\mathbb{F}_2[x]$ 的一个根, 试问 $\mathbb{F}_{16}=\mathbb{F}_2(u)$ 中哪些元素是 $\mathbb{F}_{16}-\{0\}$ 的乘法生成元?

习题4.9. 设 F 是有限域, $a,b\in F^\times$. 求证: 对每个 $c\in F$, 方程 $ax^2+by^2=c$ 在域 F 中均有解 (x,y).

习题4.10. 证明多项式 $f(x)=x^3+x+1$ 和 $g(x)=x^3+x^2+1$ 在 $\mathbb{F}_2$ 上是不可约的. 设 K 是通过添加 f 的一个根得到的扩域, 并设 L 是添加 g 的一个根得到的扩域. 具体地描述一个从 K 到 L 的同构.

习题4.11. 设 K 是有限域. 证明 K 中非零元素的乘积为 -1.

习题4.12. 在域 $\mathbb{F}_3$ 上分解 x^9-x 和 $x^{27}-x$.

习题4.13. 设 p 为素数, F 是 p^n 元域, $G=\mathrm{Aut}(F)$. 对于每个 $a\in F$, 令

$$\mathrm{Tr}(a)=\sum_{a\in G}\sigma(a),\quad N(a)=\prod_{a\in G}\sigma(a).$$

证明: (1) $\mathrm{Tr}:F\to\mathbb{F}_p$ 是加法群的满同态;

(2) $N:F^\times\to\mathbb{F}_p^\times$ 是乘法群的满同态.

习题4.14. 设 F 为 $q=p^n$ 元域, p 为素数, H 是 $\mathrm{Aut}(F)$ 的 m 阶子群. $K=\{a\in F\mid \text{对每个 }\sigma\in H,\sigma(a)=a\}$. 证明:

(1) $m\mid n$;

(2) K 是 F 中唯一的 $p^{n/m}$ 元子域.

习题4.15. 设 F 为 $q=p^n$ 元域. p 为素数. $f(x)$ 为 $F[x]$ 中不可约多项式. 证明:

(1) $f(x)$ 有重根当且仅当存在 $g(x)\in F[x]$, 使得 $f(x)=g(x^p)$;

(2) 如果 $f(x)=g(x^{p^n})$, 其中 $g(x)\in F[x]$, 但是不存在 $\tilde{g}(x)\in F[x]$ 使得 $f(x)=\tilde{g}(x^{p^{n+1}})$, 则 $p^n\mid m=\deg f$, 并且 $f(x)$ 共有 m/p^n 个不同的根, 每个根的重数均为 p^n.

习题4.16. 设 p 是素数, $q = p^n$, F 为 q 元有限域.

(1) 求群 $\mathrm{SL}_n(F)$ 的阶.

(2) 证明 $\mathrm{GL}_n(\mathbb{F}_p)$ 中对角线全为 1 的上三角阵构成 p^3 阶非阿贝尔群 (注意p^2 阶群是阿贝尔群).

第六章　Galois 理论

§6.1　Galois 理论的主要定理

设 K 是域 F 的扩张, 记为 K/F. 在未作特殊说明时, 我们设 K/F 是有限扩张.

§6.1.1　Galois 群的定义和例子

我们首先回忆一下 K 的 F-自同构的定义, 即若 σ 是 K 的自同构且 σ 在 F 上的限制为恒等映射, 则称 σ 为 K 的 F-自同构. 在本章中, 我们将频繁使用如下简单但有用的事实.

引理6.1. *设 K/F, $\widetilde{K}/\widetilde{F}$ 为域扩张, 且 $\varphi : K \to \widetilde{K}$ 为域同态且 $\varphi(F) \subseteq \widetilde{F}$. 若 $f(x) \in F[x]$, 记 $\varphi(f(x)) = \widetilde{f}(x)$, 则若 $\alpha \in K$ 为 $f(x)$ 的根, 则 $\widetilde{\alpha} = \varphi(\alpha)$ 必为 $\widetilde{f}(x)$ 的根.*

特别地, 取 $K = \widetilde{K}$, $F = \widetilde{F}$, σ 为 K 的 F-自同构, 则若 $\alpha \in K$ 为 $f(x) \in F[x]$ 的根, $\sigma(\alpha)$ 必为 $f(x)$ 的根.

定义6.2. K 的所有 F-自同构构成的集合, 在以复合运算作乘法下构成的群, 称为 K/F 的 **Galois 群** (Galois group), 记为 $\mathrm{Gal}(K/F)$ 或 $G(K/F)$.

例6.3. *设 $F = \mathbb{F}_p(T)$ 为有限域 $\mathbb{F}_p$ 的有理函数域, $K = \mathbb{F}_p(\sqrt[p]{T})$. 由于 $\alpha = \sqrt[p]{T}$ 的最小多项式为 $x^p - T = (x-\alpha)^p$, 其所有的根均为 α (重数为 p). 若 $\sigma \in \mathrm{Gal}(K/F)$, 由引理 6.1 必有 $\sigma(\alpha) = \alpha$, 即 $\sigma = 1, \mathrm{Gal}(K/F) = \{1\}$.*

例6.4 (二次扩张)**.** *设 K/F 是**二次扩张** (quadratic extension), 取 $\alpha \in K, \alpha \notin F$, 则 $K = F(\alpha)$. 设 α 在 F 上的最小多项式为 $f(x) = x^2 + bx + c$. 如果 α, α' 为 $f(x)$ 的两个根, 则*

$$\alpha + \alpha' = -b, \quad \alpha \cdot \alpha' = c,$$

故 $\alpha' = -b - \alpha \in F(\alpha) = K$. 令 σ 为 K 的 F-自同构, 则由引理 6.1, $\sigma(\alpha) = \alpha$ 或 α'. 若 $\sigma(\alpha) = \alpha$, 则 $\sigma = 1$. 故若 $\alpha \neq \alpha'$, 则 $\mathrm{Gal}(K/F) = \{1, \sigma\}$, 其中 $\sigma(\alpha) = \alpha'$. 若 $\alpha = \alpha'$, 则 $\mathrm{Gal}(K/F) = \{1\}$.

我们来讨论一下 $\alpha=\alpha'$ 的情况. 此时 $2\alpha=-b$. 如果2在 F 上可逆, 则 $\alpha=-b/2\in F$, 不可能. 故此时 F 的特征为 2 且 $b=0$, $f(x)=x^2+c$ 为 $F[x]$ 的不可约多项式, 它的根是两重根.

对于 $\mathrm{char}F\neq 2$ 的情形, $f(x)=(x+\frac{b}{2})^2+\frac{4c-b^2}{4}$. 令 $D=\frac{1}{4}(b^2-4c)$, 则 $K=F(\sqrt{D})$. 此时 $\mathrm{Gal}(K/F)=\{1,\sigma\}$, 其中 $\sigma(\sqrt{D})=-\sqrt{D}$.

例6.5 (双二次扩张)**.** 我们首先假设 $\mathrm{char}F\neq 2$. 令 $K=F(\alpha,\beta)$, 其中 $\alpha^2=D_1\in F$, $\beta^2=D_2\in F$. 如果 $[K:F]=4$, 则称 K/F 为**双二次扩张** *(biquadratic extension)*, 此时 $[K:F(\alpha)]=[K:F(\beta)]=2$, $\{1,\alpha,\beta,\alpha\beta\}$ 为 K 的一组 F-基. 对于任意 $\sigma\in\mathrm{Gal}(K/F)$, $\sigma(\alpha)=\pm\alpha$, $\sigma(\beta)=\pm\beta$. 故 $|\mathrm{Gal}(K/F)|\leqslant 4$, 但是 $\mathrm{Gal}(K/F(\alpha))=\{1,\sigma\}$, 其中 $\sigma(\alpha)=\alpha$, $\sigma(\beta)=-\beta$. $\mathrm{Gal}(K/F(\beta))=\{1,\tau\}$ 其中 $\tau(\alpha)=-\alpha$, $\tau(\beta)=\beta$. 故 $\mathrm{Gal}(K/F)=\{1,\sigma,\tau,\sigma\tau\}\cong\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ 为 *Klein* 群 K_4.

例6.6 (三次扩张)**.** 设 $K=\mathbb{Q}(\sqrt[3]{2})$, $F=\mathbb{Q}$, 则 $[K:F]=3$, K/F 为**三次扩张** *(cubic extension)*. 此时 $\mathrm{Gal}(K/F)=\{1\}$.

在本章中, 我们将特别证明如下定理

定理6.7. 设 K/F 为域的有限扩张, 则 $|\mathrm{Gal}(K/F)|\leqslant[K:F]$.

定义6.8. 称域扩张 K/F 是 **Galois 扩张**, 如果 $|\mathrm{Gal}(K/F)|=[K:F]$.

由定义, 我们知二次扩张($\mathrm{char}F=2, f(x)=x^2+c$ 除外)和双二次扩张均是 Galois 扩张. 而当 $\mathrm{char}F=2$, α 是不可约多项式 $f(x)=x^2+c$ 的根时, $F(\alpha)/F$ 不是 Galois 扩张. 例 6.3 和例 6.6 中的扩张均不是 Galois 扩张.

由于 $G=G(K/F)$ 是 $\mathrm{Aut}(K)$ 的子群, G 作用在 K 上. 令

$$K^G=\{\alpha\in K\mid \varphi(\alpha)=\alpha \text{ 对任意 } \varphi\in G \text{ 成立}\}. \tag{6.1}$$

由定理 6.7, 我们有如下推论.

推论6.9. 如果 K/F 是 *Galois* 扩张, 设 $G=\mathrm{Gal}(K/F)$ 是其 *Galois* 群, 则 $K^G=F$.

