前 言

近世代数是数学学科中的重要基础课之一，也是一门比较抽象的学科。为了帮助广大同学更好地掌握近世代数的基本概念和基本理论，综合运用各种解题技巧和方法，提高分析问题和解决问题的能力，我们根据杨子胥教授编著的《近世代数》第二版（高等教育出版社出版）编写了本辅导教材。

本辅导教材以章为单位，每章由导读、知识点考点精要、释疑解惑、典型题精讲和习题全解等部分组成。

导读 列出相应各章应掌握的知识点以及重点、难点内容。

知识点考点精要 列出相应各章的基本概念、重要定理和重要公式，突出必须掌握和理解的核心内容以及考点的核心知识。

释疑解惑 对本章重点、难点内容以及难以理解的问题给以详细剖析。

典型题精讲 选择若干概念性、启发性、综合性较强的典型题目，剖析解题思路，归纳解题经验和技巧，并作出必要的注释，帮助大家提升解题能力。

习题全解 教材中课后习题数量大、层次多，基础性问题可从多个角度帮助同学们理解基本概念和基本理论，综合性问题则有助于广大读者进一步的提高和应用，不少问题需要独特的解题思路和方法。因此，对教材课后全部习题给出了详细解答。由于近世代数解题方法千变万化，大多习题我们只给出了一种参考解答或提示，其他方法留给读者思考。

本辅导教材由滕加俊、滕兴虎、吴红等同志编写，全书由滕加俊教授统稿。由于作者水平有限，加之时间仓促，书中不足之处敬请广大同行和读者批评指正。

作者

2006 年 9 月

目 录

第一章 基本概念

导读

本章主要介绍了学习本课程及其他数学分支的基础知识，内容有集合、映射的概念，代数运算及各种运算律，同态、同构的概念与性质以及等价关系。

一、基本要求

1. 理解集合的概念，掌握集合的各种运算及其运算性质；
2. 理解映射和代数运算的概念，掌握代数运算的结合律、分配律、交换律；
3. 熟练掌握映射的同态、同构的概念及其性质；
4. 掌握等价关系的概念，理解等价关系与集合分类的关系。

二、重点与难点

1. 代数运算；
2. 映射的同态与同构；
3. 等价关系与集合的分类。

知识点考点精要

一、集合

1. 集合的概念

(1) 集合

若干个(有限个或无限个)固定元素的全体称为集合，简称为集。常用

大写拉丁字母 A、B、C、… 表示。

集合中的每一个体称为元素或元。常用小写拉丁字母 a、b、c、… 表示。

元素与集合的关系：$x \in A$ 或 $x \notin A$，也可记作 $A \ni x$ 或 $A \not\ni x$。

注 ① 不含任何元素的集合称为空集合，常记作 $\varnothing$。

② 常用 $\mathbf{Z}$ 表示整数集，$\mathbf{Z}^*$ 表示非零整数集；$\mathbf{Q}$ 表示有理数集，$\mathbf{Q}^*$ 表示非零有理数集。

(2) 子集与真子集

若集合 A 中的每个元素都属于集合 B，则称 A 是 B 的一个子集，常记作 $A \subseteq B$。若 A 是 B 的一个子集，又 B 中有元素不在 A 中，则称 A 是 B 的一个真子集，记为 $A \subset B$。

注 空集 $\varnothing$ 是任何集合的一个子集。

(3) 幂集

集合 A 的所有子集(包括 $\varnothing$) 所作成的集合，称为 A 的幂集，记作 $P(A)$。$|A| = n$ 时，$|P(A)| = 2^n$。

2. 集合的运算

(1) 交集

由集合 A 与集合 B 的所有公共元素构成的集合，记为 $A \cap B$，叫做 A 与 B 的交集，简称 A 与 B 的交，即

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

(2) 并集

由属于集合 A 或集合 B 的所有元素作成的集合，记为 $A \cup B$，叫做 A 与 B 的并集，简称 A 与 B 的并，即

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

(3) 差集

A、B 是两个集合，称集合

$$A - B = \{x \mid x \in A, x \notin B\}$$

为 A 与 B 的差集。

(4) 余集

集合 X 与 Y 满足 $Y \subseteq X$，则称差集 $X - Y$ 为 Y 在 X 中的余集，记作 Y'。

3. 运算律

(1) 幂等性 $A \cap A = A$，$A \cup A = A$；

(2) 交换性 $A \cap B = B \cap A, A \cup B = B \cup A$;

(3) 结合性 $(A \cap B) \cap C = A \cap (B \cap C)$,

$(A \cup B) \cup C = A \cup (B \cup C)$;

(4) 分配性 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;

(5) 德·摩根律 $(A \cup B)' = A' \cap B', (A \cap B)' = A' \cup B'$。

二、映射与变换

1. 相关概念

(1) 映射

设 X 与 Y 是两个集合。如果有一个法则 φ,它对于 X 中每个元素 x,在 Y 中都有一个惟一确定的元素 y 与它对应,则称 φ 为集合 X 到集合 Y 的一个映射,常记作

$$\varphi: x \longrightarrow y \text{ 或 } y = \varphi(x)$$

(2) 映射的象与原象

在映射 $y = \varphi(x)(x \in X, y \in Y)$ 中,y 叫做 x 在映射 φ 之下的象,x 叫做 y 在映射 φ 之下的原象或逆象。

(3) 满射

φ 是集合 X 到集合 Y 的一个映射。若在 φ 下 Y 中每个元素在 X 中都有逆象,则称 φ 为 X 到 Y 的一个满射,也称为 X 到 Y 上的一个映射。

(4) 单射

φ 是集合 X 到集合 Y 的一个映射。若在 φ 下 X 中不相等的元素在 Y 中的象也不相等,则称 φ 为 X 到 Y 的一个单射,或 X 到 Y 里的一一映射。

(5) 双射

集合 X 到 Y 的一个映射,如果既是单射又是满射,则称它为 X 到 Y 的一个双射,或 X 到 Y 上的一一映射。

(6) 逆映射

设 φ 是集合 X 到集合 Y 的一个双射,且 $\varphi(x) = y$,则法则

$$\varphi^{-1}: y \longrightarrow x, \text{即 } \varphi^{-1}(y) = x$$

为集合 Y 到 X 的一个双射,并称 φ^{-1} 为 φ 的逆映射。

φ^{-1} 的逆映射即为 φ,即 $(\varphi^{-1})^{-1} = \varphi$。

(7) 变换

集合 X 到自身的映射,称为集合 X 的一个变换。

类似可定义出满射变换、单射变换和双射变换,其中 X 的双射变换也称为 X 的一个一一变换。

(8) 置换

有限集合 X 上的双射变换 φ 称为一个 n 次置换,常用以下符号表示:

$$\varphi=\begin{pmatrix}1 & 2 & \cdots & n\\ \varphi(1) & \varphi(2) & \cdots & \varphi(n)\end{pmatrix}$$

2. 映射的相等

设 σ 与 τ 都是集合 X 到 Y 的映射,如果对 X 中每个元素 x 都有

$$\sigma(x)=\tau(x)$$

则称 σ 与 τ 是 X 到 Y 的两个相等的映射,记为

$$\sigma=\tau$$

3. 双射的条件

必要条件　设 X 与 Y 为两个有限集合,则存在 X 到 Y 的一个双射的必要条件是 $|X|=|Y|$,即二者包含的元素个数相等。

充要条件(1)　φ 是集合 X 到集合 Y 的一个映射,则 φ 是 X 到 Y 的一个双射的充要条件是 φ 为"双方单值",即 φ 对 X 中每个元素在 Y 中只有一个象,且对 Y 中每个元素在 X 中有且只有一个逆象。

充要条件(2)　设 X 与 Y 是两个有限集合,且 $|X|=|Y|$,φ 是从 X 到 Y 的一个映射,则 φ 是双射的充要条件是 φ 是满射(单射)。

4. 满射与单射的关系

若 X 与 Y 是两个有限集合,且 $|X|=|Y|$,φ 是从 X 到 Y 的一个映射,则 φ 是满射当且仅当 φ 是单射。

5. 双射变换个数判定定理

设 X 是一个有限集合且 $|X|=n$,则 X 上共有 $n!$ 个双射变换。

6. 映射乘积的定义

设 τ 是集合 M_1 到集合 M_2 的一个映射,σ 是集合 M_2 到集合 M_3 的一个映射,则

$$x\longrightarrow\sigma(\tau(x))\qquad(\forall\ x\in M_1)$$

是 M_1 到 M_3 的一个映射,记为 $\sigma\tau$,即

$$\sigma\tau(x) = \sigma(\tau(x)) \qquad (\forall\ x \in M_1)$$

并称其为映射的合成或映射的乘法，$\sigma\tau$ 称为 τ 与 σ 的乘积。

三、代数运算

1. 代数运算的定义

集合 M 上的一个法则，若它对 M 中任意两个有次序的元素 a 与 b，在 M 中都有一个惟一确定的元素 d 与它们对应，则这个法则称为集合 M 的一个代数运算，常记作"$\circ$"。因此有

$$a \circ b = d$$

2. 变换的运算

设 M 是任意一个非空集合，$T(M)$ 表示 M 的全体变换作成的集合，$S(M)$ 表示 M 的全体双射变换作成的集合，则

$$S(M) \subseteq T(M)$$

(1) 变换的乘法

任取 σ、$\tau \in T(M)$，则乘积 $\sigma\tau$ 即

$$\sigma\tau(x) = \sigma(\tau(x)) \qquad (\forall\ x \in M)$$

也是 M 的一个变换，这样就有 $\sigma\tau \in T(M)$，并称之为变换的乘法，它是 $T(M)$ 的一个代数运算。

(2)$S(M)$ 上变换的乘法

变换的乘法是 $S(M)$ 上的一个代数运算，即 M 的任意两个双射交换的乘积仍是 M 的一个双射变换。

(3) 乘法表

有限集合 $M = \{a_1, a_2, \cdots, a_n\}$ 上的代数运算

$$a_i \circ a_j = a_{ij} \in M \quad (i, j = 1, 2, \cdots, n)$$

直观上可列成下表：

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	a_{11}	a_{12}	$\cdots$	a_{1n}
a_2	a_{21}	a_{22}	$\cdots$	a_{2n}
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	a_{n1}	a_{n2}	$\cdots$	a_{nn}

常称其为 M 的“乘法表”。

四、运算律

1. 结合律

(1) 定义

设 M 是一个有代数运算 $\circ$ 的集合，如果对 M 中任意元素 a、b、c 都有

$$(a \circ b) \circ c = a \circ (b \circ c)$$

则称 M 的这个运算满足结合律。

(2) 性质定理

若集合 M 的代数运算 $\circ$ 满足结合律，则对 M 中任意 $n(n \geqslant 3)$ 个元素无论怎样加括号，其结果都相等。

注 对 M 中 n 个元素 $a_1, a_2, \cdots, a_n$ 共有 $\dfrac{(2n-2)!}{n!(n-1)!}$ 种加括号方法。

2. 交换律

(1) 定义

若集合 M 的代数运算 $\circ$ 对 M 中任意元素 a、b 都有

$$a \circ b = b \circ a$$

则称 M 的这个代数运算满足交换律。

(2) 性质定理

若集合 M 的代数运算 $\circ$ 既满足结合律又满足交换律，则对 M 中任意 n 个元素进行运算时可以任意结合和交换元素的前后次序，其结果均相等。

3. 分配律

(1) 定义

设集合 M 有两个代数运算 $\circ$ 及 $\oplus$，若对 M 中任意元素 a、b、c 都有

$$a \circ (b \oplus c) = (a \circ b) \oplus (a \circ c)$$

则称运算 $\circ$ 对 $\oplus$ 满足左分配律；若

$$(b \oplus c) \circ a = (b \circ a) \oplus (c \circ a)$$

则称运算 $\circ$ 对 $\oplus$ 满足右分配律。

(2) 性质定理

设集合 M 有两个代数运算 $\circ$ 及 $\oplus$，其中 $\oplus$ 满足结合律，而 $\circ$ 对 $\oplus$ 满足左分配律，则对 M 中任意元素 a 及 $b_i(i = 1, 2, \cdots, n)$，有

$$a \circ (b_1 \oplus b_2 \oplus \cdots \oplus b_n) = (a \circ b_1) \oplus (a \circ b_2) \oplus \cdots \oplus (a \circ b_n)$$

对右分配律有类似结果。

五、同态与同构

1. 同态的定义

(1) 同态映射

设集合 M 与 $\overline{M}$ 各有代数运算 $\circ$ 及 $\bar{\circ}$，且 φ 是 M 到 $\overline{M}$ 的一个映射。若 φ 满足条件：

$\forall a、b \in M$，在 φ 下由

$$a \longrightarrow \bar{a},\quad b \longrightarrow \bar{b}$$

总有

$$a \circ b \longrightarrow \bar{a} \mathbin{\bar{\circ}} \bar{b}$$

即 $\overline{a \circ b} = \bar{a} \mathbin{\bar{\circ}} \bar{b}$ 或 $\varphi(a \circ b) = \varphi(a) \mathbin{\bar{\circ}} \varphi(b)$，则称 φ 是 M 到 $\overline{M}$ 的一个同态映射。

(2) 集合间的同态

若集合 M 到 $\overline{M}$ 存在同态满射，则称 M 与 $\overline{M}$ 同态，记为 $M \sim \overline{M}$。集合 M 到自身的同态映射，称为 M 的自同态映射，或简称 M 的自同态。

2 同态性质定理

(1) 设集合 M 与 $\overline{M}$ 分别有代数运算 $\circ$ 与 $\bar{\circ}$，且 $M \sim \overline{M}$，则

① 当 $\circ$ 满足结合律时，$\bar{\circ}$ 也满足结合律；

② 当 $\circ$ 满足交换律时，$\bar{\circ}$ 也满足交换律。

(2) 设集合 M 有代数运算 $\circ$ 及 $\oplus$，集合 $\overline{M}$ 有代数运算 $\bar{\circ}$ 及 $\bar{\oplus}$；又 φ 是 M 到 $\overline{M}$ 的一个满射，且对 $\circ$ 与 $\bar{\circ}$ 以及 $\oplus$ 与 $\bar{\oplus}$ 同态，则当 $\circ$ 对 $\oplus$ 满足左(右)分配律时，$\bar{\circ}$ 对 $\bar{\oplus}$ 也满足左(右)分配律。

3. 同构的定义

(1) 同构映射

设 φ 是 M 到 $\overline{M}$ 的一个(关于代数运算 $\circ$ 及 $\bar{\circ}$)同态满射，若 φ 又是单射，则称 φ 是 M 到 $\overline{M}$ 的一个同构映射。

(2) 集合间的同构

若集合 M 到 $\overline{M}$ 存在同构映射，则称 M 与 $\overline{M}$ 同构，记作 $M \cong \overline{M}$，集合 M 到自身的同构映射，称为 M 的自同构映射，或简称 M 的自同构。

六、等价关系与集合的分类

1. 关系

设 M 是一个集合，如果有一个法则 R，它对 M 中任二元素 a、b 可确定"是"或"不是"符合这个法则，则称此法则 R 为 M 的元素间的一个关系，简称 M 的一个关系。

2. 等价关系

如果集合 M 的一个关系 R 满足以下条件：

(1) 反身性　对 M 中任意元素 a 都有 aRa；

(2) 对称性　如果 aRb，必有 bRa；

(3) 传递性　如果 aRb，bRc，必有 aRc。

则称这个关系为 M 的一个等价关系。

等价关系常用符号"$\sim$"表示，当 $a \sim b$ 时，称 a 与 b 等价。

3. 类与分类

若把集合 M 的全体元素分成若干互不相交的子集（即任二互异子集都无公共元素），则称每个这样的子集叫做 M 的一个类；类的全体叫做 M 的一个分类。

4. 集合的分类与集合的等价关系间的联系

(1) 集合 M 的一个分类决定 M 的一个等价关系。

(2) 集合 M 的一个等价关系决定 M 的一个分类。

5. 剩余类（同余类）

由等价关系　　$aRb \Leftrightarrow a \equiv b \pmod n$

所决定的整数集 Z 的分类有 n 个，若用 $\overline{m}$ 表示整数 m 所在的类，则这 n 个类可表示为

$$\overline{0}, \overline{1}, \cdots, \overline{n-1}$$

称其为以 n 为模的剩余类（同余类），其中

$$\overline{1} = \{\cdots, -2n+1, -n+1, n+1, 2n+1, \cdots\}$$

易知：

两个整数 a 与 b 同在一个类，即 $\overline{a} = \overline{b}$ 的充要条件是 n 整除 a 与 b 的差。

释疑解惑

一、关于集合的理解

1. 集合是数学里的一个“原始概念”，不给精确定义，只给一般性的解释。对集合的解释是多种的，如，

“若干个(有限个或无限个)固定事物的全体叫做一个集合。”

“具有某种特定性质的事物的全体叫做集合。”

“一些特定的放在一起的对象叫做集合。”

“在一定范围内的一些确定的不同对象的全体称为一个集合。”

等等，但它们的涵义是一致的。其共同的特点是：

(1)“对象”，“事物”，“全体”等没有严格定义，不是数学中已定义的概念。

(2) 集合的元素具有确定性，任一集合 A 和任一元素 a，其关系要么是 a 属于 A，要么是 a 不属于 A，不能模棱两可，应是确定的。

(3) 集合中的元素应是互异且排列是无序的。

(4) 一些集合可以作为元素组成一个新的集合，但任何集合不能是它自身的一个元素，不能说“所有集合的集合”，不能把 $\{a\}$ 与 a 等同，否则会引起逻辑上的矛盾。