证明. 令 $L=K^G$. 首先显然有 $F\subseteq L$, 故 $\mathrm{Gal}(K/L)\subseteq G$. 其次对于任意 $\varphi\in G$, $\varphi|_L=\mathrm{id}$, 故 $\varphi\in\mathrm{Gal}(G/L)$. 因此 $G=\mathrm{Gal}(K/L)$. 由 $|G|=[K:F]\leqslant[K:F]$ 知 $F=L$. □

在例 6.3, 例 6.4, 例 6.6 中, 我们可以发现 K/F 的 Galois 群的阶小于 $[K:F]$ 有两种情况. 一种情况是 K 中的元素 α 的最小多项式有重根(例 6.3 与例 6.4). 第二种情况是 α 的最小多项式的根不全在 K 中. 由此, 我们将讨论两种情况: 可分扩张与正规扩张.

§6.1.2 可分多项式与可分扩张

设 $f(x)\in F[x]$ 为首一多项式, 则 $f(x)$ 有重根当且仅当 $(f,f')\neq 1$ (定理 4.27). 若 $f(x)$ 是不可约多项式, 这也等同于 $f'\neq 0$. 故若

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

则

$$f'(x)=nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1=0,$$

即有 $\mathrm{char}F=p>0$, 且 $a_i=0$ 如果 $p\nmid i$. 综上所述, 我们有

引理6.10. *设 $f(x)\in F[x]$ 为首一不可约多项式. 若 $f(x)$ 有重根, 则 $\mathrm{char}F=p>0$ 且 $f(x)=g(x^p)$.*

定义6.11. 如果多项式 $f(x)\in F[x]$ 的不可约因子无重根, 称 $f(x)$ 为**可分多项式** (separable polynomial). 反之, 称 $f(x)$ 为**不可分多项式** (inseparable polynomial).

由上述引理可知, 如果 $\mathrm{char}F=0$, 则所有的多项式都是可分多项式.

定义6.12. 设 $\mathrm{char}F=p$. 如果对任何 $\alpha\in F$, 均存在 $\beta\in F$ 使得 $\beta^p=\alpha$, 则称 F 为**完全域** (perfect field).

例6.13. *有限域都是完全域.*

命题6.14. *如果 F 是完全域, 则 F 上所有多项式都是可分多项式.*

证明. 如果 F 是完全域, 若

$$f(x)=g(x^p)=a_{np}x^{np}+a_{(n-1)p}x^{(n-1)p}+\cdots+a_px^p+a_0,$$

令 $b_i^p=a_{ip}$, 则 $f(x)=(b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0)^p$ 可约. □

定义6.15. 设 K/F 为代数扩张. 称 $\alpha \in K$ 为**可分元**, 如果它的不可约多项式是可分多项式. 如果所有 $\alpha \in K$ 均是可分元, 则称 K/F 是**可分扩张** (separable extension). 否则称 K/F 为**不可分扩张** (inseparable extension).

由上面的讨论, 我们有

命题6.16. *如果* $\mathrm{char}F = 0$ *或* $\mathrm{char}F = p > 0$ *但* F *是完全域, 则* F *的任意代数扩张均是可分扩张.*

我们将证明

定理6.17. *有限可分扩张都是单扩张.*

§6.1.3 正规扩张

定义6.18. 设 $f(x) \in F[x]$. 称域扩张 K 为 $f(x)$ 在 F 上的**分裂域** (splitting field), 如果下列两条件成立:

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

(2) $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

若只有(1)成立, 称 $f(x)$ 在 K 上**分裂** (split).

引理6.19. *设* $\varphi : F \to \widetilde{F}$ *为域同构,* $f(x) \in F[x]$ *不可约. 记* $\varphi(f(x)) = \widetilde{f}(x)$. *若* K/F, $\widetilde{K}/\widetilde{F}$ *为域扩张,* $\alpha \in K$, $f(\alpha) = 0$ *且* $\widetilde{\alpha} \in \widetilde{K}$, $\widetilde{f}(\widetilde{\alpha}) = 0$, *则存在唯一的域同构* $\varphi_1 : F(\alpha) \to \widetilde{F}(\widetilde{\alpha})$ *使得*

$$\varphi_1(\alpha) = \widetilde{\alpha}, \quad \varphi_1|_F = \varphi. \tag{6.2}$$

证明. 我们有 $F(\alpha) \cong F[x]/(f)$, $\widetilde{F}(\widetilde{\alpha}) \cong \widetilde{F}[x]/(\widetilde{f})$ 且 φ 自然诱导同构 $F[x]/(f) \to \widetilde{F}[\widetilde{x}]/(\widetilde{f})$, 故得到

$$\varphi_1 : F(\alpha) \xrightarrow{\sim} \widetilde{F}(\widetilde{\alpha}), \quad \varphi_1(\alpha) = \widetilde{\alpha} \ \text{ 且 } \varphi_1|_F = \varphi.$$

唯一性由(6.2)立得. □

命题6.20. $f(x)$ *在* F *上的分裂域存在且唯一.*

证明. 存在性: 我们对 $f(x)$ 的次数 n 作归纳. 当 $n=1$ 是显然成立, 此时分裂域即 F. 设对 $<n$ 的多项式均成立. 设 $f(x)$ 的一个不可约因子为 $g(x)$. 若 $g(x)$ 为线性因子, 只要取 $K=F$ 即可, 否则令 $F_1=F[x]/(g(x))=F(\alpha)$, 则 $\frac{f(x)}{g(x)}$ 的次数 $<n$, 故存在 $\frac{f(x)}{g(x)}$ 在 F_1 上的分裂域, 此域也是 $f(x)$ 在F 上的分裂域.

唯一性: 我们只需在如下命题中取 $F=\widetilde{F}, K=\widetilde{K}$ 且 $\varphi=\mathrm{id}$ 即可. □

命题6.21. *设 $\varphi: F\to\widetilde{F}$ 为域同构, $f(x)\in F[x], \widetilde{f}(x)=\varphi(f(x))$. 若 $K,\widetilde{K}$ 分别为 $f(x)$ 与 $\widetilde{f}(x)$ 在 F 上与 $\widetilde{F}$ 上的分裂域, 则存在同构*

$$\psi: K\xrightarrow{\sim}\widetilde{K}\quad \text{且 } \psi|_F=\varphi.$$

证明. 我们对 $[K:F]$ 作归纳. 若 $f(x)$ 只有线性因子, 则 $K=F, \widetilde{K}=\widetilde{F}$, 只需令 $\psi=\varphi$ 即可. 若 $f(x)$ 有次数>1的不可约因子 $g(x)$, 则 $\widetilde{g}(x)=\varphi(g(x))$ 为 $\widetilde{f}(x)$ 的不可约因子. 令 $\alpha\in K$ 为 $g(x)$ 的一个根, $\widetilde{\alpha}\in\widetilde{K}$ 为 $\widetilde{g}(x)$ 的一个根, 则由引理 6.19, 存在同构

$$\varphi_1: F(\alpha)\xrightarrow{\sim}\widetilde{F}(\widetilde{\alpha})\quad \text{且}\varphi_1|_F=\varphi.$$

此时 K (或$\widetilde{K}$) 是 $f(x)$ (或$\widetilde{f}(x)$) 在 $F(\alpha)$ (或$\widetilde{F}(\widetilde{\alpha})$) 上的分裂域, 且 $[K:F(\alpha)]<[K:F]$. 由归纳假设, 存在同构 $\psi: K\xrightarrow{\sim}\widetilde{K}, \psi|_{F(\alpha)}=\varphi_1$, 故此时 $\psi|F=\varphi$. □

定义6.22. 代数扩张 K/F 称为**正规扩张** (normal extension), 如果对任意 $\alpha\in K$, α 在 F 上的最小多项式均在 K 上分裂.

我们将证明如下定理.

定理6.23. *设 K/F 是有限扩张, 则 K/F 是 Galois 扩张当且仅当 K 是某可分多项式 $f(x)\in F[x]$ 的分裂域.*

推论6.24. *如果 K/F 为有限可分扩张, 则 K/F 包含在 F 的某 Galois 扩张中.*

证明. 由于有限可分扩张是单扩张, 令 $K=F(\alpha)$, $f(x)$ 为 α 的最小多项式. 设 L 为 $f(x)$ 在 K 上的分裂域, 则 L 是 $f(x)$ 在 F 上的分裂域, 故由上述引理, L/F 是 Galois 扩张. □

推论6.25. *设 K/F 是 Galois 扩张, L 是其中间域, 则 K/L 也是Galois 扩张.*

证明. 由定理, K 是某可分多项式 $f(x) \in F[x]$ 在 F 上的分裂域, 故也是 $f(x)$ 在 L 上的分裂域, 所以 K/L 是 Galois 扩张. □

§6.1.4 Galois 理论基本定理

下面我们可以陈述 Galois 理论的基本定理.

定理6.26 (Galois 基本定理)**.** *设 K/F 是 Galois 扩张, $G = G(K/F)$ 为其 Galois 群, 则*

(1) 映射

$$\{G\text{的所有子群}\} \longrightarrow \{K/F\text{的所有中间域}\}$$
$$H \longmapsto K^H$$

是一一对应, 其逆为

$$L \longmapsto G(K/L)$$

且若 $H = G(K/L)$, 则

$$[K : L] = |H|, \quad [L : F] = (G : H).$$

(2) 上述对应诱导一一对应

$$\{G\text{的所有正规子群}\} \longleftrightarrow \{K/F\text{的}Galois\text{ 子扩张}L/F\}.$$

此时若 $H = G(K/L)$, 则

$$G(L/F) \cong G/H.$$

习 题

习题1.1. *设 $F = \mathbb{F}_q$ 为 q 元有限域, $(n, p) = 1$, E 为 $x^n - 1$ 在 F 上的分裂域. 证明 $[E : F]$ 等于满足 $n \mid q^k - 1$ 的最小正整数 k.*

习题1.2. 设 F 为域, $f(x)$ 为 $F[x]$ 中 n 次多项式, E 为 $f(x)$ 在 F 上的分裂域. 求证 $[E:F] \mid n!$.

习题1.3. 设 E 为 x^8-1 在 $\mathbb{Q}$ 上的分裂域, 则 $E/\mathbb{Q}$ 是几次扩张? 确定 Galois 群 $\mathrm{Gal}(E/\mathbb{Q})$.

习题1.4. 设 E/F 是域的扩张. 如果对每个元素 $\alpha \in E$, $\alpha \notin F$, α 在 F 上均是超越元素, 则称 E/F 是**纯超越扩张**. 证明:

(1) $F(x)/F$ 是纯超越扩张.

(2) 对于任意域扩张 E/F, 存在唯一的中间域 M, 使得 E/M 为纯超越扩张, 而 M/F 为代数扩张.

习题1.5. 设 F 为特征 0 域, $f(x)$ 为 $F[x]$ 中正次数首一多项式, $d(x) = (f, f')$. 求证: $g(x) = f(x)/d(x)$ 和 $f(x)$ 有同样的根,并且 $g(x)$ 无重根.

习题1.6. 设 F 为特征 p 域, p 为素数, $f(x)$ 为 $F[x]$ 中不可约多项式, 求证: $f(x)$ 的所有根均有相同的重数, 且这个公共重数有形式 $p^n (n \geqslant 0)$.

习题1.7. 设 E/F 为可分扩张, M 为 E/F 的中间域, 求证 E/M 和 M/F 均是可分扩张.

习题1.8. 设 F 为特征 $p > 0$ 域, E/F 为代数扩张. 证明对每个 $\alpha \in E$ 均存在整数 $n \geqslant 0$, 使得 α^{p^n} 在 F 上可分.

习题1.9. 设 $E = \mathbb{F}_p(x, y)$, $F = \mathbb{F}_p(x^p, y^p)$, p 为素数. 证明:

(1) $[E:F] = p^2$;

(2) E/F 不是单扩张;

(3) E/F 有无限多个中间域.

习题1.10. (1) 若 E/F 为代数扩张, F 为完全域, 则 E 也为完全域;

(2) 若 E/F 为有限生成扩张, E 为完全域, 则 F 也为完全域;

(3) 若 E/F 为代数扩张(不必为有限扩张), 问(2) 中结论是否成立?

习题1.11. 设 $E = \mathbb{Q}(\alpha)$, 其中 $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$. 证明:

(1) $\alpha^2 - 2$ 也是 $x^3 + x^2 - 2x - 1 = 0$ 的根;

(2) $E/\mathbb{Q}$ 是正规扩张.

习题1.12. 设 E/F 和 K/F 均是正规扩张, 求证 EK/F 也是正规扩张.

习题1.13. (1) 如果 E/M 和 M/F 均是域的正规扩张, 试问 E/F 是否一定为正规扩张?

(2) 如果 E/F 是正规扩张, M 是它们的中间域, 试问 E/M 和 M/F 是否一定为正规扩张?

习题1.14. 设 E/F 为代数扩张. 证明 E/F 为正规扩张当且仅当对于 $F[x]$ 中任意不可约多项式 $f(x)$, $f(x)$ 在 $E[x]$ 中的所有不可约因子均有相同的次数.

§6.2 方程的 Galois 群

我们首先使用上节理论来讨论方程的 Galois 群.

§6.2.1 三次方程的分裂域

设 F 为域. 为简单起见, 我们假设 $\mathrm{char}F \neq 3$. 设 $f(x) = x^3 + a_2x^2 + a_1x + a_0$. 作移轴变换 $x = x_1 - \frac{a_2}{3}$, 我们不妨假设 $f(x) = x^3 + px + q$. 设 $f(x)$ 为 F 上的不可约可分多项式, 令 K 为 $f(x)$ 的分裂域. 令

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3),$$

则

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 & = & 0 \\ \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 & = & p \\ \alpha_1\alpha_2\alpha_3 & = & -q \end{cases}$$

我们有域扩张

$$F \subseteq F(\alpha_1) \subseteq K = F(\alpha_1, \alpha_2, \alpha_3),$$

其中 $[F(\alpha_1) : F] = 3$ 而 $[K : F(\alpha_1)] = 1$ 或 2. 设 $G = G(K/F)$, 则 G 作用在集合 $\{\alpha_1, \alpha_2, \alpha_3\}$ 上. 若 $\sigma \in G, \sigma(\alpha_i) = \alpha_i$, 则 σ 作用在 K 上为恒等映射, 所以 G 在 $\{\alpha_1, \alpha_2, \alpha_3\}$ 上的作用是忠实作用, 我们有单射 $i : G \hookrightarrow S_3$.

由于 S_3 中唯一的 3 阶子群是 A_3, 故若 $K = F(\alpha_1)$, 则 $G = \{1, \sigma, \sigma^2\}$, 其中 $\sigma : \alpha_1 \mapsto \alpha_2 \mapsto \alpha_3$. 若 $[K : F(\alpha_1)] = 2$, 则 $G \cong S_3$. 令

$$\Delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \in K. \tag{6.3}$$

则若 $G \cong A_3$, 对于 $\tau = (ij) \in S_3$, $\tau\Delta = -\Delta$. 我们有 $F \neq F(\Delta) \subseteq K^{A_3}$. 由 Galois 理论基本定理, $[K^{A_3} : F] = (S_3 : A_3) = 2$, 故 $K^{A_3} = F(\Delta)$. 若 $G = A_3$, 则对任意 $\sigma \in A_3$, $\sigma\Delta = \Delta$, 所以 $\Delta \in F$.

综上所述, 我们有

定理6.27. *设 K 是可分不可约多项式 $f(x) = x^3 + px + q$ 上的分裂域, 则 $[K : F] = 6$ 当且仅当 $D = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2 \in F^\times \backslash F^{\times 2}$. 此时 $\mathrm{Gal}(K/F) \cong S_3$, 否则 $\mathrm{Gal}(K/F) = A_3 \cong \mathbb{Z}/3\mathbb{Z}$.*

§6.2.2 一般情况

设 $\mathrm{char}F \neq 2$, $f(x)$ 为 $F[x]$ 上首一 n 次多项式且无重根. 令 K 是 $f(x)$ 在 F 上的分裂域, 则

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n), \quad \alpha_i \in K,$$

$$K = F(\alpha_1, \ldots, \alpha_n).$$

令 $\mathrm{Gal}(f) = \mathrm{Gal}(K/F)$, 则 $\mathrm{Gal}(f)$ 作用在 $\{\alpha_1, \ldots, \alpha_n\}$ 上, 且作用是忠实的, 即有

$$\mathrm{Gal}(f) \hookrightarrow S_n.$$

我们将 $\mathrm{Gal}(f)$ 视为 S_n 的子群.

定义6.28. $D = D(f) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2$ 称为多项式 f 的**判别式** (discriminant).

由定义立得: 多项式 f 无重根当且仅当其判别式 $D \neq 0$.

命题6.29. *$D \in F$, 且子群 $\mathrm{Gal}(K/F) \cap A_n$ 对应的子域为 $F(\sqrt{D})$. 故 $\mathrm{Gal}(f) \subseteq A_n$ 当且仅当 $\sqrt{D} \in F$.*

证明. 令

$$\Delta = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j) = \sqrt{D},$$

即 $D = \Delta^2$. 若 σ 为奇置换, 则 $\sigma(\Delta) = -\Delta$; 若 σ 为偶置换, 则 $\sigma(\Delta) = \Delta$. 故对所有 $\sigma \in \mathrm{Gal}(K/F)$, $\sigma(D) = D$, 即 $D \in F$ 且 $\mathrm{Gal}(K/F(\Delta)) = \mathrm{Gal}(K/F) \cap A_n$. □

我们下面给出一个计算 $D(f)$ 的方法.

引理6.30. *若 $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$, 则*

$$D=D(f)=(-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}f'(\alpha_i). \tag{6.4}$$

证明. 由 $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$,

$$f'(x)=\sum_{i=1}^{n}\prod_{j\neq i}(x-\alpha_j),$$

所以 $f'(\alpha_i)=\prod\limits_{j\neq i}(\alpha_i-\alpha_j)$, 故

$$D(f)=\prod_{1\leqslant i<j\leqslant n}(\alpha_i-\alpha_j)^2=(-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}f'(\alpha_i).$$

□

例6.31. *若 $f(x)=x^3+px+q$, 则 $f'(x)=3x^2+p$,*

$$D(f)=\prod_{i=1}^{3}(3\alpha_i^2+p)=-4p^3-27q^2. \tag{6.5}$$

引理6.32. *若 $f(x)$ 不可约, 则 $\mathrm{Gal}(f)$ 的作用在 $\{\alpha_1,\ldots,\alpha_n\}$ 上传递.*

证明. 令 $\alpha_1\neq\alpha_2$ 为 f 的两个根, 则存在同构 $\varphi:F(\alpha_1)\to F(\alpha_2)$ 使得 $\varphi|_F=\mathrm{id}$ 且 $\varphi(\alpha_1)=\alpha_2$. 由命题6.21, φ 延拓为 $K\xrightarrow{\psi}K$, 且 $\psi|_F=\mathrm{id}$, 即 $\psi\in\mathrm{Gal}(f),\psi(\alpha_1)=\alpha_2$. □

定理6.33. *如果 $F=\mathbb{Q}$, $f(x)$ 是 p 次有理系数不可约多项式, 且 $f(x)$ 恰好有两个复根, 则 $\mathrm{Gal}(f)=S_p$.*

证明. 令 K 为 $f(x)$ 的分裂域, α 为 $f(x)$ 的一个根, 则 $p=[\mathbb{Q}(\alpha):\mathbb{Q}]\mid[K:\mathbb{Q}]$. 故 $\mathrm{Gal}(f)$ 包含 p 阶元, 但 $\mathrm{Gal}(f)\subseteq S_p$, 故此 p 阶元必为 p轮换.