2. 按集合的定义可得两个集合相等的充要条件

$$A = B \Leftrightarrow A \subseteq B \text{ 且 } B \subseteq A$$

二、关于映射的理解

1. 集合 A 到集合 B 的一个法则 φ 必须满足两个条件才是映射：

(1) 对 A 中的每个元素 a(一个都不漏地) 在 B 中确定一个象 a'；

(2) 对 A 中的每个元素 a 在 B 中所确定的象 a' 必须是惟一的，不能是两个或多个。

2. 判定两个映射 σ 与 τ 相等，只须满足两个条件：

(1) σ 与 τ 具有相同的定义域与相同的值域；

(2)σ 与 τ 对定义域中每个元素的作用相同，即 $\sigma(a)=\tau(a)$。

3. 各类映射间的关系图

各类映射间的关系图如图 1-1 所示。

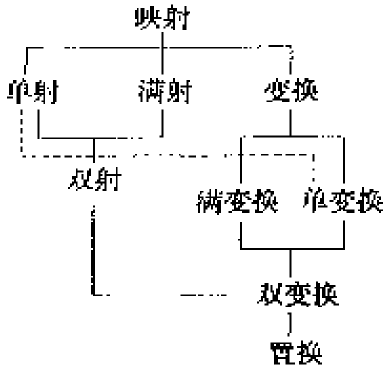

图 1-1

4. 各类映射的判别法

判断一映射是单射、满射还是双射，通常按定义或教材中的两个定理进行，也可按下述结论进行。

(1)$\sigma: X \longrightarrow Y$ 是双射 $\Leftrightarrow$ 存在 $\tau: Y \longrightarrow X$，使得

$$\tau\sigma=\varepsilon_X \text{ 且 } \sigma\tau=\varepsilon_Y$$

其中 ε_X 与 ε_Y 分别为 X 与 Y 的恒等变换。

(2) 设 $|X|\geqslant 2$，则 $\sigma: X \longrightarrow Y$ 是单射 $\Leftrightarrow$ 存在 $\tau: Y \longrightarrow X$ 使 $\tau\sigma=\varepsilon_X$，且当这种 τ 惟一时，σ 必为双射。

(3)$\sigma: X \longrightarrow Y$ 是双射 $\Leftrightarrow$ 存在 $\tau: Y \longrightarrow X$ 使

$$\sigma\tau=\varepsilon_Y$$

且当这种 τ 惟一时，σ 必为双射。

5. 映射(变换) 的乘积

(1) 若 φ 是集合 X 到 Y 的一个双射，则 φ 存在逆映射 φ^{-1}，其中 φ^{-1} 是从 Y 到 X 的一个双射，因此

$$\varphi^{-1}\varphi=\varepsilon_X, \varphi\varphi^{-1}=\varepsilon_Y$$

一般地 $\varepsilon_X \neq \varepsilon_Y$，当 $X=Y$ 时，才有 $\varepsilon_X=\varepsilon_Y$ 即

$$\varphi^{-1}\varphi=\varphi\varphi^{-1}$$

(2) 按教材的定义，任取 $\sigma,\tau \in T(M)$，$\forall x \in M$，有

$$\sigma\tau(x)=\sigma(\tau(x))$$

即这两个变换的积是按“自右向左乘法”进行的，有的教材中规定了其他顺序的乘法，如自左向右乘法等，在阅读参考书时需注意。一般地“自右向左乘法”与“自左向右乘法”有很大差异，如置换

$$\sigma=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \tau=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$

求 $\sigma\tau$。

若按“自右向左乘法”(即教材中的约定)，即先 τ 后 σ，则有

$$\sigma\tau=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

若按“自左向右乘法”，即先 τ 后 σ，则有

$$\sigma\tau=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

在本教材中，均按“自右向左乘法”进行。

(3) 映射与函数间的关系

设 φ 是从集合 X 到集合 Y 的一个映射，若集合 Y 是实数集 $\mathbf{R}$(或其子集)，则 φ 就成为通常意义的函数。即函数是映射的一个特例。

三、关于运算律的说明

1. 分配律和通常所说的分配律有所不同，在一个有两个代数运算 $\circ$ 与 $\oplus$ 的代数系统中，在谈到分配律时应指明哪一代数运算对哪一代数运算的分配律，是左分配律还是右分配律，或是两个分配律均满足。

2. 在证明某代数运算满足结合律、交换律或分配律时，应按定义进行，在证明某代数运算不满足某运算律时，只须举出反例即可。

四、同态与同构

1. 在证明两个代数系统$(M,\circ)$与$(\overline{M},\bar{\circ})$同构(同态)时，只需找出它们间的一个同构(同态)映射即可，它们间的同构(同态)映射可能不止一个。

在证明它们不同构(不同态)时，只需证明它们之间不存在任何同构(同态)映射，通常采用反证法。

2. 在证明映射 $\varphi:A\longrightarrow B$ 保持某代数运算时，应避免出现遗漏现象，对有限集合，更要注意要取遍 A 中所有元素。

3. 对于有多个(两个及两个以上)代数运算的代数系统，在指明 φ 为其间的同构(同态)映射时，一定要注意这些代数运算的顺序，映射 φ 是保持的哪一代数运算。

4. 两个代数系统同构时，它们各自由运算表现出来的性质是完全相同的，因此，代数系统的代数性质，就是在同构映射下保持不变的性质，代数学研究的目标，正是发挥这种性质。

典型题精讲

1. 证明不存在集合 A 到它的幂集 $P(A)$ 的满射。

证明 用反证法。

假设存在 A 到 $P(A)$ 的满射 φ。则任 $a \in A$，有 $\varphi(a) \in P(A)$，因 $P(A)$ 是 A 的幂集，故 $\varphi(a)$ 是 A 的子集。于是

$$a \in \varphi(a) \text{ 或 } a \notin \varphi(a)$$

两者中只有一个成立，令

$$S = \{a \in A \mid a \notin \varphi(a)\}$$

则 S 在 A 中的余集是

$$S' = \{a \in A \mid a \in \varphi(a)\}$$

显见 $A = S \cup S'$ 且 $S \cap S' = \varnothing$。

又 φ 是满射，故 $P(A)$ 中的元素 S 必在 A 中有原象，不妨设为 s，则

$$\varphi(s) = S$$

对于 s 下列两者之一成立，

$$s \in S \text{ 或 } s \notin S$$

但是当 $s \in S$ 时，由于 $S = \varphi(s)$，这与 S 的构成矛盾；当 $s \notin S$ 时，即 $s \in S'$，由 S' 的构成有 $s \in \varphi(s) = S$，这同 $S \cap S' = \varnothing$ 相矛盾。

故不存在集合 A 到它的幂集 $P(A)$ 的满射。

---

2. 设 φ 是双射，且 $\varphi\psi$ 有意义。证明：

(1) ψ 是单射 $\Leftrightarrow \varphi\psi$ 是单射；

(2) ψ 是满射 $\Leftrightarrow \varphi\psi$ 是满射。

证明 不妨设 $\varphi: B \longrightarrow C$，$\psi: A \longrightarrow B$。

(1)“$\Rightarrow$” 若 ψ 是单射，则任 $a, b \in A$，$a \neq b$ 时必有 $\psi(a) \neq \psi(b)$，又显见 φ 也是单射，故

$$\varphi(\psi(a)) \neq \varphi(\psi(b))$$

即 $\varphi\psi(a) \neq \varphi\psi(b)$，从而 $\varphi\psi$ 为单射。

“$\Leftarrow$” 若 $\varphi\psi$ 是单射，则任 $a, b \in A$，$a \neq b$ 时必有 $\varphi\psi(a) \neq \varphi\psi(b)$，即

$$\varphi(\psi(a)) \neq \varphi(\psi(b))$$

又 φ 是单射，故 $\psi(a) \neq \psi(b)$，从而 ψ 为单射。

(2)"$\Rightarrow$" 设 ψ 是满射。任 $a'' \in C$，由 φ 是满射可知存在 $a' \in B$，使

$$\varphi(a') = a''$$

再由 ψ 是满射知，存在 $a \in A$，使

$$\psi(a) = a'$$

从而
$$\varphi\psi(a) = \varphi(\psi(a)) = \varphi(a') = a''$$

即 $\varphi\psi$ 是满射。

"$\Leftarrow$" 设 $\varphi\psi$ 是满射。任 $b' \in B$，令 $\varphi(b') = b'' \in C$，故存在 $b \in A$，使得 $\varphi\psi(b) = b''$，从而

$$\varphi(\psi(b)) = \varphi\psi(b) = b'' = \varphi(b')$$

由 φ 是单射知

$$\psi(b) = b'$$

即 ψ 是满射。

---

3. 设 φ 是单射，且 $\varphi\psi$ 和 $\varphi\psi'$ 都有意义。证明 $\varphi\psi = \varphi\psi' \Leftrightarrow \psi = \psi'$。

证明 仅证必要性。

不妨设 $\psi: A \longrightarrow B$，$\psi': A' \longrightarrow B'$，$\varphi: C \longrightarrow D$，由 $\varphi\psi$ 和 $\varphi\psi'$ 都有意义知

$$B = B' = C$$

又 $\varphi\psi = \varphi\psi'$，故 $A = A'$，因此 ψ 和 ψ' 都是 A 到 B 的映射。

$\forall a \in A$，由 $\varphi\psi = \varphi\psi'$ 知

$$\varphi\psi(a) = \varphi\psi'(a)$$

即

$$\varphi(\psi(a)) = \varphi(\psi'(a))$$

由于 φ 是单射，可得

$$\psi(a) = \psi'(a)$$

由 a 的任意性知

$$\psi = \psi'$$

---

4. 设 $A = \{a, b, c\}$，规定 A 的两个不同的代数运算。

解 ① 约定

$$\circ:(x,y)\longrightarrow a=x\circ y\quad(\forall x、y\in A)$$

乘法表如下

$\circ$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

易知通过$\circ$，对于A的任两个元素都可以得出一个惟一确定的结果a，而$a\in A$，故$\circ$为A的一个代数运算。

② 约定

$$\circ:(x,y)\longrightarrow x=x\circ y\quad(\forall x,y\in A)$$

乘法表如下

$\circ$	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

易知它也是A的一个代数运算。

---

5. 假定φ是A与$\overline{A}$间的一个双射，$a\in A$，问

$$\varphi^{-1}(\varphi(a))=?\qquad\varphi(\varphi^{-1}(a))=?$$

若φ是A的一个双射变换，结果又是多少？

解 若φ是双射

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

而$\varphi(\varphi^{-1}(a))$未必有意义。

若φ是A的一个双射变换，则

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

---

6. 假定A和$\overline{A}$对于代数运算$\circ$和$\overline{\circ}$同态，而$\overline{A}$和$\overline{\overline{A}}$对于代数运算$\overline{\circ}$和$\overline{\overline{\circ}}$来说同态。证明：$A$和$\overline{\overline{A}}$对于代数运算$\circ$和$\overline{\overline{\circ}}$来说同态。

证明 依题意存在一个A到$\overline{A}$的同态满射

$$\varphi_1 : a \longrightarrow \overline{a} = \varphi_1(a) \quad (a \in A, \overline{a} \in \overline{A})$$

且任 $a, b \in A$，有

$$\varphi_1(a \circ b) = \overline{a}\ \overline{\circ}\ \overline{b} = \varphi_1(a)\ \overline{\circ}\ \varphi_1(b)$$

同样存在 $\overline{A}$ 到 $\overline{\overline{A}}$ 的一个同态满射

$$\varphi_2 : \overline{a} \longrightarrow \overline{\overline{a}} = \varphi_2(\overline{a}) \quad (\overline{a} \in \overline{A}, \overline{\overline{a}} \in \overline{\overline{A}})$$

且任 $\overline{a}, \overline{b} \in \overline{A}$，有

$$\varphi_2(\overline{a}\ \overline{\circ}\ \overline{b}) = \overline{\overline{a}}\ \overline{\overline{\circ}}\ \overline{\overline{b}} = \varphi_2(\overline{a})\ \overline{\overline{\circ}}\ \varphi_2(\overline{b})$$

定义

$$\varphi : a \longrightarrow \varphi_2(\varphi_1(a)) \quad (a \in A)$$

下面证明 φ 是 A 到 $\overline{\overline{A}}$ 的一个同态满射。

① 由 φ_1, φ_2 为同态满射知，对 $\forall a \in A$，$\varphi_1(a)$ 是 $\overline{A}$ 的一个惟一确定的元素，而 $\varphi_2(\varphi_1(a))$ 是 $\overline{\overline{A}}$ 的一个惟一确定的元素，故 φ 是 A 到 $\overline{\overline{A}}$ 的一个映射。

② 由 φ_1, φ_2 为同态满射，故任 $\overline{\overline{a}} \in \overline{\overline{A}}$，存在一个元素 $\overline{a} \in \overline{A}$，使 $\varphi_2(\overline{a}) = \overline{\overline{a}}$，且存在一个元素 $a \in A$，使 $\varphi_1(a) = \overline{a}$，故在 φ 之下

$$a \longrightarrow \varphi_2(\varphi_1(a)) = \varphi_2(\overline{a}) = \overline{\overline{a}}$$

即 φ 是从 A 到 $\overline{\overline{A}}$ 的一个满射。

③ 同样由 φ_1, φ_2 为同态满射知，$\forall a, b \in A$，有

$$\begin{aligned}\varphi(a \circ b) &= \varphi_2(\varphi_1(a \circ b)) = \varphi_2(\varphi_1(a)\ \overline{\circ}\ \varphi_1(b)) \\ &= \varphi_2(\varphi_1(a))\ \overline{\overline{\circ}}\ \varphi_2(\varphi_1(b)) \\ &= \varphi(a)\ \overline{\overline{\circ}}\ \varphi(b)\end{aligned}$$

即 φ 是从 A 到 $\overline{\overline{A}}$ 的一个同态满射。

---

7. $A = \{$所有有理数$\}$，A 的代数运算是普通加法。$\overline{A} = \{$所有非零的有理数$\}$，$\overline{A}$ 的代数运算是普通乘法。证明：对给定的代数运算来说，A 与 $\overline{A}$ 间没有同构映射存在。

证明 用反证法。

设 φ 是 A 与 $\overline{A}$ 间对所给代数运算的一个同构映射，且 $\varphi(0) = \overline{a}$，则由 φ 是同构映射知

$$\varphi(0) = \varphi(0 + 0) = \varphi(0)\varphi(0) = \overline{a}^{\,2}$$

又同构映射是单射，故 $\overline{a}=\overline{a}^2$，于是

$$\overline{a}^2-\overline{a}=\overline{a}(\overline{a}-1)=0$$

由 $\overline{a}\in\overline{A}$ 知 $\overline{a}\neq 0$，故 $\overline{a}=1$，因此

$$\varphi(0)=1$$

又 φ 是满射，故对于 $-1\in\overline{A}$，必存在 $a\in A$，使

$$\varphi(a)=-1$$

于是

$$\varphi(2a)=\varphi(a+a)=\varphi(a)\varphi(a)=(-1)^2=1$$

故由 φ 是单射知 $2a=0$，即 $a=0$，故 $\varphi(0)=-1$，这同已证 $\varphi(0)=1$ 矛盾。综上可知，同构映射 φ 不存在。

---

8. 证明：实数集与整数集对普通加法不同构，即 $\{R;+\}$ 与 $\{Z;+\}$ 不同构。

证明　用反证法。设 φ 为 $\{R;+\}$ 与 $\{Z;+\}$ 间的同构映射，则对于 $1\in Z$，存在 $a\in R$，使

$$\varphi(a)=1$$

又 $\frac{a}{2}\in R$，故存在 $n\in Z$，使

$$\varphi\left(\frac{a}{2}\right)=n$$

从而

$$2n=\varphi\left(\frac{a}{2}\right)+\varphi\left(\frac{a}{2}\right)=\varphi\left(\frac{a}{2}+\frac{a}{2}\right)=\varphi(a)=1$$

于是 $n=\frac{1}{2}$，但 $\frac{1}{2}\notin Z$，矛盾，故不存在 $\{R;+\}$ 到 $\{Z;+\}$ 的同构映射。

---

9. 有人说：假如一个关系 R 适合对称性和传递性，那么它也适合反身性。他的推论方法是：

因为 R 适合对称性

$$aRb\Rightarrow bRa$$

又因为 R 适合传递性

$$aRb,bRa\Rightarrow aRa$$

这个推论方法有什么错误？

解 其错误在于对"等价关系"定义的陈述没有准确地理解。

$$aRb \Rightarrow bRa$$

的含义是：由 aRb 可得 bRa；假如对于某元素 a，找不到任何元素 b，使 aRb 成立，那么就得不出 bRa，因而也得不出 aRa。

例如，设 $A = Z$，如下定义 A 中的关系：

$$aRb \Leftrightarrow ab > 0$$

R 虽然满足对称性和传递性，但不满足反身性，这是因为

$$0R0$$

不成立。

习题全解

§ 1 集合(P5)

1. 证明本节的等式(4)：

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

证明 先证 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$。

取任意的 $x \in A \cap (B \cup C)$，则 $x \in A$ 且 $x \in B \cup C$，即 $x \in A$，同时还有 $x \in B$ 或 $x \in C$。若 $x \in B$，则 $x \in A \cap B$；若 $x \in C$，则 $x \in A \cap C$，从而 $x \in (A \cap B) \cup (A \cap C)$，由 x 的任意性可知

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$$

取任意的 $x \in (A \cap B) \cup (A \cap C)$，则 $x \in A \cap B$ 或 $x \in A \cap C$，即 $x \in A$ 且 $x \in B$ 或 $x \in A$ 且 $x \in C$，从而 $x \in A$ 且 $x \in B$ 或 $x \in C$，即 $x \in A \cap (B \cup C)$，由 x 的任意性可知

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$$

因此

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

再证 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$。

取任意的 $x \in A \cup (B \cap C)$，则 $x \in A$ 或 $x \in B \cap C$，即 $x \in B$ 且 $x \in C$，同时还可能 $x \in A$，从而 $x \in (A \cup B) \cap (A \cup C)$，由 x 的任意性