考虑复共轭在 K 上的限制 σ, 则 σ 固定 $f(x)$ 的所有实根, 且将 $f(x)$ 的两个复根对换, 即 σ 在 S_p 中是一个对换. 由于 S_p 由一个 p 轮换与一个对换生成(参见 §2.1, 特别是命题 2.11 和习题), 故 $\mathrm{Gal}(f)=S_p$. □

注记. 我们可以将 F 改为 $\mathbb{R}$ 的任何子域, 则上述定理仍成立.

§6.2.3 对称多项式

设 E 为域, $x_1,\dots,x_n$ 为未定元. $K=E(x_1,\dots,x_n)$ 为 E 的 n 元有理函数域. 令

$$p_1=\sum_{i=1}^{n}x_i,\quad p_2=\sum_{1\leqslant i<j\leqslant n}x_ix_j,\quad \cdots,\quad p_n=x_1\cdots x_n.$$

定义6.34. 多项式

$$p_k=\sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n}x_{i_1}x_{i_2}\cdots x_{i_k}\tag{6.6}$$

称为 $x_1,\dots,x_n$ 的 k 次**基本对称多项式** (elementary symmetric polynomial).

令 $F=E(p_1,\dots,p_n)$, 则 K 是多项式

$$f(x)=(x-x_1)\cdots(x-x_n)=x^n-p_1x^{n-1}+\cdots+(-1)^np_n\in F[x]$$

的分裂域. 由于 $f(x)$ 无重根, 故 K/F 为 Galois 扩张. 我们下面来决定 $\mathrm{Gal}(K/F)$. 首先 $\mathrm{Gal}(K/F)\hookrightarrow S_n$. 令 $\sigma\in S_n$, 我们定义 σ 在 K 上如下作用:

$$\sigma(f(x_1,\dots,x_n))=f(x_{\sigma(1)},\dots,x_{\sigma(n)}),$$

则 $\sigma\in\mathrm{Aut}K$ 且 $\sigma(p_i)=p_i$, 即 $\sigma\in\mathrm{Gal}(K/F)$, 所以 $S_n\subseteq\mathrm{Gal}(K/F)$, 故

$$\mathrm{Gal}(K/F)\cong S_n.$$

我们有

定理6.35. (1) $E(x_1,\dots,x_n)^{S_n}=E(p_1,\dots,p_n)$.

(2) *若 $f(x_1,\dots,x_n)\in E[x_1,\dots,x_n]$ 被 S_n 固定, 则存在唯一的多项式 $g(p_1,\dots,p_n)\in E[p_1,\dots,p_n]$ 使得*

$$f(x_1,\dots,x_n)=g(p_1,\dots,p_n).$$

注记. 我们称被 S_n 作用固定的多项式为**对称多项式** (symmetric polynomial). 定理中(2)即是说明所有对称多项式均可唯一表为基本对称多项式的多项式.

证明. (1) 由上述说明立即得到.

(2) 首先证明存在性, 我们对 n 作归纳. 当 $n=1$ 时显然. 设对于 $<n$ 成立. 若 $f(x_1,\dots,x_n)$ 被 S_n 固定, 则 $f(x_1,\dots,x_{n-1},0)$ 被 S_{n-1} 固定. 由归纳假设

$$f(x_1,\dots,x_{n-1},0)=g^0(p_1^0,\dots,p_{n-1}^0),$$

其中 $p_i^0=p_i(x_1,\dots,x_{n-1},0)$. 考虑

$$f(x_1,\dots,x_n)-g^0(p_1,\dots,p_{n-1})=f'(x_1,\dots,x-n),$$

则 $f'(x_1,\dots,x_n)$ 被 S_n 固定, 且当 $x_n=0$ 时, $f'(x_1,\dots,x_{n-1},0)=0$, 即 $x_n|f'(x_1,\dots,x_n)$. 由对称性, $x_i|f'(x_1,\dots,x_n)$, 故 $p_n|f'(x_1,\dots,x_n)$. 令 $f'(x_1,\dots,x_n)=p_nh(x_1,\dots,x_n)$, 则

$$f(x_1,\dots,x_n)=g^0(p_1,\dots,p_{n-1})+p_nh(x_1,\dots,x_n),$$

$h(x_1,\dots,x_n)$ 为对称多项式. 注意到

$$\deg g^0(p_1,\dots,p_{n-1})=\deg g^0(p_1^0,\dots,p_{n-1}^0)\leqslant\deg f,$$

我们有 $\deg h\leqslant\deg f$, 对 $\deg f$ 再作归纳即得.

再证唯一性. 我们要证明 $p_1,\dots,p_n$ 不存在代数关系式, 即若

$$\sum a_{i_1,\dots,i_n}p_1^{i_1}\cdots p_n^{i_n}=0,\quad a_{i_1,\dots,i_n}\in E,$$

则 $a_{i_1,\dots,i_n}=0$. 我们对 n 作归纳. $n=1$ 时由 x_1 的超越性即知. 若对小于 n 成立, 则对于 n 情形, 取 $x_n=0$, 则

$$\sum a_{i_1,\dots,i_n}(p_1^0)^{i_1}\cdots(p_n^0)^{i_n}=0,\quad p_i^0=p_i(x_1,\dots,x_{n-1},0).$$

由归纳假设 $a_{i_1,\dots,i_{n-1},0}=0$, 故

$$\sum a_{i_1,\dots,i_n}p_1^{i_1}\cdots p_n^{i_n}=p_n\sum_{i_n\geqslant1}a_{i_1,\dots,i_n}p_1^{i_1}\cdots p_{n-1}^{i_{n-1}}p_n^{i_n-1}.$$

再作一次归纳(对 $\sum a_{i_1,\dots,i_n}p_1^{i_1}\cdots p_n^{i_n}$ 最高项次数作归纳), 即知对 $i_n\geqslant1$ 时, $a_{i_1,\dots,i_n}=0$. □

定理6.36. 设 $t_1,\dots,t_n$ 为未定元, $F=E(t_1,\dots,t_n)$,

$$f(x)=x^n-t_1x^{n-1}+t_2x^{n-2}+\cdots+(-1)^nt_n\in F[x].$$

则 $f(x)$ 是 F 上的不可约可分多项式. 令 K 为 $f(x)$ 在 F 上的分裂域, 则

$$\mathrm{Gal}(K/F)\cong S_n.$$

证明. 设 $s_1,\dots,s_n$ 为 $f(x)$ 的根, 则

$$F(x)=x^n-t_1x^{n-1}+t_2x^{n-1}+\cdots+(-1)^nt_n=(x-s_1)\cdots(x-s_n),$$

故

$$K=E(t_1,\dots,t_n)(s_1,\dots,s_n)=E(s_1,\dots,s_n).$$

令 $\tilde{K}=E(x_1,\dots,x_n)$, 其中 $x_1,\dots,x_n$ 为未定元, $\tilde{F}=E(p_1,\dots,p_n)$, 则由定理 6.35, $\mathrm{Gal}(\tilde{K}/\tilde{F})=S_n$. 由于 $t_1,\dots,t_n$ 为未定元, 故存在环同态

$$\sigma:E[t_1,\dots,t_n]\to E[p_1,\dots,p_n],\quad t_i\mapsto p_i.$$

由于 $x_1,\dots,x_n$ 为未定元, 故存在环同态

$$\tau:E(x_1,\dots,x_n)\to E(s_1,\dots,s_n),\quad x_i\mapsto s_i.$$

则 $\tau\sigma(t_i)=\tau(p_i)=t_i$, 即 $\tau\sigma=1$, 故 σ 为单同态. 又显然 σ 为满同态, 故 σ 为同构, 它诱导同构 $\sigma:F\to\tilde{F}$. 由命题6.21, σ 扩充为域同构 $\rho:K\to\tilde{K}$, 故 $\mathrm{Gal}(K/F)\xrightarrow{\sim}\mathrm{Gal}(\tilde{K}/\tilde{F})=S_n$. 由于

$$\begin{aligned}[K:F]&=[F(s_1,\dots,s_n):F]\\&=\prod_{i=1}^{n}[F(s_1,\dots,s_i):F(s_1,\dots,s_{i-1})]\leqslant n!,\end{aligned}$$

故 $[K:F]=|\mathrm{Gal}(K/F)|=n!$, $f(x)$ 的根两两不同, 且 $[F(s_1):F]=n$, 故 $f(x)$ 为不可约可分多项式. □

习　　题

习题2.1. 设 F 为实数域 $\mathbb{R}$ 的子域. $f(x)$ 为 $F[x]$ 中三次不可约多项式. 证明若 $d(f)>0$, 则 $f(x)$ 有三个实根; 若 $d(f)<0$, 则 $f(x)$ 只有一个实根.

习题2.2. 设 F 是特征为 2 的域. 求 $f(x)$ 在 F 上的*Galois*群, 其中

(1) $f(x)=x^3+x+1$; (2) $f(x)=x^3+x^2+1$.

习题2.3. 确定 $f(x)$ 在域 F 上的 *Galois* 群, 其中

(1) $f(x)=x^4-5,\ F=\mathbb{Q},\ \mathbb{Q}(\sqrt{5}),\ \mathbb{Q}(\sqrt{-5})$.

(2) $f(x)=x^4-10x^2+4,\ F=\mathbb{Q}$.

(3) $f(x)=x^5-6x+3,\ F=\mathbb{Q}$.

习题2.4. 设 p 为素数, $a\in\mathbb{Q}$, x^p-a 为 $\mathbb{Q}[x]$ 中不可约多项式. 证明 x^p-a 在 $\mathbb{Q}$ 上的 *Galois* 群同构于 p 元域 $\mathbb{F}_p$ 上 2 阶一般线性群 $\mathrm{GL}_2(\mathbb{F}_p)$ 的子群

$$\left\{\begin{pmatrix}k & l\\ 0 & 1\end{pmatrix} \mid l,k\in\mathbb{F}_p, 0\neq k\in\mathbb{F}_p\right\}.$$

习题2.5. 证明 $\mathbb{Q}(\sqrt[4]{2}(1+\sqrt{-1})/\mathbb{Q}$ 是四次扩张; 并求出它的 *Galois*群.

习题2.6. 任一有限群均是某个域上可分多项式的 *Galois*群.

§6.3 Galois 扩张的一些例子

在本节, 我们将详细讲述 Galois 扩张的一些例子.

§6.3.1 分圆扩张

设 F 为域, n 为正整数, 且若 $\mathrm{char}F=p>0$, 则 $p\nmid n$. 考虑多项式 $f(x)=x^n-1$ 在 F 上的分裂域 K, 我们令 ζ_n 为 $f(x)$ 的一个根且对任意 $1\leqslant i<n$, $\zeta_n^i\neq 1$, 即 ζ_n 是所谓 n 次**本原单位根** (primitive roots of unity), 则 $\{\zeta_n^i \mid 0\leqslant i\leqslant n-1\}$ 为 $f(x)$ 的所有根. 故 $K=F(\zeta_n)$, 多项式

$$x^n-1=\prod_{i=0}^{n-1}(x-\zeta_n^i) \tag{6.7}$$

为可分多项式.

对于任意 $\sigma \in \mathrm{Gal}(K/F)$, σ 由 ζ_n 的像唯一确定. 设 $\sigma(\zeta_n) = \zeta_n^a$, 则对任意 $1 \leqslant i < n$, $\zeta_n^i \neq 1$, 由 $\zeta_n^i \neq 1$ 知 $\zeta_n^{ai} \neq 1$, 即 $(a, n) = 1$. 我们有群同态

$$\mathrm{Gal}(K/F) \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto a \mod n.$$

此同态显然为单同态, 故 $\mathrm{Gal}(K/F)$ 可视为 $(\mathbb{Z}/n\mathbb{Z})^\times$ 的一个子群.

例6.37. 设 $F = \mathbb{Q}, n = p^m$, 其中 $m \in \mathbb{N}, p$ 为奇素数. 我们证明

$$[\mathbb{Q}(\zeta_{p^m}) : \mathbb{Q}] = \varphi(p^m) = |(\mathbb{Z}/p^m\mathbb{Z})^\times|, \tag{6.8}$$

故 $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^m}) : \mathbb{Q}) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$.

事实上, ζ_{p^m} 满足多项式

$$\Phi_{p^m}(x) = \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} = x^{p^{m-1}(p-1)} + x^{p^{m-1}(p-2)} + \cdots + x^{p^{m-1}} + 1.$$

又由 *Eisenstein* 判别法 $\Phi_{p^m}(x+1)$ 是不可约多项式, 故 $\Phi_{p^m}(x)$ 也不可约. 所以

$$[\mathbb{Q}(\zeta_{p^m}) : \mathbb{Q}] = \deg \Phi_{p^m}(x) = \varphi(p^m).$$

注记. 可以证明, 对一般的 n,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

取 $n = p$ 为奇素数, 我们来讨论一下 $\mathbb{Q}(\zeta_p)$ 的子域. 此时 $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ 为 $p-1$ 阶循环群. 令 σ 为其生成元, 则 $\sigma^{\frac{p-1}{2}} = -1$ 是 Galois 群中唯一 2 阶元, 因此必为复共轭在 $\mathbb{Q}(\zeta_p)$ 上的限制. 子群 $\{1, -1\}$ 对应的子域必包含 $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. 另一方面, ζ_p 在 $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ 上的不可约多项式 $x^2 - (\zeta_p + \zeta_p^{-1})x + 1$ 为二次式. 故 $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p + \zeta_p^{-1})] = 2$. 又由于 $[\mathbb{Q}(\zeta_p) : L] = 2$, 所以 $L = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

另一方面, $\langle \sigma^2 \rangle$ 是 $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ 的唯一指数为 2 的子群, 它对应于 $\mathbb{Q}$ 的一个二次扩张 M. 考虑

$$f(x) = x^{p-1} + x^{p-2} + \cdots + 1 = \prod_{i=1}^{p-1}(x - \zeta_p^i),$$

则

$$D(f)=(-1)^{(p-1)/2}\prod_{i=1}^{p-1}f'(\zeta_p^i).$$

由 $f(x)(x-1)=x^p-1$ 知 $f'(\zeta_p^i)(\zeta_p^i-1)=p\zeta_p^{(p-1)i}$, $f'(\zeta_p^i)=p\zeta_p^{-i}/(\zeta_p^i-1)$,

$$D=(-1)^{(p-1)/2}\prod_{i=1}^{p-1}f'(\zeta_p^i)=(-1)^{(p-1)/2}p^{p-2}\notin\mathbb{Q}^2,$$

故 $M=\mathbb{Q}(\sqrt{D})=\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$.

命题6.38. *设 p 为素数, 则正 p 边形可以尺规作出当且仅当 $p=2^{2^n}+1$ 为 Fermat 素数.*

证明. 推论 5.34 已经证明其必要性. 反之, 若 $p=2^{2^n}+1$ 为 Fermat 素数, 则 $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})\cong\mathbb{Z}/2^{2^n}\mathbb{Z}$ 为 2^{2^n} 阶循环群. 由 Galois 理论, 存在 $\mathbb{Q}=K_0\subseteq K_1\subseteq\cdots\subseteq K_{2^n}=\mathbb{Q}(\zeta_p)$, 使得 $[K_{i+1}:K_i]=2$, 故 $\zeta_p+\zeta_p^{-1}$ 可构造. □

§6.3.2 Kummer扩张

设 F 为域, $\zeta_n\in F$, 且如果 $\mathrm{char}F=p$, 则 $p\nmid n$. 对于元素 $a\in F$, 考虑 $f(x)=x^n-a$ 的分裂域 K. 如果 $\alpha=\sqrt[n]{a}$ 为 $f(x)$ 的一个根, 则 $\{\zeta_n^i\alpha\mid 0\leqslant i\leqslant n-1\}$ 为 $f(x)$ 的所有根, 即

$$f(x)=x^n-a=\prod_{i=0}^{n-1}(x-\zeta_n^i\alpha)$$

为可分多项式. 故 $K=F(\alpha,\zeta_n)$ 是 F 的 Galois 扩张, 我们称此形式的 Galois 扩张为 **Kummer 扩张** (Kummer extension).

若 $\sigma\in\mathrm{Gal}(K/F)$, 则 $\sigma(\alpha)=\zeta_n^i\alpha$ 对某个 $0\leqslant i\leqslant n-1$ 成立. 我们定义映射

$$\begin{aligned}\varphi:\mathrm{Gal}(K/F)&\longrightarrow\mathbb{Z}/n\mathbb{Z}\\ \sigma&\longmapsto i\mod n.\end{aligned}$$

由 $\sigma\tau(\alpha)=\sigma(\tau(\alpha))$ 可知 φ 为群的单同态, 故 $\mathrm{Gal}(K/F)$ 是循环群 $\mathbb{Z}/n\mathbb{Z}$ 的一个子群.

§6.3.3 有限域的扩张

设 $F=\mathbb{F}_q$ 为 q 元有限域, 则 $q=p^f$, p 为素数. 如 $[K:F]$ 为 n 次有限扩张, 则 $K\cong\mathbb{F}_{q^n}$ 为 q^n 元域, 它是多项式 $x^{q^n}-x$ 的分裂域, 故 K/F 是 Galois 扩张. 由有限域的基本定理, $K/\mathbb{F}_p$ 为 nf 次循环群, 它的一个生成元是 Frobenius 映射 $\sigma_p: x\mapsto x^p$. 我们有

$$\begin{aligned}\mathrm{Gal}(K/F)&=\ker(\mathrm{Gal}(K/\mathbb{F}_p)\to\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p))\\&=\langle\sigma_p^f\rangle\cong\mathbb{Z}/n\mathbb{Z}.\end{aligned}$$

习　　题

习题3.1. 设 F 为域, $c\in F$, p 为素数.

(1) 当 $\mathrm{char}F=p$ 时, 证明 x^p-c 在 $F[x]$ 中不可约当且仅当 x^p-c 在 F 中无根.

(2) 当 $\mathrm{char}F\neq p$ 时, 证明 F 有 p 个不同的 p 次单位根. 由此证明 x^p-c 在 $F[x]$ 中不可约当且仅当 x^p-c 在 F 中无根.

习题3.2. 试求出 *Kummer* 扩张的 *Galois* 群.

习题3.3. 设 E 为 x^4-2 在 $\mathbb{Q}$ 上的分裂域.

(1) 试求出 $E/\mathbb{Q}$ 的全部中间域.

(2) 试问哪些中间域是 $\mathbb{Q}$ 的 *Galois* 扩张? 哪些域彼此共轭?

习题3.4. 设 E 为 x^4-2 在 $\mathbb{F}_5$ 上的分裂域. 试求出 $E/\mathbb{F}_5$ 的 *Galois* 群和全部中间域.

习题3.5. 对于 $n=8,9,12$, 求出 $G=\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, 并列出 G 的全部子群和它们对应的 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 的中间域.

习题3.6. 设 $n\geqslant 2$ 为正整数, 证明 $\mathbb{Q}(\zeta_n)\cap\mathbb{R}=\mathbb{Q}(\zeta_n+\zeta_n^{-1})$.