知

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$$

取任意的 $x \in (A \cup B) \cap (A \cup C)$，则 $x \in A \cup B$ 且 $x \in A \cup C$，即 $x \in A$ 或 $x \in B$ 同时还有 $x \in A$ 或 $x \in C$，从而 $x \in A$ 或 $x \in B \cap C$，故 $x \in A \cup (B \cap C)$，由 x 的任意性知

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$$

因此
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

注 证明两集合 A 与 B 相等，一般是利用 $A = B$ 的充要条件

$$A \subseteq B \text{ 且 } B \subseteq A$$

---

2. 若 $A \cap B = A \cap C$，问：是否 $B = C$？把 $\cap$ 改成 $\cup$ 时又如何？

解 不一定有 $B = C$。如 $A = \varnothing$，$B = \{2\}$，$C = \{3\}$，$A \cap B = B \cap C = \varnothing$；

又如 $A = \{1,2\}$，$B = \{1,3\}$，$C = \{1,4\}$，则 $A \cap B = A \cap C = \{1\}$，但均有 $B \neq C$。

把 $\cap$ 改成 $\cup$ 时也不一定有 $B = C$，如 $A = \{1,2\}$，$B = \{1\}$，$C = \{2\}$，则 $A \cup B = A \cup C = A = \{1,2\}$，但 $B \neq C$；又如 $A = \{1,2\}$，$B = \{2,3\}$，$C = \{1,3\}$，则 $A \cup B = A \cup C = \{1,2,3\}$，但 $B \neq C$。

注 此例说明集合的交运算及并运算没有所谓的消去律。

---

3. 设 A 是有限集合，且 $|A| = n$，证明 $|P(A)| = 2^n$。

证明 由 $|A| = n$ 可知 A 的含 $k(0 \leqslant k \leqslant n)$ 个元素的子集共有 C_n^k 个，因此有限集 A 的所有子集个数为

$$C_n^0 + C_n^1 + \cdots + C_n^n = (1+1)^n = 2^n$$

即
$$|P(A)| = 2^n$$

---

4. 设 A、B 是两个有限集合，证明 $|A \cup B| + |A \cap B| = |A| + |B|$。

证明 设 $|A| = m$，$|B| = n$，$|A \cap B| = k$，则 $|A \cup B| = m + n - k$，即

$$|A \cup B| + |A \cap B| = |A| + |B|$$

5. 设 A、B 是两个集合，称集合

$$A-B=\{a \mid a \in A, a \notin B\}$$

为 A 与 B 的差集。特别，当 $Y \subseteq X$ 时，用 Y' 表示 $X-Y$，并称为 Y 在 X 中的余集。证明德·摩根(A. De Morgan, 1806 ~ 1871)律：若 A、$B \subseteq X$，则

$$(A \cup B)'=A' \cap B', \quad (A \cap B)'=A' \cup B'$$

证明 先证 $$(A \cup B)'=A' \cap B'$$

取任意的 $x \in (A \cup B)'$，则 $x \notin (A \cup B)$，即 $x \notin A$ 且 $x \notin B$，故 $x \in A'$ 且 $x \in B'$，从而 $x \in A' \cap B'$，由 x 的任意性可知

$$(A \cup B)' \subseteq A' \cap B'$$

取任意的 $x \in A' \cap B'$，则 $x \notin A$ 且 $x \notin B$，即 $x \notin (A \cup B)$，故 $x \in (A \cup B)'$，由 x 的任意性可知

$$A' \cap B' \subseteq (A \cup B)'$$

因此

$$(A \cup B)'=A' \cap B'$$

再证 $$(A \cap B)'=A' \cup B'$$

取任意的 $x \in (A \cap B)'$，则 $x \notin (A \cap B)$，即 $x \notin A$ 或 $x \notin B$，故 $x \in A'$ 或 $x \in B'$，即 $x \in A' \cup B'$，由 x 的任意性可知

$$(A \cap B)' \subseteq A' \cup B'$$

取任意的 $x \in A' \cup B'$，则 $x \notin A$ 或 $x \notin B$，即 $x \notin A \cap B$，故 $x \in (A \cap B)'$，由 x 的任意性知

$$A' \cup B' \subseteq (A \cap B)'$$

$$(A \cap B)'=A' \cup B'$$

§2 映射与变换(P11)

1. 设 $X=\{1,2,3,4,5\}$，$Y=\{0,2,4,6,8,10\}$，试给出 X 到 Y 的两个单射。

解 $X=\{1,2,3,4,5\}$，$Y=\{0,2,4,6,8,10\}$，则法则

$$\varphi_1: x \longrightarrow 2x, \text{ 即 } \varphi_1(x)=2x$$

及法则

$$\varphi_2: x \longrightarrow 2(x-1), \text{ 即 } \varphi_2(x)=2(x-1)$$

是 X 到 Y 的两个不同的单射。

2. 设 X 是数域 F 上全体 $n(n>1)$ 阶方阵作成的集合。问

$$\varphi: \boldsymbol{A} \longrightarrow |\boldsymbol{A}|$$

是否为 X 到 F 的一个映射?其中 $|\boldsymbol{A}|$ 为 $\boldsymbol{A}$ 的行列式,是否为满射或单射?

解 按方阵及方阵的行列式关系可以知道对于每一个 X 中的方阵 $\boldsymbol{A}$,在 F 中有惟一的 $|\boldsymbol{A}|$ 与之对应,因此 φ 是 X 到 F 的一个映射。又任意 $a \in F$,有

$$a = \begin{vmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{vmatrix}$$

即存在 n 阶方阵

$$\boldsymbol{A} = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

使 $|\boldsymbol{A}| = a$,即存在 $\boldsymbol{A}$,使得 $\varphi(\boldsymbol{A}) = |\boldsymbol{A}| = a$,因此 φ 是 X 到 F 的一个满射。显见,若

$$\boldsymbol{B} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & a & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

也有 $\varphi(\boldsymbol{B}) = |\boldsymbol{B}| = a$,因此 φ 不是 X 到 F 的一个单射。

---

3. 设 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 是数域 F 上两个 n 阶相似方阵,$F[\boldsymbol{A}]$ 为系数属于 F 的关于 $\boldsymbol{A}$ 的一切多项式作成的集合。问:法则

$$\varphi: f(\boldsymbol{A}) \longrightarrow f(\boldsymbol{B})$$

是否为 $F[\boldsymbol{A}]$ 到 $F[\boldsymbol{B}]$ 的映射?其中 $f(x)$ 是系数属于 F 的任意多项式,又 φ 是否为单射或满射?

解 因为 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 为两个相似方阵,故存在一个可逆的方阵 $\boldsymbol{C}$,使 $\boldsymbol{B} = \boldsymbol{CAC}^{-1}$。

若 $f(\boldsymbol{A})=g(\boldsymbol{A})$，则有 $f(\boldsymbol{B})=g(\boldsymbol{B})$，故 φ 为 $F[\boldsymbol{A}]$ 到 $F[\boldsymbol{B}]$ 的映射，实际上有

$$f(\boldsymbol{B})=f(\boldsymbol{CAC}^{-1})=\boldsymbol{C}f(\boldsymbol{A})\boldsymbol{C}^{-1}=\boldsymbol{C}g(\boldsymbol{A})\boldsymbol{C}^{-1}=g(\boldsymbol{CAC}^{-1})=g(\boldsymbol{B})$$

因此 φ 是 $F[\boldsymbol{A}]$ 到 $F[\boldsymbol{B}]$ 的映射。

类似地，若 $f(\boldsymbol{B})=g(\boldsymbol{B})$，则

$$f(\boldsymbol{A})=f(\boldsymbol{C}^{-1}\boldsymbol{BC})=\boldsymbol{C}^{-1}f(\boldsymbol{B})\boldsymbol{C}=\boldsymbol{C}^{-1}g(\boldsymbol{B})\boldsymbol{C}=g(\boldsymbol{C}^{-1}\boldsymbol{BC})=g(\boldsymbol{A})$$

即 φ 为单射。又对 $F[\boldsymbol{B}]$ 中的任意元素 $f(\boldsymbol{B})$，总存在 $F[\boldsymbol{A}]$ 中的元素 $f(\boldsymbol{A})$ 与之对应，即

$$\varphi(f(\boldsymbol{A}))=f(\boldsymbol{B})$$

因此可知 φ 又是满射，从而 φ 是双射。

---

4. 对本节给出的 3 次置换，求出下列各元素：

(1) $\varphi_5(\varphi_3(\varphi_1(1)))=?$

(2) $\varphi_6(\varphi_4(\varphi_2(2)))=?$

解 (1) $\varphi_1(1)=1,\varphi_3(1)=2,\varphi_5(2)=1$，故 $\varphi_5(\varphi_3(\varphi_1(1)))=1$。

(2) $\varphi_2(2)=3,\varphi_4(3)=1,\varphi_6(1)=3$，故 $\varphi_6(\varphi_4(\varphi_2(2)))=3$。

---

5. 给出整数集的两个不同的双射。

解 如 $\varphi_1:x\longrightarrow x+1$ 及 $\varphi_2:x\longrightarrow x-1$ 即为整数集自身的双射，其中 x 为任一整数。

§ 3 代数运算(P15)

1. 设 M 是正整数集，下列各法则哪些是 M 的代数运算？

(1) $a\circ b=a^b$；

(2) $a\circ b=a+b-2$；

(3) $a\circ b=a$。

解 因为对于正整数 $a,b,a+b-2$ 未必是正整数，因此(2) 不是代数运算。(1) 与(3) 是代数运算。

---

2. 设 $\circ$ 及 $\bar{\circ}$ 是集合 M 的两个代数运算，如果在 M 中存在 a,b 使

$$a\circ b\neq a\mathbin{\bar{\circ}}b$$

则称 $\circ$ 及 $\bar{\circ}$ 是 M 的两个不同的代数运算。

如果 $|M| = n$，问：可以为 M 规定出多少种不同的代数运算？

解 由两个不同的代数运算定义可知，$|M| = n$ 时可规定的不同的代数运算的个数即为 M 中 n 个元素可重复的全排列 n^n。

---

3. 试对数域 F 上全体 n 阶方阵的集合规定两个(异于矩阵普通运算)不同的代数运算。

解 矩阵的普通运算有矩阵乘法、矩阵加法及矩阵减法，因此，可定义如下代数运算

$$\boldsymbol{A} \circ \boldsymbol{B} = \boldsymbol{A}, \quad \boldsymbol{A} \circ \boldsymbol{B} = \boldsymbol{AB} + \boldsymbol{E}$$

---

4. 设 $M = \{1,2,3\}$，问：$|T(M)| = ?$ $|S(M)| = ?$ 再列出 $S(M)$ 的乘法表。

解 由习题 2 可知 $|T(M)| = 3^3 = 27$，而 $|S(M)|$ 为不可重复的排列数 $3!$，即 $|S(M)| = 6$，易当求得 $S(M)$ 乘法表如下：

$\cdot$	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_1	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_2	φ_2	φ_1	φ_5	φ_6	φ_3	φ_4
φ_3	φ_3	φ_4	φ_1	φ_2	φ_6	φ_5
φ_4	φ_4	φ_3	φ_6	φ_5	φ_1	φ_2
φ_5	φ_5	φ_6	φ_2	φ_1	φ_4	φ_3
φ_6	φ_6	φ_5	φ_4	φ_3	φ_2	φ_1

---

5. 设 M 为正整数集合，试给出 M 的两个双射变换 σ、τ，使得

$$\sigma\tau \neq \tau\sigma$$

解 取 $\sigma: 1 \longrightarrow 2, 2 \longrightarrow 1, x \longrightarrow x\ (x = 3,4,\cdots)$

$\tau: 1 \longrightarrow 3, 3 \longrightarrow 1, x \longrightarrow x\ (x = 2,4,5,\cdots)$

则 $\sigma\tau: 1 \longrightarrow 3, 2 \longrightarrow 1, 3 \longrightarrow 2, x \longrightarrow x\ (x = 4,5,\cdots)$

$\tau\sigma: 1 \longrightarrow 2, 2 \longrightarrow 3, 3 \longrightarrow 1, x \longrightarrow x\ (x = 4,5,\cdots)$

显然 σ 与 τ 为 M 的双射且 $\sigma\tau \neq \tau\sigma$。

§ 4 运算律(P20)

1. 设 M 为实数集，问

$$a \circ b = 2a + 3b \quad (a,b \in M)$$

是否满足结合律和交换律?

解 注意到

$$1 \circ 0 = 2, \qquad 0 \circ 1 = 3$$

故不满足交换律;

又 $(1 \circ 0) \circ 0 = 2 \circ 0 = 4, \qquad 1 \circ (0 \circ 0) = 1 \circ 0 = 2$

故也不满足结合律。

---

2. 下列各集合对所规定的代数运算是否满足结合律和交换律?

(1)M 为整数集,$a \circ b = a^2 + b^2$;

(2)M 为有理数集,$a \circ b = a + b - ab$。

解 (1) 由 $b \circ a = b^2 + a^2 = a^2 + b^2 = a \circ b$,故满足交换律,又由于

$$(a \circ b) \circ c = (a^2 + b^2)^2 + c^2 \text{与} a \circ (b \circ c) = a^2 + (b^2 + c^2)^2$$

未必相等,如

$$(1 \circ 1) \circ 0 = 2^2 = 4, \quad 1 \circ (1 \circ 0) = 1 + 1 = 2$$

因此不满足结合律。

(2) 由于

$$b \circ a = b + a - ba = a + b - ab = a \circ b$$

$$\begin{aligned}(a \circ b) \circ c &= (a + b - ab) + c - (a + b - ab)c \\ &= a + b + c - ab - ac - bc + abc\end{aligned}$$

$$\begin{aligned}a \circ (b \circ c) &= a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - ab - ac - bc + abc\end{aligned}$$

所以交换律与结合律均满足。

---

3. 设 $M = \{1,2,3\}$,试为 M 规定一个满足结合律和交换律的代数运算,再规定一个满足交换律但不满足结合律的代数运算。

解 设 $a \circ b = \max\{a,b\}$,则它是 M 的一个代数运算,且

$$b \circ a = \max\{b,a\} = a \circ b$$

$$(a \circ b) \circ c = a \circ (b \circ c) = \max\{a,b,c\}$$

故 $a \circ b = \max\{a,b\}$ 为 M 的一个满足结合律和交换律的代数运算。

又设 $a \circ b = (|a - b|)!$,则它是 M 的一个代数运算,且

$$b \circ a = (|b-a|)! = (|a-b|)! = a \circ b$$

即满足交换律，又

$$(1 \circ 1) \circ 3 = 1 \circ 3 = 2$$

$$1 \circ (1 \circ 3) = 1 \circ 2 = 1$$

所以该运算不满足结合律。

---

4. 数域 F 上全体非零多项式的集合对于

$$f(x) \circ g(x) = (f(x), g(x))$$

是否满足结合律和交换律？其中 $(f(x), g(x))$ 表示 $f(x)$ 与 $g(x)$ 的首系数是 1 的最高公因式。

解 由 $g(x) \circ f(x) = (g(x), f(x)) = (f(x), g(x)) = f(x) \circ g(x)$

故满足交换律，又由最高公因式的性质可知

$$\begin{aligned}(f(x) \circ g(x)) \circ h(x) &= ((f(x), g(x)), h(x)) \\ &= (f(x), (g(x), h(x))) \\ &= f(x) \circ (g(x) \circ h(x))\end{aligned}$$

所以也满足结合律。

---

5. 证明本节定理 3：

设集合 M 有两个代数运算 $\circ$ 及 $\oplus$，其中 $\oplus$ 满足结合律，而 $\circ$ 对 $\oplus$ 满足左分配律，则对 M 中任意元素 a 及 $b_1, b_2, \cdots, b_n$ 有

$$a \circ (b_1 \oplus b_2 \oplus \cdots \oplus b_n) = (a \circ b_1) \oplus (a \circ b_2) \oplus \cdots \oplus (a \circ b_n)$$

证明 当 $n = 2$ 时，由 $\circ$ 对 $\oplus$ 满足左分配律，故

$$a \circ (b_1 \oplus b_2) = (a \circ b_1) \oplus (a \circ b_2)$$

设 $n = k$ 时，结论成立，即

$$a \circ (b_1 \oplus b_2 \oplus \cdots \oplus b_k) = (a \circ b_1) \oplus (a \circ b_2) \oplus \cdots \oplus (a \circ b_k)$$

当 $n = k+1$ 时，由 $\oplus$ 满足结合律且 $\circ$ 对 $\oplus$ 满足左分配律可知

$$\begin{aligned}&a \circ (b_1 \oplus b_2 \oplus \cdots \oplus b_k \oplus b_{k+1}) \\ &= a \circ ((b_1 \oplus b_2 \oplus \cdots \oplus b_k) \oplus b_{k+1}) \\ &= a \circ (b_1 \oplus b_2 \oplus \cdots \oplus b_k) \oplus (a \circ b_{k+1}) \\ &= (a \circ b_1) \oplus (a \circ b_2) \oplus \cdots \oplus (a \circ b_k) \oplus (a \circ b_{k+1})\end{aligned}$$

即 $n = k + 1$ 时结合律也成立，故由以上可知对 M 中任意元素 a 及 b_1，

$b_2,\cdots,b_n$，有

$$a\circ(b_1\oplus b_2\oplus\cdots\oplus b_n)=(a\circ b_1)\oplus(a\circ b_2)\oplus\cdots\oplus(a\circ b_n)$$

§5 同态与同构(P24)

1. 设 M 为实数集，代数运算是普通乘法。问：以下各映射是否为 M 的自同态映射？是否为自同态满射和自同构映射？说明理由。

$(1)x\longrightarrow|x|$， $(2)x\longrightarrow 2x$， $(3)x\longrightarrow x^2$， $(4)x\longrightarrow -x$。

解 $(1)x\circ y=xy\longrightarrow|xy|=|x||y|=|x|\circ|y|$，因此该映射是 M 的自同态映射，但不是满射，也不是单射。