习题3.7. 设 p 是素数, $(\frac{a}{p})$ 为 *Legendre* 符号. 设高斯和

$$g=\sum_{a\in\mathbb{F}_p}\zeta_p^a\Big(\frac{a}{p}\Big). \tag{6.9}$$

证明:

(1) $\sum\limits_{a\in\mathbb{F}_p}\zeta_p^a=0$.

(2) $g\cdot\overline{g}=p$, 其中 $\overline{g}$ 是 g 的复共轭.

(3) $g=\pm\sqrt{(-1)^{(p-1)/2}p}$.

(4) $\mathbb{Q}(\zeta_p)$ 有唯一的二次子域 $K=\mathbb{Q}(g)$.

§6.4 方程的根式可解性

Galois 理论的最初最重要的应用是用来回答一般 n 次方程是否有求根公式这一古典数学问题. Galois 的深刻思想即是将此问题通过 Galois 理论基本定理, 转换为群论问题.

我们首先有定义:

定义6.39. 域的扩张称为**根式扩张** (radical extension)是指 $K=F(d)$, 其中 $d^n=a$ 对某个 $a\in F$ 成立, 换言之, 即 $K=F(\sqrt[n]{a}),a\in F$.

定义6.40. 设 F 为域, $f(x)$ 为 $F[x]$ 上首一多项式, $\deg f\geqslant 1$, K 为 $f(x)$ 在 F 上的分裂域. 方程 $f(x)=0$ 称为 F 上**根式可解** (radical solvable)是指存在根式扩张序列

$$F=F_0\subseteq F_1\subseteq\cdots\subseteq F_n$$

使得 $K\subseteq F_n$.

若存在根式扩张序列, 使得 $F_1=F,F_n=K$, 称 K/F 有**根式扩张塔** (radical extension towel).

本节的主要定理是:

定理6.41. 如果 $\mathrm{char}F=0$, $f(x)$ 在 F 上根式可解当且仅当 $f(x)$ 在 F 上的 *Galois* 群 $\mathrm{Gal}(f)$ 为可解群.

为证明此定理, 我们首先回顾一下可解群的定义和性质.

- 有限群 G 是**可解群** (solvable group)是指存在正规子群序列

$$G_n=\{1\}\lhd G_{n-1}\lhd\cdots\lhd G_1=G$$

使得 G_i/G_{i+1} 均是阿贝尔群.

- 由有限阿贝尔群的结构定理, 上述条件等价于 G_i/G_{i+1} 是素数阶循环群.
- G 为可解群当且仅当对某个正规子群 $N \lhd G$, N 与 G/N 均为可解群.
- 可解群的子群和商群均是可解群.

由于对称群 S_n 当 $n \geqslant 5$时不是可解群, 当 $n \leqslant 4$ 时为可解群. 由上述定理, 我们立刻有 Galois 的著名定理.

定理6.42. *设* $\mathrm{char}F = 0$, $n \geqslant 5$, $t_1, \ldots, t_n$ *为未定元, 则一般方程*

$$f(x) = x^n - t_1 x^{n-1} + \cdots + (-1)^n t_n = 0$$

在域 $F(t_1, \ldots, t_n)$ *上根式不可解.*

证明. 我们在定理 6.36 已经证明 $\mathrm{Gal}(f) \cong S_n$. □

我们假设 $\mathrm{char}F = 0$. 为了证明定理 6.41, 我们需要有几个引理.

引理6.43. *如果* $\zeta_p \in F$, K/F *是* p *次循环扩张, 则* K/F *为 Kummer 扩张, 即有* $K = F(d), d^p \in F$.

证明. 取 $c \in K \backslash F$, 则 $K = F(c)$. 令 $\mathrm{Gal}(K/F) = \langle \sigma \rangle$, 则 $\sigma^p = 1$. 令 $c_i = \sigma^{i-1}(c) \in K$. 令

$$d_i = c_1 + c_2 \zeta_p^i + \cdots + c_p \zeta_p^{(p-1)i} \in K,$$

则 $\sigma(d_i) = \zeta_p^{-i} d_i$, 故有 $\sigma(d_i^p) = d_i^p$. 由于

$$(d_1, \cdots, d_p) = (c_1, \cdots, c_p) \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \zeta_p & \zeta_p^2 & \cdots & \zeta_p^{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_p^{p-1} & \zeta_p^{2(p-1)} & \cdots & \zeta_p^{(p-1)^2} \end{pmatrix} = (c_1, \cdots, c_p) A.$$

而 $A \in M_p(F)$ 且 $\det A \neq 0$ (由范德蒙行列式的性质). 故

$$(c_1, \cdots, c_p) = (d_1, \cdots, d_p) A^{-1}.$$

由于 $c_1, \cdots, c_p$ 不在 F 中, 故一定存在 $d_i \in K$ 但 $d_i \notin F$. 取 $d = d_i$, 则 $K = F(d), d^p \in F$. □

引理6.44. *设 E/F 为域的扩张, 则 $f(x)$ 在 E 上的 Galois 群同构于其在 F 上的 Galois 群的子群.*

证明. 设 $K = F(\alpha_1, \ldots, \alpha_n)$ 是 $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ 在 F 上的分裂域, 则 $KE = E(\alpha_1, \ldots, \alpha_n)$ 为 $f(x)$ 在 E 上的分裂域. 对于 $\sigma \in \mathrm{Gal}(KE/E)$,

$$\sigma(\alpha_i) = \alpha_j \in \{\alpha_1, \ldots, \alpha_n\},$$

故 $\sigma(K) = K$, 所以

$$\varphi : \mathrm{Gal}(KE/E) \to \mathrm{Gal}(K/F), \quad \sigma \mapsto \sigma|_K$$

为群同态. 若 $\varphi(\sigma) = 1$, 则 $\sigma|_K = \mathrm{id}$. 又由于 $\sigma|_E = \mathrm{id}$, 故 $\sigma|_{KE} = \mathrm{id}$, 即 $\sigma = 1$. 故 φ 为单同态. □

注记. 若 K/F 为 Galois 扩张, E/F 为域扩张. 同样的证明可知 KE/E 为 Galois 扩张且 $\mathrm{Gal}(KE/E) \leqslant \mathrm{Gal}(K/F)$.

引理6.45. *若 E/F 为有限扩张, N 为 E 在 F 上的正规闭包, 则 E/F 包含在 F 的根式扩张塔中当且仅当 N/F 包含在 F 的根式扩张塔中.*

证明. 充分性显然. 反之, 若存在根式扩张塔

$$F = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$$

使得 $F_n \supseteq E$. 设 $F_i = F_{i-1}(d_i), d_i^{m_i} \in F_{i-1}$. 我们只需证明 F_n 在 F 上的正规闭包 M/F 存在根式扩张塔.

设 $f_i(x)$ 是 d_i 在 F 上的不可约多项式, $d_{i1} = d_i, \ldots, d_{ij}$ 为它的所有根, 则 $M = F(d_ij)$. 令 $M_1 = F_1$, $M_i = M_{i-1}(d_{i1}, \ldots, d_{ij})$. 只要证明 M_i/M_{i-1} 存在根式扩张塔即可. 对于 $i = 2$, 我们有

$$F_1 \subseteq F(d_2) \subseteq F(d_{21}, d_{22}) \subseteq \cdots \subseteq F(d_{2j}) = M_2.$$

由于 $d_{2j}^{n_2} \in F_1$, 上述域扩张序列为根式扩张塔. 对一般的 i, 若 $d_{ij} = \sigma(d_i)$, 其中 $\sigma \in \mathrm{Gal}(M/F_1)$, 则 $\sigma(F_{i-1})(d_{ij})/\sigma(F_{i-1})$ 为根式扩张. 由于 $M_{i-1} \supseteq \sigma(F_{i-1})$, 故 $M_{i-1}(d_{ij})/M_{i-1}$ 为根式扩张, 即有 M_i/M_{i-1} 由根式扩张塔. □

有了如上准备, 我们可以证明定理 6.41.

定理 6.41 的证明. 设 E 是 $f(x)$ 在 F 上的分裂域. 设 $E \subseteq K$ 且 K/F 有根式扩张塔

$$F = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n = K,$$

其中 $F_i = F_{i-1}(d_i)$, $d_i^{n_i} \in F_{i-1}$. 我们要证明 $\mathrm{Gal}(f) = \mathrm{Gal}(E/F)$ 可解.

首先由引理 6.45, 我们可以假设 K/F 为 Galois 扩张, 故只需证明 $\mathrm{Gal}(K/F)$ 为可解群. 令 N 为所有 n_i 的乘积, $\zeta = \zeta_n$, 令 $F_i' = F_i(\zeta)$, 则 F_1'/F_1 为分圆扩张, F_i'/F_i 均为 Kummer 扩张. 它们均是 Galois 扩张, 且其 Galois 群是阿贝尔群. 由于 K/F 是 Galois 扩张, K 是某多项式 $g(x)$ 在 F 上的分裂域, 则 $K(\zeta)$ 是 $g(x)\cdot(x^N-1)$ 在 F 上的分裂域, 故 $K(\zeta)/F = F_n'/F$ 也是 Galois 扩张. 我们有

$$\{1\} = \mathrm{Gal}(F_n'/F_n') \lhd \cdots \lhd \mathrm{Gal}(F_n'/F_1') \lhd \mathrm{Gal}(F_n'/F_1)$$

为可解列, 故 $\mathrm{Gal}(K(\zeta)/F)$ 为可解群. 因此其商群 $\mathrm{Gal}(K/F)$ 与 $\mathrm{Gal}(E/F)$ 也是可解群.

反之, 若 $\mathrm{Gal}(E/F)$ 为可解群. 令 $n = [E:F]$, $\zeta = \zeta_n$, 则由引理 6.44, $E(\zeta)/F(\zeta)$ 是 Galois 扩张且 $\mathrm{Gal}(E(\zeta)/F(\zeta))$ 为可解群 $\mathrm{Gal}(E/F)$ 的子群. 于是有正规咧

$$\{1\} \lhd H_{n-1} \lhd \cdots \lhd H_1 = \mathrm{Gal}(E(\zeta)/F(\zeta)),$$

其中 H_i/H_{i-1} 为素数 p_i 阶循环群. 令其对应的域扩张为

$$F_1 = F(\zeta) \subseteq F_2 \subseteq \cdots \subseteq F_n = E(\zeta).$$

则 $[F_i : F_{i-1}] = p_i | n$. 由引理 6.43, $F_i = F_{i-1}(d_i)$ 为根式扩张, 又显然 F_1/F 为根式扩张,

$$F \subseteq F_1 \subseteq \cdots \subseteq F_n = E(\zeta)$$

为根式扩张塔, 所以 $f(x) = 0$ 在 F 上根式可解. □

习　　题

习题4.1. 将 $\cos 20^\circ$ 和 $\cos \frac{360^\circ}{7}$ 表示成根式形式.

习题4.2. 试导出三次方程的求根公式*(Cardano* 公式*):* 设 F 是特征 0 域,

$$f(x)=x^3-t_1x^2+t_2x-t_3\in F(t_1,t_2,t_3)[x]$$

的三个根为

$$\begin{aligned}x_1&=\frac{t_1}{3}+\alpha+\beta,\\ x_2&=\frac{t_1}{3}+\omega\alpha+\omega^2\beta,\\ x_3&=\frac{t_1}{3}+\omega^2\alpha+\omega\beta,\end{aligned}$$

其中 $p=-\frac{1}{3}t_1^2+t_2,\ q=-\frac{2}{27}t_1^3+\frac{1}{3}t_1t_2-t_3,$

$$\begin{aligned}\alpha&=\sqrt[3]{-\frac{q}{2}+\sqrt{(q/2)^3+(p/2)^3}},\\ \beta&=\sqrt[3]{-\frac{q}{2}-\sqrt{(q/2)^3+(p/2)^3}},\quad \alpha\beta=-p/3.\end{aligned}$$

习题4.3. 求下列方程在复数域 $\mathbb{C}$ 中的根*:*

(1) $x^3-2x+4=0$*;*

(2) $x^3-15x+4=0$*;*

(3) $x^4-2x^3-8x-3=0$.

习题4.4. 证明方程 $x^p-x-t=0$ 在 $\mathbb{F}_p(t)$ 上根式不可解, 但是多项式 x^p-x-t 在 $\mathbb{F}_p(t)$ 上的 *Galois* 群是循环群. 这表明定理 *6.41* 中 "$\mathrm{char}F=0$"的条件一般是不能去掉的.

§6.5 主要定理的证明

在本书, 我们将给出第 §6.1 节中所述的几个基本定理的证明.

定理6.46. 有限可分扩张是单扩张, 即若 K/F 为有限可分扩张, 则存在 $\gamma\in K, K=F(\gamma)$.

证明. 令 $K=F(\alpha_1,\ldots,\alpha_n)$.

若 F 为有限域, 则 K 也是有限域. 取 x 为循环群 $K^\times$ 的生成元, 则 $K=F(x)$. 下面我们假设 F 为无限域. 由归纳假设, 我们只要证明 $F(\alpha,\beta)=F(\gamma)$ 即可.

令 γ 在 F 上的不可约多项式为 $f(x)$, β 在 F 上的不可约多项式为 $g(x)$. 记

$$f(x)=\prod_{i=1}^{r}(x-\alpha_i),\quad \alpha_1=\alpha,$$
$$g(x)=\prod_{j=1}^{s}(x-\beta_j),\quad \beta_1=\beta,$$

其中 α_i,β_j 在 $f(x)g(x)$ 的某个分裂域 E 中, $F(\alpha,\beta)/F$ 为可分扩张, α_i 两两不同, β_j 也两两不同. 由于对于 $(i,j)\neq(1,1)$,

$$\alpha_i+x\beta_j=\alpha_1+x\beta_1$$

最多有一个解, 故存在 $c\in F$, 使得对所有 $(i,j)\neq(1,1)$,

$$\alpha_i+c\beta_j\neq\alpha_1+c\beta_1.$$

令 $\gamma=\alpha+c\beta$, 首先显然有 $F(\alpha,\beta)\supseteq F(\gamma)$. 另一方面, 由 $g(\beta)=0, f(\gamma-c\beta)=0$, 故 $g(x)$ 与 $f(\gamma-cx)$ 在 $F(\gamma)[x]$ 上有公共根. 但由 $\alpha_i+c\beta_j\neq\alpha_1+c\beta_1$, 它们在 E 上只有一个公共根, 故

$$(g(x),f(\gamma-cx))=x-\beta\in F(\gamma)[x],$$

即 $\beta\in F(\gamma)$, $\alpha=\gamma-c\beta\in F(\gamma)$, 所以 $F(\alpha,\beta)\subseteq F(\gamma)$. □

命题6.47. *设 $G\subseteq\mathrm{Aut}(K)$ 为有限群, $F=K^G$, $\beta\in K$. 设 $\{\beta_1=\beta,\dots,\beta_r\}=G\beta$ 为群 G 作用下 β 的轨道, 则 β 在 F 上代数且其在 F 上的不可约多项式为 $g(x)=(x-\beta_1)\cdots(x-\beta_r)$.*

证明. 首先对所有 $\sigma\in G$, 由 $\sigma(g(x))=g(x)$ 知 $g(x)\in F[x]$. 故 β 在 F 上代数. 令 $f(x)$ 为 β 在 F 上的不可约多项式, 则 $f(x)|g(x)$.

另一方面, 由于 $(x-\beta)|f(x)$, 故 $(x-\beta_i)|f(x)$, 所以 $g(x)|f(x)$. 故 $f(x)=g(x)$. □

例6.48. *令 $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$, $G=\{1,\sigma,\tau,\sigma\tau\}$, 其中*

$$\sigma(\sqrt{2})=\sqrt{2},\quad \sigma(\sqrt{3})=-\sqrt{3},$$
$$\tau(\sqrt{2})=-\sqrt{2},\quad \tau(\sqrt{3})=\sqrt{3}.$$

则 $\beta=\sqrt{2}+\sqrt{3}$ 的轨道为 $\{\pm\sqrt{2}\pm\sqrt{3}\}$. β 在 $\mathbb{Q}=K^G$ 上的最小多项式为

$$\begin{aligned} g(x) &= (x+\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x-\sqrt{2}-\sqrt{3}) \\ &= x^4-10x^2+1. \end{aligned}$$

推论6.49. *如果 K/F 是 Galois 扩张, $g(x)\in F[x]$ 不可约. 若 g 在 K 上有根, 则 g 在 K 上分裂且 $g(x)$ 可分. 即 K/F 为正规可分扩张.*

证明. 由 K/F 为 Galois 扩张, $F=K^G$. 若 $\beta\in K$ 为 $g(x)$ 的根, 由上述命题, $g(x)=(x-\beta_1)\cdots(x-\beta_r)$ 为可分多项式, 其根 $\beta_i\in G\beta\subseteq K$. □

定理6.50. (1) *若 K/F 为有限扩张, 则 $|\mathrm{Gal}(K/F)|\leqslant[K:F]$.*

(2) *设 $G\subseteq\mathrm{Aut}(K)$ 为有限群, $F=K^G$, 则 $[K:F]\leqslant|G|$. 若 K/F 可分, 则等号成立.*

注记. (1) 即第 §6.1 节定理, (2) 是所谓的 Artin 引理.

证明. (1) 令 $K=F(\alpha_1,\ldots,\alpha_n)$, Ω 为 K 的代数闭包, 则 $F(\alpha_1)\hookrightarrow\Omega$ 且保持 F 不动的嵌入由 α_1 在 F 上的不可约多项式的根决定, 即 F-嵌入的个数$\leqslant[F(\alpha_1):F]$. 由归纳知 K 到 Ω 的 F-嵌入的个数$\leqslant[K:F]$. 故 K 的 F-自同构个数小于或等于 $[K:F]$, 即 $|\mathrm{Gal}(K/F)|\leqslant[K:F]$.

(2) 设 $m>n$, $u_1,\ldots,u_m\in K$. 我们证明它们 F-线性相关. 设 $G=\{g_1=1,\ldots,g_n\}$. 由于 $m>n$, 线性方程组

$$\sum_{j=1}^{m}g_i(u_j)x_j=0\quad(1\leqslant i\leqslant n) \tag{6.10}$$

有非平凡解 $(b_1,\ldots,b_m)\neq(0,\ldots,0)$. 设 $(b_1,\ldots,b_m)$ 为所有非零解中非零分量最少的, 调整 u_j 与 x_j 的次序, 不妨设 $b_1\neq0$, 则 $(1,b_1^{-1}b_2,\ldots,b_1^{-1}b_m)$ 也是方程组的解, 故不妨设 $b_1=1$.

如果 $b_j\in F$ 对所有 j 成立, 取 $i=1$, 则 $u_1,\ldots,u_m$ 线性相关. 如果存在 $b_j\notin F$, 不妨设 $b_2\notin F=K^G$, 则存在 $g_k\in G$, $g_k(b_2)\neq b_2$. 由于

$$\sum_{i=1}^{m}g_kg_i(u_j)g_k(b_j)=0\quad(1\leqslant i\leqslant n),$$

故 $\{1 = g_k(b_1), g_k(b_2), \ldots, g_k(b_m)\}$ 也是方程组(6.10)的解, 所以 $\{0, g_k(b_2)-b_2, \ldots, g_k(b_m) - b_m\}$ 是(6.10)的非零解, 且非零分量个数比 $(b_1, \ldots, b_m)$ 少, 矛盾.