$(2)x\circ y=xy\longrightarrow 2xy\neq(2x)\circ(2y)(xy\neq 0$ 时)，因此该映射不是 M 的自同态映射，当然不是自同构映射，但是双射。

$(3)x\circ y=xy\longrightarrow(xy)^2=x^2y^2=x^2\circ y^2$，因此该映射是 M 的自同态映射，但不是满射，也不是单射。

$(4)x\circ y=xy\longrightarrow-(xy)\neq(-x)\circ(-y)$，因此该映射不是 M 的自同态映射，当然不是自同构映射，但是双射。

---

2. 证明本节定理 2：

设集合 M 有代数运算 $\circ$ 及 $\oplus$，集合 $\overline{M}$ 有代数运算 $\bar{\circ}$ 及 $\bar{\oplus}$；又 φ 是 M 到 $\overline{M}$ 的一个满射，且对 $\circ$ 与 $\bar{\circ}$ 及 $\oplus$ 与 $\bar{\oplus}$ 同态，则当 $\circ$ 对 $\oplus$ 满足左(右)分配律时，$\bar{\circ}$ 对 $\bar{\oplus}$ 也满足左(右)分配律。

证明 任取 $\bar{a}$、$\bar{b}$、$\bar{c}\in\overline{M}$，由于 φ 为满射，故有 a、b、$c\in M$，使

$$a\longrightarrow\bar{a},b\longrightarrow\bar{b},c\longrightarrow\bar{c}$$

又由于 φ 对 $\circ$ 与 $\bar{\circ}$ 及 $\oplus$ 与 $\bar{\oplus}$ 同态，故

$$a\circ(b\oplus c)\longrightarrow\bar{a}\,\bar{\circ}\,\overline{(b\oplus c)}=\bar{a}\,\bar{\circ}\,(\bar{b}\,\bar{\oplus}\,\bar{c})$$

$$(a\circ b)\oplus(a\circ c)\longrightarrow\overline{(a\circ b)}\,\bar{\oplus}\,\overline{(a\circ c)}=(\bar{a}\,\bar{\circ}\,\bar{b})\,\bar{\oplus}\,(\bar{a}\,\bar{\circ}\,\bar{c})$$

又 $\circ$ 对 $\oplus$ 满足左分配律，故

$$a\circ(b\oplus c)=(a\circ b)\oplus(a\circ c)$$

所以有
$$\bar{a}\,\bar{\circ}\,(\bar{b}\oplus\bar{c})=(\bar{a}\circ\bar{b})\oplus(\bar{a}\circ\bar{c})$$

即 $\bar{\circ}$ 对 $\bar{\oplus}$ 也满足左分配律，同理可证当 $\circ$ 对 $\oplus$ 满足右分配律时，$\bar{\circ}$ 对 $\bar{\oplus}$ 也满足右分配律。

3. 设 Q 是有理数集，代数运算是普通加法，试给出 Q 的一个除恒等变换以外的自同构。

解 如

$$\varphi: x \longrightarrow kx \quad (\forall x \in Q)$$

其中 k 为某一有理数，且 $k \neq 0, k \neq 1$，则 φ 为 Q 的非恒等变换的自同构。

---

4. 设集合 M 有代数运算 $\circ$，集合 $\overline{M}$ 有代数运算 $\bar{\circ}$，且 $M \sim \overline{M}$，问：当 $\bar{\circ}$ 满足结合律时，$\circ$ 如何？

解 当 $\bar{\circ}$ 满足结合律时，$\circ$ 未必满足，如 M 为实数集，代数运算是普通减法，则该运算不满足结合律，又如 $\overline{M} = \{0\}$，代数运算为普通减法，该运算满足结合律，但显然有

$$\varphi: x \longrightarrow 0 \quad (\forall x \in M)$$

是 M 到 $\overline{M}$ 的同态满射，$M \sim \overline{M}$。

---

5. 设 M_1, M_2, M_3 是三个代数系统，证明：

(1) 若 $M_1 \cong M_2$，则 $M_2 \cong M_1$；

(2) 若 $M_1 \cong M_2, M_2 \cong M_3$，则 $M_1 \cong M_3$。

证明 (1) 由 $M_1 \cong M_2$ 可知，存在 M_1 到 M_2 的一个同构映射

$$\varphi: x \longrightarrow y \quad (\forall x \in M_1)$$

则显然 $\varphi^{-1}: y \longrightarrow x$ 也是 M_2 到 M_1 的一个同构映射(其中 $y = \varphi(x)$)，故

$$M_2 \cong M_1$$

(2) 由 $M_1 \cong M_2, M_2 \cong M_3$，故有 M_1 到 M_2 及 M_2 到 M_3 的同构映射 φ 与 ψ，且使

$$\varphi: a \longrightarrow b, \qquad \psi: b \longrightarrow c$$

则 $\psi\varphi: a \longrightarrow c$ 为 M_1 到 M_3 的同构映射，因此 $M_1 \cong M_3$。

§6 等价关系与集合的分类(P28)

1. 设 M 为整数集，规定

$$aRb \Leftrightarrow 4 \mid a + b$$

问：R 是否为 M 的一个关系？是否满足反身性、对称性和传递性？

解 R 是 M 的一个关系，例如，

因为 $4 \mid 1+3$，所以 $1R3$。又因为 $4 \nmid 1+4$，所以 $1\overline{R}4$，等等。显然这一

关系是满足对称性的，但由 $4 \nmid 1+1, 4 \nmid 3+3$ 等，可知 R 不满足反身性，又由$4 \mid 1+3, 4 \mid 3+5$，但$4 \nmid 1+5$，可知 R 不满足传递性。

---

2. 设 M 是实数集，问以下各关系是否为 M 的等价关系？

(1)$aRb \Leftrightarrow a \leqslant b$； (2)$aRb \Leftrightarrow ab \geqslant 0$；

(3)$aRb \Leftrightarrow a = b$； (4)$aRb \Leftrightarrow a^2 + b^2 \geqslant 0$。

解 (1) 不是等价关系，因为不满足对称性，如 $2R3$，但 $3\overline{R}2$。

(2) 不是等价关系，因为不满足传递性，如 $1R0, 0R(-1)$，但 $1\overline{R}(-1)$。

(3) 是等价关系，因为 $a = a$ 即 aRa，满足反身性，

aRb，即 $a = b$，故 $b = a$，bRa，满足对称性，

aRb, bRc，即 $a = b, b = c$，故 $a = c$，aRc，满足传递性。

(4) 是等价关系，因为

$a^2 + a^2 \geqslant 0$，即 aRa，满足反身性，

aRb，故 $a^2 + b^2 \geqslant 0$，即有 $b^2 + a^2 \geqslant 0$，bRa，满足对称性，

aRb, bRc，即 $a^2 + b^2 \geqslant 0, b^2 + c^2 \geqslant 0$，故有 $a^2 + c^2 \geqslant 0$，aRc，满足传递性。

---

3. 试指出上题中等价关系所决定的分类。

解 (3) 中每个实数是一个类；(4) 中所有的实数是一个类。

---

4. 分别举出三个例子各满足等价关系中的两个条件，而另一个条件不满足。

解 上面第2题中的(1)与(2)分别是不满足对称性和传递性而分别满足其他两个条件的例子。若设 M 是实数集，规定

$$aRb \Leftrightarrow ab \neq 0$$

则若 aRb，而$ab \neq 0$，则 $ba \neq 0$，bRa，满足对称性，若 aRb, bRc，即 $ab \neq 0$，$bc \neq 0$，则 $ac \neq 0$，aRc，满足传递性。

---

5. 设 M 是任意非空集合，并令

$$R = \{(a,b) \mid a, b \in M\}$$

证明：M 的一个关系决定 R 的一个子集，反之，R 的任一子集决定 M 的一个关系，且不同的关系决定 R 的两个不同的子集。

证明　M 中的两个元素 a、b 若符合 M 的一个关系，则记为 (a,b)，所有这样 (a,b) 构成集合 R_1，则它是 R 的一个子集，且不同的关系决定 R 的不同子集。

若 $R_2 \subseteq R$，即 R_2 为 R 的一个子集，规定关系 R

$$aRb \Leftrightarrow (a,b) \in R_2$$

则由子集 R_2 可确定 M 的一个关系。

---

6. 设 A、B 为集合 M 的任二非空子集，A' 与 B' 分别为 A 与 B 在 M 中的余集，证明：

(1) $A-B=A\cap B'$；

(2) $(A\cup B)-(A\cap B)=(A-B)\cup(B-A)$
$$=(A\cup B)\cap(A'\cup B')。$$

证明　(1) $\forall x\in A-B$，则 $x\in A$ 且 $x\notin B$，即 $x\in A$ 且 $x\in B'$，即 $x\in A\cap B'$，故 $A-B\subset A\cap B'$；$\forall x\in A\cap B'$，则 $x\in A$ 且 $x\in B'$，即 $x\in A$，且 $x\notin B$，故 $x\in A-B$，$A\cap B'\subset A-B$，因此 $A-B=A\cap B'$。

(2) 由(1) 及分配律，德·摩根律，有

$$(A\cup B)-(A\cap B)=(A\cup B)\cap(A\cap B)'$$
$$=(A\cup B)\cap(A'\cup B')$$

$$\begin{aligned}&(A-B)\cup(B-A)\\&=(A\cap B')\cup(B\cap A')\\&=[(A\cap B')\cup B]\cap[(A\cap B')\cup A']\\&=[(A\cup B)\cap(B'\cup B)]\cap[(A\cup A')\cap(B'\cup A')]\\&=(A\cup B)\cap(B'\cup A')\\&=(A\cup B)\cap(A'\cup B')\end{aligned}$$

所以 $(A\cup B)-(A\cap B)=(A-B)\cup(B-A)=(A\cup B)\cap(A'\cup B')$

---

7. 设 φ 是集合 X 到集合 Y 的任意一个映射，A 与 B 分别为 X 与 Y 的非空子集，证明

(1) $\varphi^{-1}(\varphi(A))\supseteq A$，且当 φ 为单射时等号成立；

(2)$\varphi(\varphi^{-1}(B)) \subseteq B$，且当 φ 为满射时等号成立。

证明 (1) $\forall x \in A$，则 $\varphi(x) \in \varphi(A)$，从而 $x \in \varphi^{-1}(\varphi(A))$，$A \subseteq \varphi^{-1}(\varphi(A))$。

若 φ 为单射时，$\forall y \in \varphi^{-1}(\varphi(A))$，则 $\varphi(y) \in \varphi(A)$，从而有 $x \in A$，使 $\varphi(x) = \varphi(y)$，又 φ 为单射，故 $x = y$，因此 $y \in A$，所以 $\varphi^{-1}(\varphi(A)) \subseteq A$，故 φ 为单射时等号成立，即 $A = \varphi^{-1}(\varphi(A))$。

(2) 任意 $y \in \varphi(\varphi^{-1}(B))$，存在 $x \in \varphi^{-1}(B)$，使 $\varphi(x) = y$，又由 $x \in \varphi^{-1}(B)$ 可知 $\varphi(x) \in B$，故 $y \in B$，$\varphi(\varphi^{-1}(B)) \subseteq B$。

当 φ 为满射时，$\forall y \in B$，则存在 $x \in X$，使 $\varphi(x) = y$，故 $x \in \varphi^{-1}(B)$，$\varphi(x) \in \varphi(\varphi^{-1}(B))$ 从而 $y \in \varphi(\varphi^{-1}(B))$，因此 $B \subseteq \varphi(\varphi^{-1}(B))$，所以 φ 为满射时等号成立，即 $B = \varphi(\varphi^{-1}(B))$。

---

8. 设 φ 是集合 X 到集合 Y 的一个映射，而 A 与 B 是 X 的任二非空子集。证明：

(1)$\varphi(A \cup B) = \varphi(A) \cup \varphi(B)$；

(2)$\varphi(A \cap B) \subseteq \varphi(A) \cap \varphi(B)$。

证明 (1) 任意的 $y \in \varphi(A \cup B)$，则存在 $x \in A \cup B$，使 $y = \varphi(x)$。若 $x \in A$，则 $\varphi(x) \in \varphi(A)$，若 $x \in B$，则 $\varphi(x) \in \varphi(B)$，从而 $\varphi(x) \in \varphi(A) \cup \varphi(B)$，即 $y \in \varphi(A) \cup \varphi(B)$，故 $\varphi(A \cup B) \subseteq \varphi(A) \cup \varphi(B)$。

反之，任意的 $y \in \varphi(A) \cup \varphi(B)$，即 $y \in \varphi(A)$ 或 $y \in \varphi(B)$。当 $y \in \varphi(A)$ 时，则存在 $x \in A$，使 $y = \varphi(x)$，而 $\varphi(x) \in \varphi(A) \subseteq \varphi(A \cup B)$，故 $y \in \varphi(A \cup B)$。

同理可证 $y \in \varphi(B)$ 时亦有 $y \in \varphi(A \cup B)$，所以

$$\varphi(A) \cup \varphi(B) \subseteq \varphi(A \cup B)$$

因此
$$\varphi(A \cup B) = \varphi(A) \cup \varphi(B)$$

(2) 任意 $y \in \varphi(A \cap B)$，则存在 $x \in A \cap B$，使 $\varphi(x) = y$。由于 $x \in A \cap B$，故 $x \in A$ 且 $x \in B$，所以 $\varphi(x) \in \varphi(A)$ 且 $\varphi(x) \in \varphi(B)$，因此 $y \in \varphi(A) \cap \varphi(B)$，从而 $\varphi(A \cap B) \subseteq \varphi(A) \cap \varphi(B)$。

---

9. 设 σ 与 τ 分别为集合 A 到 B 以及集合 B 到 C 的映射。证明：

(1) 若 σ、τ 都是单射，则 $\tau\sigma$ 是单射；反之，若 $\tau\sigma$ 是单射，则 σ 是单射；

(2) 若 σ、τ 都是满射，则 $\tau\sigma$ 是满射；反之，若 $\tau\sigma$ 是满射，则 τ 是满射。

证明 (1) 易知 $\tau\sigma$ 是集合 A 到 C 的映射，设 $x_1,x_2\in A$ 且 $x_1\neq x_2$，由 σ 是单射可知

$$\sigma(x_1)\neq\sigma(x_2)$$

又因为 τ 是单射，故

$$\tau(\sigma(x_1))\neq\tau(\sigma(x_2))$$

即 $(\tau\sigma)(x_1)\neq(\tau\sigma)(x_2)$，所以 $\tau\sigma$ 是集合 A 到 C 的单射。

反之，若 $\tau\sigma$ 是 A 到 C 的单射，设 $x_1,x_2\in A$，且 $x_1\neq x_2$，则

$$(\tau\sigma)(x_1)\neq(\tau\sigma)(x_2)$$

即 $\tau(\sigma(x_1))\neq\tau(\sigma(x_2))$，从而 $\sigma(x_1)\neq\sigma(x_2)$（否则与 $\tau\sigma$ 为单射矛盾），故 σ 是 A 到 B 的单射。

(2) 若 σ、τ 都是满射，则任意的 $y\in C$，由 τ 是 B 到 C 的满射，故存在 $y'\in B$，使 $\tau(y')=y$，又 σ 是 A 到 B 的满射，故存在 $x\in A$，使 $\sigma(x)=y'$。从而

$$y=\tau(y')=\tau(\sigma(x))=(\tau\sigma)(x)$$

所以 $\tau\sigma$ 是 A 到 C 的满射。

反之，若 $\tau\sigma$ 是 A 到 C 的满射，则任意的 $y\in C$，必存在 $x\in A$，使

$$(\tau\sigma)(x)=\tau(\sigma(x))=y$$

令 $y'=\sigma(x)$，则 $y'\in B$ 且 $\tau(y')=y$，从而 τ 是集合 B 到 C 的满射。

---

10. 设 σ 是集合 A 到 B 的一个映射，证明：

(1) σ 是单射 $\Leftrightarrow$ 存在 B 到 A 的映射 τ，使 $\tau\sigma=1_A$；

(2) σ 是满射 $\Leftrightarrow$ 存在 B 到 A 的映射 τ，使 $\sigma\tau=1_B$，其中 1_A、1_B 分别为集合 A、B 的恒等映射。

证明 (1) 必要性

若 σ 是单射，令 $B'=\{b'\mid b'\in B,b'\notin\sigma(A)\}$，则

$$B=B'\cup\sigma(A)\text{ 且 }B'\cap\sigma(A)=\varnothing$$

由 σ 是单射，则当 $b\in\sigma(A)$ 时，必存在惟一的 $a\in A$，使得 $b=\sigma(a)$，现取定某一 $a_0\in A$，令

$$\tau: b\longrightarrow a\quad(b\in\sigma(A)\text{ 时})$$
$$b'\longrightarrow a_0\quad(b\in B'\text{ 时})$$

则 τ 是从集合 B 到集合 A 的一个映射，且对任意的 $a\in A$，均有

$$(\tau\sigma)(a)=a$$

即 $$\tau\sigma = 1_A$$

充分性

若存在从 B 到 A 的映射 τ，使得 $\tau\sigma = 1_A$，因为 1_A 也是单射，故由上一题结论知 σ 是单射。

(2) 必要性

若 σ 是满射，则对任意的 $b \in B$，在 A 的子集 $\sigma^{-1}(b)$ 中任意取定一个 a，令

$$\tau: b \longrightarrow a$$

其中 $\sigma(a) = b$，则 τ 是一个从 B 到 A 的映射，且对任 $b \in B$，有

$$(\sigma\tau)(b) = \sigma(\tau(b)) = \sigma(a) = b$$

即 $$\sigma\tau = 1_B$$

充分性

若存在从 B 到 A 的映射 τ，使 $\sigma\tau = 1_B$，则由于 1_B 也是满射及上一题的结论可知 σ 是满射。

---

11. 设 σ 是集合 A 到集合 B 的一个映射，证明：

(1) σ 是单射 $\Leftrightarrow$ 对任意集合 X 到 A 的任意映射 τ_1、τ_2，若有 $\sigma\tau_1 = \sigma\tau_2$，必有 $\tau_1 = \tau_2$；