如果 K/F 为可分扩张. 由单扩张定理, $K = F(\beta)$. 则 β 在 G 作用下的固定子群将 K 固定, 故为 $\{1\}$. 所以 $|G\beta| = n$ 为 β 在 F 上的次数, 即 $[K : F]$. □

推论6.51. *如果 K/F 为可分扩张, 则*

$$|\mathrm{Gal}(K/F)| \mid [K : F].$$

证明. 令 $G = \mathrm{Gal}(K/F) \leqslant \mathrm{Aut}K$, 则 $K^G \supseteq F$, K/K^G 为可分扩张, 故 $|G| = [K : K^G] \mid [K : F]$. □

推论6.52. *若 $G \subseteq \mathrm{Aut}(K)$ 为有限群, $F = K^G$, 则 K/F 是 Galois 扩张且 $\mathrm{Gal}(K/F) = G$.*

证明. 首先由于 G 中元素均是 K 的 F-自同构, $G \leqslant \mathrm{Gal}(K/F)$. 其次, 由命题6.47, K 上任何元素在 F 上均可分, 故 K/F 为可分扩张, 故

$$|\mathrm{Gal}(K/F)| \leqslant [K : F] = |G|,$$

故 $G = \mathrm{Gal}(K/F)$, K/F 为 Galois 扩张. □

定理6.53. *设 K/F 为有限扩张, 则下列条件等价:*

(1) *K/F 为 Galois 扩张.*

(2*a*) *K 是 $F[x]$ 上某些不可约可分多项式的分裂域.*

(2*b*) *K 是 $F[x]$ 上某个可分多项式的分裂域.*

(2*c*) *K 是正规可分扩张.*

(3*a*) *$F = K^{\mathrm{Gal}(K/F)}$.*

(3*b*) *G 是 $\mathrm{Aut}(K)$ 的有限子群, 且 $F = K^G$.*

证明. (1) $\Longrightarrow$ (2c) 是定理 6.50 的推论.

(2c) $\Longrightarrow$ (2b) $\Longrightarrow$ (2a) 显然.

(3b) $\Longrightarrow$ (1) 即推论 6.52.

(3a) $\Longrightarrow$ (3b) 显然.

(1) $\Longrightarrow$ (3a) 即推论 6.9.

(2a) $\Longrightarrow$ (1) 在下述命题中取 $F=\tilde{F}$, $\varphi=\mathrm{id}$, $f(x)$ 为不可约可分多项式, $K=\tilde{K}$ 即得. □

命题6.54. *设 $\varphi: F\to\tilde{F}$, $f(x)\in F[x]$, $f(x)\neq 0$, $\tilde{f}(x)=\varphi(f(x))\in\tilde{F}[x]$. 设 $f(x),\tilde{f}(x)$ 的不可约因子无重根, K 与 $\tilde{K}$ 分别为 $f(x)$ 与 $\tilde{f}(x)$ 在 F 与 $\tilde{F}$ 上的分裂域, 则同构 $\psi: K\xrightarrow{\sim}\tilde{K}$ 且 $\psi|_F=\varphi$ 的个数恰好为 $[K:F]$.*

证明. 不妨假设 $f(x)$ 无线性因子. 由引理 6.19 知, 若 $\alpha\in K$ 为 $f(x)$ 的根, $g(x)$ 是 α 在 F 上的不可约多项式. $\tilde{g}(x)=\varphi(g(x))$, $\tilde{\alpha}$ 为 $\tilde{g}(x)$ 的根, 则存在 $\varphi_1: F(\alpha)\xrightarrow{\sim}\tilde{F}(\tilde{\alpha})$ 且 $\varphi_1|_F=\varphi$. 由归纳法, 即知存在同构 $\psi: K\xrightarrow{\sim}\tilde{K}$, $\psi|_F=\varphi$.

更进一步地, 若 $\psi: K\xrightarrow{\sim}\tilde{K}$, 则 $\psi(\alpha)$ 必为 $\tilde{g}(x)$ 的根. 要得到 ψ, 我们先得到 $\varphi_1: F(\alpha)\to\tilde{F}(\psi(\alpha))$, 这样的 φ_1 的个数为 $\deg\tilde{g}=\deg g=[F(\alpha):F]$. 对于每个 φ_1, 注意到 K 为 $f(x)$ 在 $F(\alpha)$ 上的分裂域 $\tilde{K}$ 为 $\tilde{f}(x)$ 在 $\tilde{F}(\tilde{\alpha})$ 上的分裂域, 且 $[K:F(\alpha)]\leqslant[K:F]$. 我们由对 $[K:F]$ 作归纳假设, 故共有 $[K:F(\alpha)]$ 种不同同构 ψ, 使得 $\psi|_{F(\alpha)}=\varphi_1$, 所以共有 $[K:F(\alpha)]\cdot[F(\alpha):F]=[K:F]$ 种同构 $\psi: K\xrightarrow{\sim}\tilde{K}$, $\psi|_F=\varphi$. □

***Galois* 基本定理的证明**. 有了上面的准备, 我们可以证明 Galois 理论基本定理, 即

(i) 给定 L 为 K/F 的中间域. 令 $H=\mathrm{Gal}(K/L)$, 则 H 在 L 上的作用平凡, 故 $L\subseteq K^H$. 另一方面, 由于 K 是 L 的 Galois 扩张, 故 $[K:L]=|H|$. 所以 $|H|=[K:K^H]=[K:L]$, 故 $L=K^H$.

(ii) 给定 $H\leqslant G$. 令 $L=K^H$, 故 H 是 $\mathrm{Gal}(K/L)$ 的子群, 但 $|H|\geqslant[K:K^H]=[K:L]=|\mathrm{Gal}(K/L)|$, 所以 $H=\mathrm{Gal}(K/L)$ 且 $[L:F]=(G:H)$.

(iii) 如果 $H\leqslant G, \sigma\in G$, 则群 $\sigma H\sigma^{-1}$ 对应的子域为 σL, 即有 $\mathrm{Gal}(K/\sigma L)=\sigma H\sigma^{-1}$. 事实上, 只要验证 $\mathrm{Gal}(K/\sigma L)\supseteq\sigma H\sigma^{-1}$, 再由对称性立得.

(iv) 如果 $H\lhd G$ 是 G 的正规子群. 令 $L=K^H$, 由于 $H=\sigma H\sigma^{-1}$, 故 $L=\sigma L$ 对所有 $\sigma\in G$ 成立. 我们得到群同态

$$\pi: G\to\mathrm{Gal}(L/F)$$

且 $\ker\pi=H$, 故有 $\bar{\pi}: G/H\hookrightarrow\mathrm{Gal}(L/F)$. 由于 $(G:H)=[L:F]\geqslant|\mathrm{Gal}(L/F)|$, $\bar{\pi}$ 为同构, 即 $\mathrm{Gal}(L/F)\cong G/H$.

反之, 若 L/F 为Galois扩张, 令 $H=\mathrm{Gal}(K/L)$, 由于 L 是某可分多项式 $g(x)=(x-\beta_1)\cdots(x-\beta_k)\in F[x]$ 的分裂域. 由于 $\sigma(g(x))=g(x)$ 对所有 $\sigma\in\mathrm{Gal}(K/F)$ 成立, $\sigma L=L$, 故 $H=\sigma H\sigma^{-1}$, 即 $H\lhd G$. □

习　　题

习题5.1. 设 $E=\mathbb{C}(t)$ 为有理函数域, $\sigma,\tau\in G=\mathrm{Gal}(E/\mathbb{C})$, 其中 $\sigma(t)=\zeta_3 t$, $\tau(t)=t^{-1}$. 证明:

(1) τ 和 σ 生成的群 H 是 G 的 6 阶子群;

(2) $\mathrm{Inv}(H)=\mathbb{C}(t^3+t^{-3})$.

习题5.2. 设域 F 的特征为素数 p, $\sigma\in G=\mathrm{Gal}(F(x)/F)$, 其中 $\sigma(x)=x+1$. 令 H 为由 σ 生成的 G 的子群. 证明 $|H|=p$. 试确定 $\mathrm{Inv}(H)$.

习题5.3. 设域 F 的特征为素数 p, $a\in F$. 如果 x^p-x-a 在 $F[x]$ 中不可约, 令 α 为一个根, 证明 $F(\alpha)/F$ 为 *Galois* 扩张并计算出它的 *Galois* 群.

习题5.4. 设 L 和 M 均是域 E 的子域. 证明如果 $L/L\cap M$ 为有限 *Galois*扩张, 则 LM/M 也为有限 *Galois* 扩张, 并且

$$\mathrm{Gal}(LM/M)\cong\mathrm{Gal}(L/L\cap M).$$

习题5.5. 设 E/F 为有限 *Galois* 扩张, N 和 M 为中间域, $E\supseteq N\supseteq M\supseteq F$, 并且 N 是 M 在 F 上的正规闭包. 证明

$$\mathrm{Gal}(E/N)=\bigcap_{\sigma\in\mathrm{Gal}(E/F)}\sigma\mathrm{Gal}(E/M)\sigma^{-1}.$$

习题5.6. 设 E/F 为有限 *Galois*扩张. 如果对任一域 $K(F\subsetneq K\subseteq E)$, K 对 F 均有相同的扩张次数 $[K:F]$, 则 $[E:F]=p$.

习题5.7. (1) 证明 $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q}$ 是 *Galois* 扩张, 并求出 *Galois* 群;

(2) 求元素 $\sqrt{6}+\sqrt{10}+\sqrt{15}$ 在 Q 上的极小多项式;

(3) 证明 $\sqrt{6}\in\mathbb{Q}(\sqrt{6}+\sqrt{10}+\sqrt{15})$;

(4) 求 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{6}+\sqrt{10}+\sqrt{15})$ 上的极小多项式.

索　引