(2) σ 是满射 $\Leftrightarrow$ 对任意集合 Y 与 B 到 Y 的任意映射 τ_1、τ_2，若有 $\tau_1\sigma = \tau_2\sigma$，则有 $\tau_1 = \tau_2$。

证明 (1) 必要性

若 σ 是单射，τ_1，τ_2 为从任意集合 X 到 A 的任意映射，且 $\sigma\tau_1 = \sigma\tau_2$，任取 $a \in X$，则

$$(\sigma\tau_1)(a) = (\sigma\tau_2)(a)$$

即 $\sigma(\tau_1(a)) = \sigma(\tau_2(a))$，又 σ 是单射，故必有 $\tau_1(a) = \tau_2(a)$，从而 $\tau_1 = \tau_2$。

充分性

对任意集合 X 到 A 的任意映射 τ_1、τ_2，若由 $\sigma\tau_1 = \sigma\tau_2$，可得 $\tau_1 = \tau_2$，则 σ 必是单射。

否则，则存在 $a_1, a_2 \in A$，$a_1 \neq a_2$，但有 $\sigma(a_1) = \sigma(a_2)$，令 $X = A$，及

$$\tau_1: x \longrightarrow a_1, \quad \tau_2: x \longrightarrow a_2 \quad (\forall x \in X)$$

则有

$$(\sigma\tau_1)(x) = \sigma(\tau_1(x)) = \sigma(a_1)$$

$$(\sigma\tau_2)(x)=\sigma(\tau_2(x))=\sigma(a_2)$$

从而由 $\sigma(a_1)=\sigma(a_2)$ 可得 $(\sigma\tau_1)(x)=(\sigma\tau_2)(x)$，故 $\sigma\tau_1=\sigma\tau_2$，进而由题设知 $\tau_1=\tau_2$，又 $\tau_1(x)=a_1$，$\tau_2(x)=a_2$ 及 $a_1\neq a_2$ 知 $\tau_1(x)\neq\tau_2(x)$，进而 $\tau_1\neq\tau_2$，矛盾，所以 σ 必为单射。

(2) 必要性

设 σ 为满射，则对任意 $b\in B$，存在 $a\in A$，使 $\sigma(a)=b$，又对任意集合 Y 与 B 到 Y 的任意映射 τ_1、τ_2，有 $\tau_1\sigma=\tau_2\sigma$，故

$$(\tau_1\sigma)(a)=(\tau_2\sigma)(a),\tau_1(b)=\tau_2(b)$$

所以 $\tau_1=\tau_2$。

充分性

设对任意集合 Y 与 B 到 Y 的任意映射 τ_1、τ_2，若 $\tau_1\sigma=\tau_2\sigma$，必有 $\tau_1=\tau_2$，则 σ 为满射，否则

$$B'=B-\sigma(A)\neq\varnothing$$

任取集合 Y，使 $|Y|\geqslant 2$，取定 $y_1,y_2,y\in Y$ 且 $y_1\neq y_2$，则对 $b\in\sigma(A)$，$b'\in B'$，令

$$\tau_1:b\longrightarrow y,b'\longrightarrow y_1$$
$$\tau_2:b\longrightarrow y,b'\longrightarrow y_2$$

则 τ_1 与 τ_2 是 B 到 Y 中的两个不同映射。且对任意的 $a\in A$，均有

$$(\tau_1\sigma)(a)=\tau_1(\sigma(a))=y$$
$$(\tau_2\sigma)(a)=\tau_2(\sigma(a))=y$$

故 $\tau_1\sigma=\tau_2\sigma$，由题设必有 $\tau_1=\tau_2$，这同 τ_1 与 τ_2 是 B 到 Y 中的两个不同映射相矛盾。所以，σ 必为满射。

---

12. 设 A 是一个非空集合，$P(A)$ 是 A 的幂集，即由 A 的一切子集作成的集合，证明：在 $P(A)$ 与 A 间不存在双射。

证明 若 $P(A)$ 与 A 间存在双射 φ，令

$$A_1=\{\varphi(M)\mid M\in P(A),\varphi(M)\notin M\}$$

下面考查 $\varphi(A_1)$。

若 $\varphi(A_1)\in A_1$，则由集合 A_1 的定义可知 A_1 中不存在 $\varphi(A_1)$，矛盾；

若 $\varphi(A_1)\notin A_1$，则由 A_1 的定义知 $\varphi(A_1)\in A_1$，也矛盾。

所以 $P(A)$ 与 A 之间不存在双射。

第二章 群

导读

一、基本要求

1. 熟练掌握群和半群的基本概念,理解群的几个等价定义;
2. 理解并掌握单位元、逆元、消去律的概念;
3. 掌握置换群、变换群、循环群的基本知识和结构性质;
4. 熟练掌握子群的定义及性质,掌握商群的结构;
5. 理解并掌握 Lagrange 定理。

二、重点与难点

1. 群的概念、变换群、置换群、循环群、不变子群、群的同态;
2. 群的几个等价定义;
3. 子群的陪集;
4. 群同态基本定理。

知识点考点精要

一、群的相关定义

1. 群的定义

设 G 是一个非空集合,$\circ$ 是它的一个代数运算,如果满足以下条件:

(1) 结合律成立,即对 G 中任意元素 a、b、c,都有

$$(a\circ b)\circ c=a\circ(b\circ c)$$

(2)G 中有元素 e,叫做 G 的左单位元,它对 G 中每个元素 a 都有

$$e\circ a=a$$

(3) 对 G 中每个元素 a,在 G 中都有元素 a^{-1},叫做 a 的左逆元,使

$$a^{-1}\circ a=e$$

则称 G 对代数运算 $\circ$ 作成一个群。

群 G 中若任 $a,b\in G$,均有

$$a\circ b=b\circ a$$

则称 G 为交换(可换)群或 Abel 群,否则称为非交换(可换)群或非 Abel 群。

2. 群的阶

若群 G 中所含的元素个数为有限数 n,则称 n 为群 G 的阶,记作 $|G|=n$,此时群 G 称为有限群;否则,称群 G 是无限群,无限群的阶称为无限。

3. 若干群的例子

(1) 非零有理数乘群

全体非零有理数对数的普通乘法作成的群。

(2) 正有理数乘群

全体正有理数对数的普通乘法作成的群。

(3) 一般线性群

数域 F 上全体 n 阶满秩方阵对矩阵的普通乘法(或 F 上 n 维线性空间的全体满秩线性变换对线性变换的乘法)作成的群,称之为 F 上的一般线性群或 F 上的 n 阶线性群,记作 $GL_n(F)$。

(4)n 次单位根群

全体 n 次单位根对于数的普通乘法作成的群,记作 U_n,实际上它是 n 阶有限交换群。

(5) 四元数群

令 $$G=\{1,i,j,k,-1,-i,-j,-k\}$$

并规定 G 的乘法

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

$(-x)y = x(-y) = -xy$,
$-(-x) = x$,
其中 $x, y \in \{1, i, j, k\}$。

则 G 对上述规定的乘法作成的群，称为四元数群。实际上它是一个 8 阶非交换群。

4. 群的性质

(1) 群 G 的元素 a 的左逆元 a^{-1} 也是 a 的一个右逆元。即有

$$a^{-1}a = aa^{-1} = e$$

(2) 群 G 的左单位元 e 也是 G 的一个右单位元，即对群 G 中任意元素 a 均有

$$ea = ae = a$$

注 据此性质，称 e 为群 G 的单位元。

(3) 群 G 的单位元及每个元素的逆元都是惟一的。

(4) 在群中消去律成立，即

$$ab = ac \Rightarrow b = c$$
$$ba = ca \Rightarrow b = c$$

5. 半群的定义

设 S 是一个非空集合。若它有一个代数运算满足结合律，则称 S 是一个半群。

类似于群中的定义，可定义半群中的左单位元及右单位元，有单位元（既是左单位元又是右单位元）的半群称为幺半群。

在半群中，左、右单位元可能都不存在，可能只存在一个，在两个都存在时，二者必相等且为半群的惟一单位元。

6. 群的等价定义

(1) 设 G 是一个半群，则 G 作成群的充要条件是：

①G 中有右单位元 e：即 $\forall a \in G$，均有

$$ae = a$$

②G 中每个元素 a 都有右逆元 a^{-1}，即

$$aa^{-1} = e$$

(2) 设 G 是一个半群，则 G 作成群的充要条件是：$\forall a,b \in G$，方程

$$ax=b, ya=b$$

在 G 中均有解。

(3) 有限半群 G 作成群的充要条件是在 G 中两个消去律成立。

三、元素的阶及阶的性质

1. 元素阶的定义

设 G 为群，$a \in G$，使

$$a^n = e$$

的最小正整数 n，称为元素 a 的阶，记为 $|a| = n$。

若这样的 n 不存在，则称元素 a 的阶为无限(或为零)。

2. 周期群、无扭群及混合群

若群 G 中每个元素的阶都有限，则称 G 为周期群；

若群 G 中除 e 外(阶为 1)，其余元素的阶均无限，则称 G 为无扭群；

既非周期群又非无扭群的群，称为混合群。

3. 有关元素阶的性质及相关结果

(1) 有限群中每个元素的阶均有限

(2) 设群 G 中元素 a 的阶为 n，则

$$a^m = e \Leftrightarrow n \mid m$$

(3) 设群 G 中 a 的阶是 n，则

$$|a^k| = \frac{n}{(k,n)}$$

其中 k 为任意整数。

(4) 设群 G 中 $|a| = st$，则 $|a^s| = t$，其中 s,t 为正整数。

(5) 设群 G 中 $|a| = n$，则

$$|a^k| = n \Leftrightarrow (k,n) = 1$$

(6) 设群 G 中 $|a| = m$，$|b| = n$，则当 $ab = ba$ 且 $(m,n) = 1$ 时

$$|ab| = mn$$

(7) 设 G 为交换群，且 G 中所有元素有最大阶 m，则 G 中每个元素的阶都是 m 的因数，从而群 G 中每个元素均满足 $x^m = e$。

三、子群与中心

1. 相关定义

(1) 子群

设G是一个群，H是G的一个非空子集。如果H本身对G的乘法也作成一个群，则称H为群G的一个子群。记作$H\leqslant G$。

注 $|G|>1$时，G的两个子群$\{e\}$及G本身称为G的平凡子群，若存在其他子群H，称为真子群或非平凡子群，记作$H<G$。

(2) 中心元素

设G是一个群，G中元素a如果同G中每个元素都可换，则称a是群G的一个中心元素。

注 群G的单位元e总是群G的中心元素。若除e外G无其他中心元素，则称G是无中心群。

(3) 集合的乘法与逆

设A、B为群G的非空子集，记

$$AB=\{ab\mid a\in A,b\in B\},A^{-1}=\{a^{-1}\mid a\in A\}$$

则分别称AB为A与B的乘积，A^{-1}为A的逆。

注 对群G的任非空集合A、B、C，有

$$(AB)C=A(BC),A(B\cup C)=AB\cup AC$$

$$(AB)^{-1}=B^{-1}A^{-1},(A^{-1})^{-1}=A$$

2. 群与其子群间的联系

设G是一个群，$H\leqslant G$，则子群H的单位元就是群G的单位元，H中元素a的逆元就是a在G中的逆元。

3. 子群的判定定理

(1)$H\subseteq G,H\neq\varnothing$，则$H\leqslant G$的充要条件是：

①$a,b\in H\Rightarrow ab\in H$；

②$a\in H\Rightarrow a^{-1}\in H$。

(2)$H\subseteq G,H\neq\varnothing$，则$H\leqslant G$的充要条件是：

$$a,b\in H,ab^{-1}\in H$$

(3)$H\subseteq G,H\neq\varnothing$，则$H\leqslant G$的充要条件是：

$$HH=H\text{ 且 }H^{-1}=H$$

(4) $H\subseteq G,H\neq\varnothing$，则 $H\leqslant G$ 的充要条件是：

$$HH^{-1}=H$$

(5) $H\subseteq G,H\neq\varnothing$，且 $|H|$ 有限，则 $H\leqslant G$ 的充要条件是：

$$HH=H$$

(6) 设 $H\leqslant G,K\leqslant G$，则

$$HK\leqslant G\Leftrightarrow HK=KH$$

4. 特殊子群

群 G 的全体中心元素作成的集合 $C(G)$ 是 G 的一个子群，称为群 G 的中心，可简记为 C。

注 $C(G)$ 是一个交换子群；且 G 是交换群 $\Leftrightarrow C(G)=G$。

四、循环群

1. 定义

(1) 生成系

称 $\langle M\rangle$ 为群 G 中由子集 M 生成的子群，并称 M 为 $\langle M\rangle$ 的生成系。

(2) 循环群

若群 G 可由一个元素 a 生成，即 $G=\langle a\rangle$，则称 G 为由 a 生成的循环群，其中 a 称为 G 的一个生成元。

注 循环群必是交换群。

2. 循环群的结构

设 G 是循环群，即 $G=\langle a\rangle$，则

(1) 当 $|a|=\infty$ 时，由 $s\neq t$ 可得 $a^s\neq a^t$，即

$$\cdots,a^{-2},a^{-1},e,a,a^2,\cdots$$

是 $\langle a\rangle$ 的全体互异的元素。

(2) 当 $|a|=n$ 时，$\langle a\rangle$ 是 n 阶群，且

$$\langle a\rangle=\{e,a,a^2,\cdots,a^{n-1}\}$$

3. 一个常用的循环群判定定理

n 阶群是循环群 $\Leftrightarrow G$ 有 n 阶元素。

注 n 阶循环群的一个元素是不是生成元，只需判定这个元素的阶是否是 n。

4. 循环群的生成元

(1) 无限循环群$\langle a\rangle$有两个生成元，即 a 与 a^{-1}；

(2)n 阶循环群$\langle a\rangle$有 $\varphi(n)$ 个生成元，其中 $\varphi(n)$ 为 Euler 函数。

5. 循环群的同构定理

设$\langle a\rangle$是任意一个循环群

(1) 若 $|a|=\infty$，则$\langle a\rangle$与整数加群 Z 同构；

(2) 若 $|a|=n$，则$\langle a\rangle$与 n 次单位根群 U_n 同构(或与以 n 为模的剩余类加群 Z_n 同构)。

注 ① 无限循环群间彼此同构，有限同阶循环群间彼此同构。

② 在同构意义下，循环群仅有两种，即整数加群 Z 与 n 次单位根群(或剩余类加群 Z_n)。

6. 循环群的子群

(1) 循环群的子群仍为循环群

(2) 无限循环群有无限多个子群

当$\langle a\rangle$为 n 阶循环群时，对 n 的每个正因数 k，$\langle a\rangle$有且只有一个 k 阶子群，这个子群就是$\langle a^{\frac{n}{k}}\rangle$。

(3)n 阶循环群有且仅有 $T(n)$ 个子群

五、变换群

1. 变换群与对称群定义

① 变换群

设 M 是一个非空集合。则由 M 的若干个变换关于变换的乘法所作成的群，称为 M 的一个变换群；

由 M 的若干个双射变换关于变换的乘法作成的群，称为 M 的一个双射变换群；

由 M 的若干个非双射变换关于变换的乘法作成的群，称为 M 的一个非双射变换群。

② 对称群

设 M 为任一非空集合，$S(M)$ 为由 M 的全体双射变换作成的集合，则 $S(M)$ 关于变换的乘法作成一个群，这一双射变换群 $S(M)$ 称为 M 上的对称群。当 $|M|=n$ 时，其上的对称群用 S_n 表示，并称为 n 次对称群。

2. 双射变换群的一个判定

设 G 是非空集合 M 的一个变换群。则 G 是 M 的一个双射变换群的充要条件是在 G 中含有 M 的单(满)射变换。

由这一判定可知：设 G 是集合 M 的一个变换群。则 G 或是 M 的双射变换群(其单位元必是恒等变换)，或是 M 的非双射变换群。即在 M 的任意一个变换群中，不可能既含有 M 的双射变换又含有 M 的非双射变换。

3. 抽象群与变换群之间的联系

Cayley 定理

任何群都同一个(双射)变换群同构。

由 Cayley 定理可知：

任何 n 阶有限群都同 n 次对称群 S_n 的一个子群同构。

六、置换群

1. 基本定义及性质

(1) 定义

① 置换群

n 次对称群 S_n 的任意一个子群，均称为一个 n 次置换群。简称置换群。

② 循环

一个置换 σ 如果把数码 i_1 变成 i_2，i_2 变成 i_3，…，i_{k-1} 变成 i_k，又把 i_k 变成 i_1，但别的元素(若存在)都不变，则称 σ 是一个 k- 循环置换，简称 k- 循环或循环，并记作

$$\sigma = (i_1 i_2 \cdots i_k) = (i_2 i_3 \cdots i_k i_1) = \cdots = (i_k i_1 \cdots i_{k-1})$$

③1- 循环

恒等置换称为 1- 循环，记作

$$(1) = (2) = \cdots = (n)$$

④ 对换

2- 循环称为对换。

⑤ 不相连循环

无公共元素的循环称为不相连循环。

(2) 相关性质

① 不相连循环相乘时可以交换。

② 每个(非循环)置换都可表为不相连循环之积;每个循环都可表为对换之积,因此每个置换都可表为对换之积。

注 把一个置换表成对换的乘积时,表示法不是惟一的。

③ 每个置换表成对换的乘积时,其对换个数的奇偶性不变。

2. 奇置换与偶置换

(1) 定义

一个置换若分解成奇数个对换的乘积时,称为奇置换;否则称为偶置换。

(2) 奇(偶)置换的判定

σ是奇(偶)置换的充要条件是$\sigma(1)\sigma(2)\cdots\sigma(n)$是奇(偶)排列,即其反序数是奇(偶)数。

(3)n 次交代群定义

n 次对称群 S_n 中全体偶置换所作成的一个$\frac{n!}{2}$阶的子群,称为 n 次交代(交错)群,记作 A_n。

(4) 置换群中奇、偶置换的特征

① 一个 n 次置换群中的置换或者全是偶置换,或者奇、偶置换各占一半。

② 若 n 次置换群中包含有奇置换,则 $|G|$ 是一个偶数。

3. 置换的阶的判定

(1)k- 循环的阶为 k,不相连循环乘积的阶为各因子的阶的最小公倍。

(2) 设有 n 次置换 $\tau=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$,则对任意 n 次置换σ,有

$$\sigma\tau\sigma^{-1}=\begin{pmatrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n)\end{pmatrix}$$

从而当 τ 表成循环的乘积时,把出现在 τ 中各循环中的数码 i 换成$\sigma(i)$后即得 $\sigma\tau\sigma^{-1}$。

4. n 次对称群的中心

(1)$n=1$、2 时,S_1 与 S_2 都是交换群,其中心均为自身;

(2)$n\geqslant 3$ 时,n 次对称群 S_n 的中心为恒等置换,即 S_n 是一个无中心群。

5. 传递群

(1) 定义

设 G 是集合 $M=\{1,2,\cdots,n\}$ 上的一个置换群。若对 M 中任意两组 k 个互异数码 $i_1,i_2,\cdots,i_k$ 与 $j_1,j_2,\cdots,j_k(1\leqslant k\leqslant n)$，在 G 中均有置换 τ，使

$$\tau(i_1)=j_1,\tau(i_2)=j_2,\cdots,\tau(i_k)=j_k$$

则称 G 为一个 k 重传递群(可迁群)。

注 ①1 重传递群，即对 M 中任意数码 i 与 j 在 G 中都有置换 τ，使

$$\tau(i)=j$$

时，则称 G 为传递群或可迁群。

②k 重传递群$(2\leqslant k<n)$ 必是一个 $k-1$ 重传递群。

(2)k 重传递群的判定

①$M=\{1,2,\cdots,n\}$ 上置换群 G 是 $k(1\leqslant k\leqslant n)$ 重传递群的充要条件是，对 M 中任意 k 个互异的数码 $j_1,j_2,\cdots,j_k$，在 G 中有置换 τ 使

$$\tau(1)=j_1,\tau(2)=j_2,\cdots,\tau(k)=j_k$$

②M 上置换群 G 是传递群的充要条件是对 M 中任意数码 j，存在 $\tau\in G$，使

$$\tau(1)=j$$

七、陪集

1. 定义

设 G 为群，$H\leqslant G$，$a\in G$，则称群 G 的子集

$$aH=\{ax\mid x\in H\}$$

为群 G 关于子群 H 的一个左陪集，称

$$Ha=\{xa\mid x\in H\}$$

为群 G 关于子群 H 的一个右陪集。

2. 左陪集的性质

(1)$a\in aH$

(2)$a\in H\Leftrightarrow aH=H$

(3)$b\in aH\Leftrightarrow aH=bH$

(4)$aH=bH\Leftrightarrow a^{-1}b\in H$(或 $b^{-1}a\in H$)

(5)$aH\cap bH\neq\varnothing$，则 $aH=bH$

右陪集性质类似。

3. 左陪集分解

若用 $aH, bH, cH, \cdots$ 表示子群 H 在 G 中的所有不同的左陪集，则有等式

$$G = aH \cup bH \cup cH \cup \cdots$$

称其为群 G 关于子群 H 的左陪集分解，称 $\{a, b, c, \cdots\}$ 为 G 关于 H 的一个左陪集代表系，类似可得右陪集分解定义。

4. 左、右陪集间的关系

设 G 为一个群，$H \leqslant G$，又令

$$L = \{aH \mid a \in G\}, R = \{Ha \mid a \in G\}$$

则在 L 与 R 之间存在一个双射，从而左、右陪集的个数都有限且相等或者都无限。

注 由此结论可知：

$$G = aH \cup bH \cup cH \cup \cdots \Leftrightarrow G = Ha^{-1} \cup Hb^{-1} \cup Hc^{-1} \cup \cdots$$

八 指数

1. 定义

群 G 中关于子群 H 的互异的左(或右)陪集的个数叫做 H 在 G 中的指数，记为

$$(G : H)$$

2. 性质

(1) 设 H, K 是群 G 的两个子群。则群 G 关于交 $H \cap K$ 的所有左陪集，就是关于 H 与 K 的左陪集的所有非空的交。

(2) $(G : H)$ 与 $(G : K)$ 都有限时，$(G : H \cap K)$ 有限且

$$(G : H \cap K) \leqslant (G : H) \cdot (G : K)$$

(3) 设 G 为群，$H \leqslant G, K \leqslant G$，则 $(G : H)$ 与 $(G : K)$ 均有限时，指数 $(G : H \cap K)$ 也有限。

九 子群的阶、指数和群的阶之间的关系

1. Lagrange 定理

设 H 是有限群 G 的一个子群，则

$$|G|=|H|(G:H)$$

从而任何子群的阶和指数都是群 G 的阶的因数。

2. 有限群中每个元素的阶都整除群的阶

3. 设 G 为有限群，$K\leqslant H\leqslant G$，则

$$(G:H)(H:K)=(G:K)$$

4. 陪集分解的一个应用

(1) 设 G 为群，$H\leqslant G$，$K\leqslant G$，且 H、K 有限，则

$$|HK|=\frac{|H|\cdot|K|}{|H\cap K|}$$

(2) 设 p，q 是两个素数且 $p<q$，则 pq 阶群 G 至多有一个 q 阶子群。

注　这样的群的 p 阶子群可能有多个。

释疑解惑

一、两个常用的符号 $\varphi(n)$ 与 $T(n)$

1. $\varphi(n)$ 为欧拉函数，其值是在 $0,1,2,\cdots,n-1$ 中与 n 互素的整数的个数。

2. $T(n)$ 是 $n(n>1)$ 的正因数的个数，若 n 的标准分解为

$$n=p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}$$

则 n 的正因数个数为

$$T(n)=(k_1+1)(k_2+1)\cdots(k_m+1)$$

二、关于群的定义的理解

1. 群的定义是多种的，需据具体情况而定选择哪一定义方式。在教材的定义中，验证非空集合 G 关于一个乘法运算是否作成群，一般必须检验乘法的封闭性、结合律、单位元的存在及逆元的存在。

在教材中群的定义方法可称为“左左”定义法。若把其中左单位元换成右单位元，把左逆元换成右逆元，其余不变，这样也可得到群的另一定义方式，通常称为“右右”定义法。这是两种定义方法，不可混在一起。例如

不可要求有“左”单位元而每个元素有“右”逆元。如，

令 $G=\{x,y\}$，规定其运算为 $ab=b(\forall a,b\in G)$，则 G 作成半群，且 x 是 G 的左单位元，又由

$$xx=x,yx=x$$

知 x 与 y 的右逆元均为 x，但 G 并不是群。

因为由 G 中的另两个运算

$$yy=y,xy=y$$

可知对左单位元 x 而言，x 有左逆元 x 与 y，而 y 却无左逆元。

因此尽管对 G 的左单位元 x 而言，x 有左逆元 x 与 y，但 G 作不成群。

这一例子同样可说明在群的“左左”定义中，“每个元素都有左逆元”是针对同一个左单位元来说的。

如果对单位元不分左右，而改为“G 中存在单位元 e”，对逆元也不分左右，改为“$\forall a\in G$，存在 $a'\in G$，使 $aa'=a'a=e$”，其余不变，这也可作为群的定义，通常称为“双边”定义法。

在群的“方程定义法”中（教材定理 5），需要求两个方程 $ax=b$ 与 $ya=b$ 均有解，若交换律不满足，其中一个方程有解并不能保证另一个方程也有解。

2. 结合律的验证是对 G 中任意三个元素而言的，对于无限群，必须做一般性验证，对于有限群，则需讨论所有情形而不遗漏。

3. 关于消去律

在群中消去律成立是由于每一元素均有逆元。但消去律成立的代数系统未必每一元素有逆元，如$\{Z;\cdot\}$中消去律成立，但除 ±1 外其他元素没有逆元，但对一个有限半群而言，消去律则可充分保证每一元素有逆元。而消去律成立与否，从乘法表便可得出。若乘法表中每行和每列中的元素互异，即可知成立。

由群中消去律的成立还可得出其他系列结果，如：方程 $ax=b$，$ya=b$ 在 G 中解惟一；群和子群的单位元和逆元相同等。

三、群 G 中元素 a，b 与 ab 的阶

一般来说，$|a|$ 与 $|b|$ 决定不了 $|ab|$，这是由于 $c=ab$ 为 G 中另一元素。只有在特殊情况下，如 $ab=ba$、$|a|$、$|b|$ 有限且 $(|a|,|b|)=$

1 时才可决定 $|ab|=|a||b|$（见教材 §2 定理 4）。

四、子群具有传递性

若 $E\leqslant F,F\leqslant G$，则有 $E\leqslant G$，这由子群的判定可得。

但是应注意，若 H 与 G 是两个群，$H\subseteq G$，未必有 $H\leqslant G$，这是因为子群的代数运算须与原群的代数运算一致。若虽有 $H\subseteq G$，但群 G 与群 H 有不同的代数运算，则 H 不是 G 的子群。例如，取 G 为有理数加群，H 为有理数乘群，作为集合有 $H\subseteq G$，但显见 H 不是 G 的子群。

五、关于循环群的理解

循环群是一类完全弄清楚的群，主要体现在以下几个方面。

1. 循环群的元素表示形式和运算方法完全确定，循环群生成元的状况也完全清楚。

(1) 循环群元素 a 的阶具有下列重要性质：

若 $|a|=n$，则

①$a^m=e\Leftrightarrow n|m$；

②$a^{m_1}=a^{m_2}\Leftrightarrow n|m_1-m_2$；

若 $|a|=\infty$，则

③$a^{m_1}=a^{m_2}\Leftrightarrow m_1=m_2$。

在教材 §4 定理 3 中指出，生成元 a 的阶完全决定了循环群的构造。

(2) 循环群的生成元通常是不惟一的，但有

① 无限循环群 $G=\langle a\rangle$，有且仅有两个生成元 a 与 a^{-1}；

②n 阶循环群 $G=\langle a\rangle$，有 $\varphi(n)$ 个生成元，且

$$a^r\text{ 是生成元}\Leftrightarrow(r,n)=1$$

这一结果是找循环群的生成元的有效依据，如，Z_9 的生成元有 $\bar{1},\bar{2},\bar{4},\bar{5},\bar{7},\bar{8}$ 共 6 个。

2. 循环群的子群状况完全清楚

(1) 循环群 $G=\langle a\rangle$ 的子群 H 也是循环群。若 $H\neq\{e\}$，则 H 是由 H 中元素 a 的最小正整数幂 a^s 生成的。

(2) 若 $G=\langle a\rangle$ 是无限群时，子群 $H(\neq\{e\})$ 也是无限群，且存在非负整数集到 $G=\langle a\rangle$ 的所有子群构成的集的双射。

(3) 若 $G = \langle a \rangle$ 是 n 阶有限群时，则子群 H 的阶必为 n 的正约数，且对于 n 的任一正约数 d，$G = \langle a \rangle$ 有且仅有一个阶为 d 的子群。

应当注意，循环群的子群是循环群，但反之不真，即一个群若除自身外所有子群都是循环群，而这个群未必是循环群。如 Klein 四元群 K_4 它的子群(除 K_4)皆为 1 阶和 2 阶的，故都是循环群，但 K_4 不是循环群，这是因为 K_4 中没有 4 阶元素。四元数群也是这种群的例子。

3. 在同构意义下循环群只有两类：一类是无限循环群，都与整数加群 Z 同构；另一类是 n 阶循环群，都与 n 次单位根群 U_n 同构(也与以 n 为模的剩余类加群同构)。因此，在需要讨论循环群的某个性质时，只要就具体的整数加群 Z 和单位根群 U_n 或剩余类加群 Z_n 讨论即可。

关于循环群的自同构，由于同构映射下生成元映射成生成元，故很容易决定循环群的自同构。

无限循环群 $G = \langle a \rangle$ 有且只有两个自同构：

$$\varphi_1 : a \longrightarrow a \text{ 及 } \varphi_2 : a \longrightarrow a^{-1}$$

n 阶循环群 $G = \langle a \rangle$ 的自同构的个数与其生成元个数相等，即 $\varphi(n)$ 个。

六、集合 M 上的双射变换群 G 的单位元必是 M 的恒等变换

设 e 为 G 的单位元，则 $\forall \tau \in G$，有

$$\tau e = \tau$$

故 $\forall x \in M$，有

$$(\tau e)(x) = \tau(e(x)) = \tau(x)$$

而 τ 为 M 的双射变换，故 $ex = x$，即 e 为 M 的恒等变换。

实际上我们有：若 G 是集合 M 的若干变换所作成的集合，且 G 包含恒等变换，若 G 对于变换的乘法作成一个群，则 G 只能包含 M 的双射变换。

七、关于 Cayley 定理(§5 定理 3)

给定一个群 G，G 的变换群可能不止一个，但其中有一个和 G 的关系密切，即与 G 是同构的，这个与 G 同构的变换群是怎样决定的，Cayley 的证明做了回答。定理证明的思路是：先找出一个由 G 的双射变换组成的集合 $\overline{G}$，再证明 $\overline{G}$ 是群(即变换群)且 G 与 $\overline{G}$ 同构。证明中给出的 $\overline{G}$ 为

$$\overline{G} = \{\tau_a \mid a \in G\}$$

其中 $\forall a \in G, \tau_a : x \longrightarrow ax (\forall x \in G)$，且 G 到 $\overline{G}$ 的双射定义为 $\varphi : a \longrightarrow \tau_a (\forall a \in G)$。

这一定理说明：任一群 G 都与 G 上的一个变换群同构，在变换群中总能找到自己的"模型"，把 Cayley 定理用到有限群上，有：任何一个有限群都与一个置换群的子群同构，因此，对于变换群、置换群的研究具有普遍意义。

八、关于陪集

1. 一个群 G 的子群 H 的左陪集和右陪集不一定相同。如：$H = \{(1), (12)\} \leqslant S_3$，而

$$(13)H = \{(13),(123)\}, (23)H = \{(23),(132)\}$$

是 H 的两个左陪集。

$$H(13) = \{(13),(123)\}, H(23) = \{(23),(123)\}$$

是 H 的两个右陪集。

因此左陪集 aH 与右陪集 Ha 一般并不相等。

2. 两个陪集的乘积未必是陪集。如 $H = \{(1),(1,2)\} \leqslant S_3$，而

$$(1)H \text{ 与 } (13)H$$

是 H 的两个左陪集，但

$$(1)H \cdot (13)H = \{(13),(23),(123),(132)\}$$

不再是陪集。

九、关于子群 H 在 G 中的指数

尽管子群 H 的左、右陪集未必相同，但 §7 定理 1 指出，子群 H 的左、右陪集的"个数"却相等。这个共同的数目叫做子群 H 在 G 中的指数。定理 1 指出，用子群 H 对群 G 分类，不论怎样分，分得的数目均相等。又易知子群 H 与 H 的每一个左陪集间都存在一个双射 $\varphi : h \longrightarrow ah (\forall h \in H)$，因此每一类（陪集）中含有的元素的数目也均与 H 含有的元素的个数相等。即，用子群按陪集的方法对 G 分类是均匀的，不会一类多，一类少，由此自然地导出了重要的 Lagrange 定理。

十、关于 Lagrange 定理(即有限群的阶和子群的阶的关系)

Lagrange 定理指出:有限群的子群的阶必是原群阶 n 的约数。一般地,其逆定理不真,如四次交代群 A_4,$|A_4| = 12$,6 是 12 的一个约数,但 A_4 中无 6 阶子群(参见 §7 第 22 题),但对于循环群及有限可换群,Lagrange 定理的逆定理却是成立的,而且对 $|G|$ 的特殊因数 p^k(p 为素数,k 为正整数),G 的 p^k 阶子群也存在(参见第三章 §8,§9)。

十一、pq 阶群的系列性质

1. pq 阶群(p,q 为素数,$p < q$)有惟一的 q 阶子群。

2. pq 阶交换群(p、q 为互异素数)必为循环群(第三章 §2 定理 5)。

3. pq 阶群必有 p 阶子群与 q 阶子群(其中 p、q 为素数),且若 $p<q$ 时,有惟一的 q 阶正规子群(第三章 §6 定理 3)。

典型题精讲

1. 设 G 是一个群,$a,b,c \in G$,证明

$$xaxba = xbc$$

在 G 中有且仅有一个解。

证明 由 G 是群可知 $a^{-1},b^{-1} \in G$,令 $x = a^{-1}bca^{-1}b^{-1}$,直接验证即可得 $a^{-1}bca^{-1}b^{-1}$ 为方程 $xaxba = xbc$ 的一个解。

下设 x_0 为该方程在 G 中的任一解,再由消去律可知

$$x_0ax_0ba = x_0bc$$

$$ax_0ba = bc$$

从而 $x_0 = a^{-1}bca^{-1}b^{-1}$,故所给方程在 G 中有且仅有一解。

---

2. 试证在任意阶大于 2 的非交换群中,存在满足 $ab = ba$ 的两个异于恒等元的元素 a,b。

证明 因为 G 为非交换群,故由 §1 第 6 题可知,在 G 中存在 $a^2 \neq e$ 的元素 a,即 $a \neq a^{-1}$ 且 $a \neq e$。令 $b = a^{-1} \neq e$,则有

$$ab = ba$$

3. 试证一个有限群的每一个元素的阶都是有限的。

证明　设 G 为任一有限群，$a \in G$，则

$$a, a^2, a^3, \cdots$$

不可能都不相等，故存在两个互异正整数 i、j，不妨设 $i < j$，使 $a^i = a^j$，从而有

$$a^{j-i} = e$$

即存在正整数 j、i 使上式成立，从而存在最小的正整数 m，使 $a^m = e$，即 $|a| = m$，有限。

4. 设 H 是群 G 的一个非空子集，且 H 的每一个元素的阶都有限，证明：

$$H \leqslant G \Leftrightarrow ab \in H$$

证明　由第二章 §3 定理 2 可知必要性显然。下面仅证充分性，同一定理，只需证明

$$a \in H \Rightarrow a^{-1} \in H$$

设 $a \in H$，由于 H 中每一元素的阶都有限，故存在正整数 n，使 $a^n = e$，故 $a^{-1} = a^{n-1}$，而由条件 $ab \in H$ 可知 $a^{n-1} \in H$。即 $a^{-1} \in H$ 成立。

5. 证明：循环群必为交换群。

证明　设循环群 $G = \langle a \rangle$，则 $\forall x, y \in G$，存在 $m, n \in Z$，使

$$x = a^m, y = a^n$$

而
$$xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$$

即 G 为一个交换群。

6. 设群 G 中的元素 a 的阶为 n。证明：a^r 的阶是 $\frac{n}{d}$，其中 $d = (r, n)$ 是 n 和 r 的最大公因子。

证明　由 $d = (r, n)$ 可知 $r = ds$，故

$$(a^r)^{\frac{n}{d}} = (a^{ds})^{\frac{n}{d}} = (a^n)^s = e$$

下证 $|a^r| = \frac{n}{d}$，设 $|a^r| = k$，则 $k \leqslant \frac{n}{d}$，令

$$\frac{n}{d} = kq + r_1 \quad (0 \leqslant r_1 < k)$$

则 $$e = (a^r)^{\frac{n}{d}} = (a^r)^{kq+r_1} = (a^r)^{kq}(a^r)^{r_1} = (a^r)^{r_1}$$

而 $r_1 < k$，k 为 a^r 的阶，故有 $r_1 = 0$ 则

$$\frac{n}{d} = kq$$

于是有$k \mid \frac{n}{d}$。

下证$\frac{n}{d} \Big| k$，由 $(a^r)^k = a^{rk} = e$ 及 $|a| = n$ 知，$n \mid rk$，故$\frac{n}{d} \Big| \frac{r}{d}k$，但 $(r,n) = d$，所以$\left(\frac{r}{d},\frac{n}{d}\right) = 1$，进而有$\frac{n}{d} \Big| k$。

综上可知 $$|a^r| = \frac{n}{d}$$

---

7. 设 $G = \langle a \rangle$，$|G| = n$，$(r,n) = 1$，证明 $G = \langle a^r \rangle$。

证明 由上面的第 6 题知 $|a^r| = n$，故

$$a^r, (a^r)^2, \cdots, (a^r)^{n-1}, (a^r)^n = e$$

互不相同，而由 $|G| = n$ 知，G 只有 n 个元，故

$$G = \{a^r, (a^r)^2, \cdots, (a^r)^n\} = \langle a^r \rangle$$

---

8. 已知群 G 中，若 $a,b \in G$，$(|a|, |b|) = 1$，且 $ab = ba$ 时有

$$|ab| = |a||b|$$

（参见教材第二章 §2定理4）。试举例说明若 $ab \neq ba$ 时上述结论不成立。

解 在三次对称群 S_3 中，取 $a = (12)$，$b = (132)$，则 $|a| = 2$，$|b| = 3$，而

$$ab = (13), \quad ba = (23)$$

虽然$(|a|, |b|) = (2,3) = 1$，但 $ab \neq ba$，而

$$3 = |ab| = |(13)| \neq |a||b| = 6$$

---

9. 证明：一个变换群的单位元一定是恒等变换。

证明 设 M 为非空集合，G 为 M 的一个变换群，ε 为 G 的单位元。

$\forall \tau \in G, a \in M$，由于 $\tau\varepsilon = \tau$，故

$$(\tau\varepsilon)(a) = \tau(a), \tau(\varepsilon(a)) = \tau(a)$$

又 τ 是 M 的一个一一变换，故 $\varepsilon(a) = a$，即 ε 为 M 的恒等变换。

---

10. 证明：两个不相连的循环置换可以交换。

证明　设 σ, τ 为 S_n 的两个不相连的循环置换，再考查乘积 $\sigma\tau$ 使数字 $1, 2, \cdots, n$ 如何变动。共有三种情况：

① 数字 i 在 σ 中出现，且 σ 把 i 变成 j，此时由于 σ 和 τ 不相连，j 不在 τ 中出现，故 τ 使 j 不变，所以 $\sigma\tau$ 仍把 i 变成 j。

② 数字 k 在 τ 中出现，且 τ 把 k 变成 l，此时 k 不在 σ 中出现，故 σ 使 k 不变，因此 $\sigma\tau$ 仍把 k 变成 l。

③ 数字 m 不在 σ 和 τ 中出现，此时 $\sigma\tau$ 使 m 不动。

类似可考查 $\tau\sigma$ 使数字 $1, 2, \cdots, n$ 如何变动，显然有相同的结果，所以

$$\sigma\tau = \tau\sigma$$

---

11. 详细证明：一个 k- 循环置换的阶是 k。

证明　设 $\pi = (i_1 i_2 \cdots i_k)$ 是一个 k- 循环置换，则 $\pi, \pi^2, \cdots, \pi^k$ 依次把 i_1 变为 $i_2, i_3, \cdots, i_1$。类似地，π^k 把 i_2 变成 $i_2, \cdots$，把 i_k 变成 i_k。故 $\pi^k = (1)$。且由上面讨论可知若 $l < k$，则 $\pi^l \neq (1)$，从而 π 的阶为 k。

---

12. 证明：阶是素数的群必为循环群。

证明　设 G 为群且 $|G| = p$（p 为素数），任取 $a(\neq e) \in G$，则 a 生成 G 的一个循环子群 $\langle a \rangle$，设 $|\langle a \rangle| = n$，则 $n \neq 1$，又由 Lagrange 定理知 $n \mid p$，故 $n = p$，从而 $G = \langle a \rangle$ 为一个循环群。

---

13. 证明：阶是 p^m 的群（p 为素数，$m \geqslant 1$）必包含一个阶为 p 的子群。

证明　设 G 为群，且 $|G| = p^m$，任取 $a \in G(a \neq e)$，则由 Lagrange 定理知

$$|a| \mid p^m$$

又 $|a| \neq 1$，故 $|a| = p^t (t \geqslant 1)$。

若 $t = 1$，则 $|a| = p$，故 $\langle a \rangle$ 为阶为 p 的子群；

若 $t>1$，令 $b=a^{p^{t-1}}$，则 $|b|=p$ 且 $\langle b\rangle$ 为一个阶为 p 的子群。

---

14. 证明：S_3 是阶数最小的非交换群。

证明 已知 S_3 为非交换群。显见一阶群 $\{e\}$ 为交换群，又由上面第 12 题知，阶数为 2,3,5(素数) 阶的群都为循环群，故为交换群(由上面的第 5 题)。然后只需证明 4 阶群 G 是交换群。

若群 G 中有 4 阶元素，则 G 是循环群，故为交换群。若群 G 中无 4 阶元素，由 Lagrange 定理知其元素的阶为 1 或 2，因此，$\forall x\in G$，总有 $x^2=e$，由本章 §1 第 6 题知 G 为交换群，从而 S_3 为阶数最小的非交换群。

---

15. 任一 6 阶群 G 有且仅有一个 3 阶子群。

证明 由 Lagrange 定理知，G 中的非单位元的阶为 2,3 或 6。若 G 中所有非单位元的阶均为 2，则对互异的非单位元 a 和 b，由 $(ab)(ab)=e$ 知

$$ba=a^{-1}b^{-1}=ab$$

故 G 必有 4 阶子群 $N=\{e,a,b,ab\}$，由 Lagrange 定理知，这是不可能的。从而必存在 $a\in G$，使 $|a|=3$ 或 6，故

$$H=\langle a\rangle=\{e,a,a^2\} \text{ 或 } K=\langle a^2\rangle=\{e,a^2,a^4\}$$

即为 G 的 3 阶子群。若 H 与 K 是 G 的两个互异的 3 阶子群，则由 $H\cap K=\{e\}$ 知

$$|G|\geqslant|HK|=\frac{|H|\cdot|K|}{|H\cap K|}=9$$

与 $|G|=6$ 矛盾，故 G 仅有一个 3 阶子群。

习题全解

§1 群的定义和初步性质(P38)

1. 证明：对群中任意元素 a,b 有

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

又问：$(ab\cdots c)^{-1}=?$

证明 设 a、b 的逆元分别为 a^{-1}、b^{-1}，则由

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

所以由群的定义及本章 §2 定理 1 可知

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

类似可以证明

$$(ab\cdots c)^{-1} = c^{-1}\cdots b^{-1}a^{-1}$$

---

2. 问：自然数集 N 对运算

$$a \circ b = a + b + ab$$

是否作成半群、幺半群或群？为什么？

解 $(a \circ b) \circ c = (a + b + ab) \circ c = a + b + ab + c + (a + b + ab)c$

$$= a + b + c + ab + ac + bc + abc$$

$$a \circ (b \circ c) = a \circ (b + c + bc) = a + b + c + bc + a(b + c + bc)$$

$$= a + b + c + ab + ac + bc + abc$$

所以自然数集 N 对该运算可作成半群，又任意的 $a \in N$，

$$0 \circ a = 0 + a + 0a = a$$

$$a \circ 0 = a + 0 + a0 = a$$

即半群 N 存在单位元。故自然数集 N 对该运算还可作成幺半群。

但易于验证 N 中不是每个元素都有逆元，如元素 1 若存在逆元 a，则

$$a \circ 1 = a + 1 + a = 0$$

故 $a = -\frac{1}{2}$，但 $a \notin N$，所以 N 对该运算不作成群。

---

3. 令 $O_n(R) = \{\boldsymbol{A} \mid \boldsymbol{A}$ 为 n 阶实正交方阵$\}$

证明：$O_n(R)$ 对于方阵的普通乘法作成一个群（此群称为实正交群）。

证明 $\forall \boldsymbol{A}、\boldsymbol{B} \in O_n(R)$，则

$$\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}} = \boldsymbol{B}\boldsymbol{B}^{\mathrm{T}} = \boldsymbol{E}$$

从而 $$(\boldsymbol{AB})(\boldsymbol{AB})^{\mathrm{T}} = (\boldsymbol{AB})(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{A}^{\mathrm{T}}) = \boldsymbol{AEA}^{\mathrm{T}} = \boldsymbol{E}$$

故 $(\boldsymbol{AB})^{\mathrm{T}} \in O_n(R)$，因此可知普通乘法是 $O_n(R)$ 的满足结合律的一个代数运算。又 $\boldsymbol{E} \in O_n(R)$，且任 $\boldsymbol{A} \in O_n(R)$，均有

$$\boldsymbol{EA} = \boldsymbol{A} \in O_n(R)$$

故 $O_n(R)$ 有左单位元 $\boldsymbol{E}$，又因为 $\forall \boldsymbol{A} \in O_n(R)$，均有

$$A^{-1}A = E$$

且 $$A^{-1}(A^{-1})^{T} = A^{-1}(A^{T})^{-1} = A^{-1}(A^{-1})^{-1} = E$$

即 $A^{-1} \in O_n(R)$，从而 $O_n(R)$ 中每一个元素 A 在 $O_n(R)$ 中均有左逆元 A^{-1}。

综上可知 $O_n(R)$ 对于方阵的普通乘法可作成群。

---

4. 设 G 是一个群，而 u 是 G 中任意一个固定的元素，证明：G 对新运算

$$a \circ b = aub$$

也作成一个群。

证明 由 G 是一个群，从而可知新运算是 G 的一个满足结合律的代数运算，任意的 $a \in G$，因为

$$u^{-1} \circ a = u^{-1}ua = a$$

故 u^{-1} 为新运算下 G 的单位元，又

$$(uau)^{-1} \circ a = (u^{-1}a^{-1}u^{-1})ua = u^{-1}$$

因此 $(uau)^{-1}$ 为新运算下 G 中每一元素 a 的左逆元，所以，G 对新运算也作成一个群。

---

5. 设 $G = \{(a,b) \mid a,b$ 为实数且 $a \neq 0\}$，并规定

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

证明：G 对此运算作成一个群，又问：此群是否为交换群？

证明 依题意可知 $G \neq \varnothing$，若 $(a,b) \in G, (c,d) \in G$，有 $ac, ad+b$ 均为实数且 $ac \neq 0$，从而

$$(a,b) \cdot (c,d) = (ac, ad+b) \in G$$

故 $\circ$ 是 G 的一个代数运算。

再证 G 对此运算满足结合律，具有左单位元，G 中的任一元素具有左逆元。

$\forall (e,f) \in G$，则

$$\begin{aligned}[(a,b)\circ(c,d)]\circ(e,f) &= (ac, ad+b)\circ(e,f) \\ &= (ace, acf+ad+b) \\ (a,b)\circ[(c,d)\circ(e,f)] &= (a,b)\circ(ce, cf+d) \\ &= (ace, acf+ad+b)\end{aligned}$$

故 $[(a,b)\circ(c,d)]\circ(e,f) = (a,b)\circ[(c,d)\circ(e,f)]$，$G$ 对该运算满足结

合律。

又由运算的定义可知，任$(a,b)\in G$，均有$(1,0)\in G$，且

$$(1,0)\circ(a,b)=(a,b)$$

即$(1,0)$为G的左单位元，又$\left(\frac{1}{a},-\frac{b}{a}\right)\in G$，且

$$\left(\frac{1}{a},-\frac{b}{a}\right)\circ(a,b)=(1,0)$$

因此对G中的任一元素(a,b)，$\left(\frac{1}{a},-\frac{b}{a}\right)$为它的左逆元。

综上可知，G对此运算可作成一个群，又$(1,2)\in G$，$(2,1)\in G$，而

$$(1,2)\circ(2,1)=(2,3),\quad (2,1)\circ(1,2)=(2,5)$$

故$(1,2)\circ(2,1)\neq(2,1)\circ(1,2)$，因此$G$不可能为一交换群。

---

6. 证明：如果群G的每个元素都满足方程$x^2=e$，则G必为交换群。

证明 任意的$a\in G$，有$a^2=e$，故$a=a^{-1}$，从而任意的$a,b\in G$，

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

因而G为交换群。

另证：任意的$a,b\in G$，则$ab\in G$，且

$$(ab)^2=e,a^2=e,b^2=e$$

故 $$ab=a(ab)^2b=a(ab)(ab)b=a^2bab^2=ebae=ba$$

因此G是一交换群。

§2 群中元素的阶(P44)

1. 证明：群中以下每组中的元素有相同的阶：

(1)a,a^{-1},cac^{-1}；　(2)ab,ba；　(3)abc,bca,cab

证明 (1) 不妨设$|a|=n$，$|a^{-1}|=m$，由$a^n=e$，得

$$a^n(a^{-1})^n=e=(a^{-1})^n$$

故$n\mid m$。又由$(a^{-1})^m=e$，得$(a^{-1})^ma^m=e=a^m$，故$m\mid n$，所以$m=n$。

再设$|cac^{-1}|=k$则$(cac^{-1})^n=ca^nc^{-1}=cec^{-1}=e$。

故$n\mid k$，又$e=(cac^{-1})^k=ca^kc^{-1}$故$a^k=e$，因此$k\mid n$，所以有$k=n$。

综上可知 $$|a|=|a^{-1}|=|cac^{-1}|$$

(2) 注意到$ba=a^{-1}(ab)a$，由(1)可知$|ab|=|ba|$

(3) 注意到 $abc = c^{-1}(cab)c = a(bca)a^{-1}$，由(1)可知

$$|abc| = |bca| = |cab|$$

---

2. 在有理数域上二阶满秩方阵作成的乘群中，给出元素 a,b 分别满足：

(1) $|a| = \infty$，$|b|$ 有限，$|ab| = \infty$；

(2) $|a| = \infty$，$|b|$ 有限，$|ab|$ 有限。

解 (1) 设

$$a = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

则 a 的矩阵行列式值为 -2，从而 a^n 的矩阵行列式值为 $(-2)^n$，因此可知 $|a| = \infty$，再设

$$b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

则 $$b^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, b^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, b^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

故 $|b| = 4$，有限，又

$$ab = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -2 & 0 \\ 0 & 1 \end{pmatrix}$$

记 $c = ab$，则 c 的矩阵行列式值为 -2，故 c^n 的矩阵行列式值为 $(-2)^n$，从而可知 $|c| = \infty$，即 $|ab| = \infty$。

(2) 设

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

则 $$a^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, a^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \cdots, a^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

故 $|a| = \infty$，再设

$$b = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$$

则 $$b^2 = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

即 $|b| = 2$，有限，又

$$ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 0 & -1 \end{pmatrix}$$

记 $c = ab$，而

$$c^2 = \begin{pmatrix} 1 & -2 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

故 $|c| = 2$，有限。

---

3. 设 G 是群，且 $|G| > 1$，证明：若 G 中除 e 外其余元素的阶都相同，则这个相同的阶不是无限就是一个素数。

证明 任意的 $a \in G$，且 $a \neq e$，若 $|a| = \infty$，则结论成立，若 $|a| = n < \infty$，如果 n 为合数，不妨设 $n = st$，其中 $1 < s, t < n$，则 $a^s \neq e$ 且 $|a^s| = t < n$，这与 G 中除 e 外其余元素的阶均相同矛盾。

---

4. 证明：

(1) 在一个有限群里，阶数大于 2 的元素的个数一定是偶数；

(2) 偶数阶群中阶等于 2 的元素的个数一定是奇数。

证明 (1) 设 G 是一个有限群，$a \in G$，且 $|a| = k > 2$，则有

$$a \neq a^{-1}$$

否则若 $a = a^{-1}$，则 $a^2 = aa^{-1} = e$ 与 $|a| > 2$ 矛盾，由第 1 题可知

$$|a| = |a^{-1}|$$

从而

$$|a^{-1}| = k > 2$$

若 G 中存在异于 a 与 a^{-1} 的阶数大于 2 的元素 b，即

$$b \neq a, b \neq a^{-1}$$

从而 $b^{-1} \neq a^{-1}, b^{-1} \neq a$，因此 G 中阶大于 2 的元素是成对出现的，又 G 为有限群，故 G 中阶数大于 2 的元素的个数必为偶数。

(2) 设群 G 的阶数为偶数，由(1) 知阶数大于 2 的元素的个数为偶数及 G 中的单位元是惟一的阶数为 1 的元素，从而阶数等于 2 的元素的个数必为奇数。

---

5. 设群 G 中元素 a 的阶为 n，证明：

$$a^s = a^t \Leftrightarrow n \mid (s - t)$$

证明 “$\Leftarrow$” 设 $a\in G$，若 $n\mid(s-t)$，由于 $|a|=n$，则 $a^{s-t}=e$，从而 $a^s=a^t$。

“$\Rightarrow$” 若 $a^s=a^t$，故 $a^sa^{-t}=a^{s-t}=e$，又 $|a|=n$，故 $n\mid(s-t)$。

---

6. 设群 G 中元素 a 的阶是 mn，$(m,n)=1$，证明：在 G 中存在元素 b,c 使

$$a=bc=cb,\text{且 } |b|=m,\ |c|=n$$

并且这样的 b,c 还是惟一的。

证明 先证存在性。

由 $(m,n)=1$，则存在整数 s、t，使得

$$ms+nt=1$$

令 $b=a^{ms}$，$c=a^{nt}$，则

$$bc=cb=a^{ms+nt}=a$$

若 $b^r=e$，则 $(a^{ms})^r=a^{rms}=e$，又 $|a|=mn$，故

$$mn\mid rms,n\mid rs$$

又
$$b^n=(a^{ms})^n=(a^{mn})^s=e$$

及 $ms+nt=1$ 可知

$$(n,s)=1,n\mid r$$

所以
$$|b|=n$$

同理可证 $|c|=m$。

再证惟一性。

若还有 b_1、c_1，使得

$$a=b_1c_1=c_1b_1,\text{且 } |b_1|=n,\ |c_1|=m$$

则
$$a^{ms}=b_1^{ms}c_1^{ms}=b_1^{ms}$$

又 $ms=1-nt$，故

$$b_1^{ms}=b_1^{1-nt}=b_1(b_1^{nt})^{-1}=b_1$$

从而 $a^{ms}=b_1^{ms}=b_1$，又 $a^{ms}=b$，故 $b=b_1$，因此

$$b_1^{-1}=a^{-ms}$$

$$c_1=ab_1^{-1}=aa^{-ms}=a^{1-ms}=a^{nt}=c$$

所以 $b_1=b$，$c_1=c$，即 b,c 是惟一的。

▶ §3 子群(P49) ◀

1. 证明：群 G 的任意个子群的交仍是 G 的一个子群。

证明　设 $H_i \leqslant G$，记 $H = \bigcap\limits_i H_i$，则由定理 1 知 $H \neq \varnothing$。

设 $a,b \in H$，则任意的 i，$a,b \in H_i$，又 $H_i \leqslant G$，由本章 §2 定理 3 知对任意的 i，$ab^{-1} \in H_i$，从而

$$ab^{-1} \in \bigcap_i H_i$$

即 $ab^{-1} \in H$，由本章 §2 定理 3 可知 $H \leqslant G$，即群 G 的任意个子群的交仍是 G 的一个子群。

---

2. 设 H 是群 G 的一个非空子集，且 H 中每个元素的阶都有限。证明：$H \leqslant G$ 当且仅当 H 对 G 的乘法封闭。

证明　由本章 §2 定理 2 知，若 $H \leqslant G$，则 H 对 G 的乘法封闭。

若 H 对 G 的乘法封闭，求证 $H \leqslant G$，由本章 §2 定理 2 知，只需证明任意的 $a \in H$，有 $a^{-1} \in H$。

因为 H 中的每个元素的阶都有限，设 $|a| = n$，即

$$a^n = e \in H$$

从而
$$aa^{n-1} = e$$

故
$$a^{-1} = a^{n-1}$$

又由 $a \in H$ 及 H 对乘法封闭可得，$a^{n-1} \in H$，所以 $a^{-1} \in H$，因此由本章 §2 定理 2 知

$$H \leqslant G$$

---

3. 证明：交换群中所有有限阶元素作成一个子群。又，对非交换群如何？

证明　设 G 为交换群，H 为 G 中所有有限阶元素的集合，则由 $|e| = 1$ 可知，$H \neq \varnothing$。

设 $a,b \in H \leqslant G$，且 $|a| = m$，$|b| = n$，则由 G 是可交换的可知

$$(ab)^{[m,n]} = e$$

即 ab 的阶有限，$ab \in H$，又由于 $|a| = |a^{-1}|$，而 a 的阶有限，故 $a^{-1} \in H$，因此由本章 §2 定理 2 知 $H \leqslant G$。

另证：设 $a,b \in H \subseteq G$，且 $|a| = m$，$|b| = n$，由 $|b| = |b^{-1}|$ 可得 $|b^{-1}| = n$，又 G 是可交换的，故

$$(ab^{-1})^{[m,n]} = e$$

即 ab^{-1} 的阶有限，$ab^{-1} \in H$，由本章 §2 定理 3 可得 $H \leqslant G$。

对于非交换群结论未必成立，例如实数域上全体 2 阶满秩方阵的乘群中，可知元素

$$a = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, b = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

的阶均为 2，但其乘积

$$ab = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

的阶却是无限，即其全体有限阶元素对乘法不封闭，故不能作成一个子群。

---

4. 证明：一般线性群 $GL_n(F)$ 的中心是一切纯量矩阵 $aE(0 \in F)$ 作成的子群。

证明 由高等代数中关于矩阵的知识可知与所有 n 阶可逆方阵可换的方阵是全体纯量方阵，由本章 §2 定理 4 即知全体纯量方阵为一般线性群 $GL_n(F)$ 的中心。

---

5. 设 G 是群，$H \leqslant G, a \in G, a^m, a^n \in H$。证明：若 $(m,n) = 1$，则 $a \in H$。

证明 由 $(m,n) = 1$ 可知存在整数 s、t，使

$$ms + nt = 1$$

因此 $a = a^{ms+nt} = (a^m)^s(a^n)^t$，又 $H \leqslant G$，及 $a^m, a^n \in H$，所以 H 对乘法封闭，从而

$$a = (a^m)^s(a^n)^t \in H$$

---

6. 设 G 是一个阶数大于 2 的群，且 G 的每个元素都满足方程 $x^2 = e$，证明：G 必含有 4 阶子群。

证明 因为 $|G| > 2$，故存在 $a, b \in G$，使 $a \neq e, b \neq e, a \neq b$，又 G 中每个元素满足 $x^2 = e$，故 $a^2 = e, b^2 = e$，从而 $a^{-1} = a, b^{-1} = b$，且

$$H = \{e, a\} \leqslant G, K = \{e, b\} \leqslant G$$

又由 §1 第 6 题知 G 为交换群，因而 $HK = KH$，故由定理 5 知

$$HK = \{e, a, b, ab\} \leqslant G$$

又由 $a \neq e, b \neq e, a \neq b, a = a^{-1}, b = b^{-1}$ 可知 $ab \neq e, ab \neq a, ab \neq b$，因此

$$|HK| = 4$$

即 G 含有 4 阶子群 HK。

---

7. 证明：任何群都不能是两个真子群的并。

证明　反证法。

设 H、K 为群 G 的两个真子群，且 $G = H \cup K$，因为 H、K 为 G 的真子群，故存在 $a, b \in G$，使得

$$a \notin H, b \notin K$$

但 $G = H \cup K$，从而 $a \in K, b \in H$，又 $ab \in G$，故 $ab \in H$ 或 $ab \in K$。

若 $ab = c \in H$，则由 $H \leqslant G$ 可知 $b^{-1} \in H, a = cb^{-1} \in H$ 这与 $a \notin H$ 矛盾。

若 $ab = c \in K$，则由 $K \leqslant G$ 可知 $a^{-1} \in K, b = a^{-1}c \in K$，这与 $b \notin K$ 矛盾，因此假设不成立，即 G 不能是两个真子集的并。

§4　循环群(P56)

1. 设 $G = \langle a \rangle$ 为 6 阶循环群。给出 G 的一切生成元和 G 的所有子群。

解　由本章 §4 定理 2 知，$(1,6) = 1, (5,6) = 1$，因此 G 有两个生成元：a, a^5。

由本章 §4 定理 5 及推论 2 可知，6 阶循环群 G 的子群个数为 $T(6) = (1+1)(1+1) = 4$，分别为

$$\{e\}, G, \langle a^2 \rangle = \{e, a^2, a^4\}, \langle a^3 \rangle = \{e, a^3\}$$

---

2. 设群中元素 a 的阶无限，证明：

$$\langle a^s \rangle = \langle a^t \rangle \Leftrightarrow s = \pm t$$

证明　“$\Leftarrow$”　若 $s = \pm t$，则依循环群定义可知

$$\langle a^s \rangle = \langle a^t \rangle$$

“$\Rightarrow$”　若 $\langle a^s \rangle = \langle a^t \rangle$，则存在整数 m、n，使得

$$a^s = (a^t)^m = a^{tm}$$

$$a^t = (a^s)^n = a^{sn}$$

从而由 $|a|=\infty$ 可知，$s=tm$，$t=sn$，故

$$s=snm, nm=1$$

又 m 及 n 均为整数，因此必有 $m=n=\pm 1$，即 $s=\pm t$。

3. 设群中元素 a 的阶是 n，证明：

$$\langle a^s\rangle=\langle a^t\rangle \Leftrightarrow (s,n)=(t,n)$$

证明 “$\Leftarrow$” 不妨设 $(s,n)=(t,n)=d$，则存在整数 m、k，使

$$ms+kn=d$$

令 $t=dt_1$，则由 $|a|=n$ 可知

$$a^t=a^{dt_1}=a^{(ms+kn)t_1}=a^{mst_1}\cdot a^{knt_1}=(a^s)^{mt_1}\cdot(a^n)^{kt_1}=(a^s)^{mt_1}$$

故 $a^t\in\langle a^s\rangle$，$\langle a^t\rangle\subseteq\langle a^s\rangle$，同理有 $\langle a^s\rangle\subseteq\langle a^t\rangle$，所以 $\langle a^s\rangle=\langle a^t\rangle$。

“$\Rightarrow$” 因为 $|a|=n$，由本章 §2 中定理 3 得

$$|a^s|=\frac{n}{(s,n)},\ |a^t|=\frac{n}{(t,n)}$$

又 $\langle a^s\rangle=\langle a^t\rangle$，故 $|a^s|=|a^t|$，所以

$$\frac{n}{(s,n)}=\frac{n}{(t,n)},(s,n)=(t,n)$$

4. 设 a,b 是群 G 中两个有限阶元素且

$$ab=ba,(|a|,|b|)=1$$

证明：$\langle a,b\rangle=\langle ab\rangle$。

证明 由 $a\in\langle a,b\rangle$，$b\in\langle a,b\rangle$ 可得，$ab\in\langle a,b\rangle$，进而

$$\langle ab\rangle\subseteq\langle a,b\rangle$$

再证 $\langle a,b\rangle\subseteq\langle ab\rangle$。

不妨设 $|a|=m$，$|b|=n$，则 $a^m=e$，$b^n=e$，$(m,n)=1$，从而存在整数 s、t，使得

$$ms+nt=1$$

从而由 $ab=ba$ 可知

$$(ab)^{ms}=a^{ms}b^{ms}=(a^m)^s b^{ms}=b^{ms}=b^{1-nt}=b(b^n)^{-t}=b$$

又 $(ab)^{ms}\in\langle a,b\rangle$，故 $b\in\langle a,b\rangle$，进而 $b^{-1}\in\langle a,b\rangle$，所以

$$a=(ab)b^{-1}\in\langle ab\rangle$$

所以有 $\langle a,b\rangle \subseteq \langle ab\rangle$

综上可知 $\langle a,b\rangle = \langle ab\rangle$

5. 设 p 是一个素数，$G_p = \bigcup\limits_{i=1}^{\infty} U_{p^i}$，其中 U_{p^i} 是 p^i 次单位根群。证明：

(1)G_p 关于数的普通乘法作成一个群；

(2)G_p 的真子群只有 U_{p^i}，$(i = 1,2,\cdots)$。

证明 (1) 设 U_i(i 是正整数) 是全体 i 次单位根对普通乘法作成的群，令 $U = \bigcup\limits_{i=1}^{\infty} U_i$，由本章 §2 例 4 知，$U$ 对普通乘法作成一个无限交换群，任取 $a,b \in G_p$，则存在 $s \leqslant t$，使得

$$a \in U_{p^s}, b \in U_{p^t}$$

从而有 $a,b \in U_{p^t}$，$ab^{-1} \in U_{p^t}$，$ab^{-1} \in G_p$，故 $G_p \leqslant U$，即 G_p 关于数的普通乘法作成一个群。

(2) 显然 $U_{p^i}(i = 1,2,\cdots)$ 都是 G_p 的真子群。

再证 G_p 的真子群只可能是 $U_{p^i}(i = 1,2,\cdots)$。

设 $H < G_p$，则存在 $a \in G_p$，使得 $a \notin H$，设 $|a| = p^s$，即 a 是 p^s 次原根。

然后证 H 中任何元素的阶均不大于 p^s，否则，若存在 $h \in H$，使 $|h| = p^t > p^s$，则

$$a^{p^t} = (a^{p^s})^{p^{t-s}} = 1$$

故 a 是 p^t 次单位根，进而 $a \in \langle h\rangle \subseteq H$，与 $a \notin H$ 矛盾。

设 $p^m(< p^s)$ 是 H 中所有元素的最大阶，不妨设 $b \in H$，且 $|b| = p^m$，则有

$$U_{p^m} = \langle b\rangle \subseteq H$$

另一方面，由于交换群中每个元素的阶都整除最大阶，故任意 $h \in H$，h 的阶均整除 p^m，因此 h 是 p^m 次单位根，$h \in \langle b\rangle$，由 h 的任意性得 $H \subseteq \langle b\rangle$，所以

$$H = \langle b\rangle = U_{p^m}$$

所以综上可知 G_p 的真子群只有 $U_{p^i}(i = 1,2,\cdots)$。

6. 设 H 是群 G 的一个子群，且 $H \subset G$，又 $M = G - H$ 是 G 关于 H 的余

集。证明：$G=\langle M\rangle$。

证明 依题意有 $G=H\cup M$ 且 $H\cap M=\varnothing$，从而任 $x\in G$，$x\in H$ 且 $x\notin M$ 或 $x\in M$ 且 $x\notin H$。

当 $x\in H$ 且 $x\notin M$ 时，则由于 H 是 G 的子群可知 $x^{-1}\in H(x^{-1}\notin M)$，又由于 $H\subset G$，故存在 $a\in G$，$a\in M$，但 $a\notin H$，从而

$$ax\notin H, ax\in M$$

（否则若 $ax\in H$，则由 $x^{-1}\in H$ 得 $a\in H$，矛盾）又 $a^{-1}\notin H$，故 $a^{-1}\in M$，所以

$$x=a^{-1}\cdot ax\in\langle M\rangle$$

又当 $x\in M$ 且 $x\notin H$ 时，显见有 $x\in\langle M\rangle$。

综上可知 G 中任意元素都属于 $\langle M\rangle$，故 $G=\langle M\rangle$。

---

7. 证明 $\left\{1,\frac{1}{2},\frac{1}{3!},\cdots,\frac{1}{n!},\cdots\right\}$ 是有理数加群的一个生成系。

证明 任意的 $\frac{b}{a}\in Q_+$，Q_+ 为有理数的加群，则由

$$\frac{b}{a}=\frac{(a-1)!b}{a!}$$

可知 $\frac{b}{a}$ 可表为若干个 $\frac{1}{a!}$ 的代数和，即有理数加群可由 $\left\{1,\frac{1}{2},\frac{1}{3!},\cdots,\frac{1}{n!},\cdots\right\}$ 生成。

§ 5 变换群(P60)

1. 设 $M=\{1,2,3,4\}$，$H=\{\tau,\sigma\}$，其中

$$\tau=\begin{pmatrix}1&2&3&4\\1&1&3&4\end{pmatrix},\quad \sigma=\begin{pmatrix}1&2&3&4\\1&1&3&3\end{pmatrix}$$

问：H 关于变换乘法是否作成有单位元半群？是否作成群？

解 因为 $\tau\tau=\begin{pmatrix}1&2&3&4\\1&1&3&4\end{pmatrix}=\tau$，$\tau\sigma=\begin{pmatrix}1&2&3&4\\1&1&3&3\end{pmatrix}=\sigma$

$$\sigma\tau=\begin{pmatrix}1&2&3&4\\1&1&3&3\end{pmatrix}=\sigma,\sigma\sigma=\begin{pmatrix}1&2&3&4\\1&1&3&3\end{pmatrix}=\sigma$$

所以 H 可作成以 τ 为单位元的半群，但由于 σ 无逆元，故 H 不能作成群。

2. 设 M 是正整数集，而

$$\tau: 1 \longrightarrow 1, n \longrightarrow n-1 (n>1); \sigma: n \longrightarrow n+1 (n \in M)$$

问：$\tau\sigma$ 与 $\sigma\tau$ 各为何？是否相等？

解 $\tau\sigma: n \longrightarrow n (n \in M)$，即 $\tau\sigma = \varepsilon$；

$\sigma\tau: 1 \longrightarrow 2, n \longrightarrow n (n \geqslant 2)$。

因此

$$\tau\sigma \neq \sigma\tau$$

3. 设 M 是有理数集，又令

$$\tau_{(a,b)}: x \longrightarrow ax+b \quad (a,b,x \in M, \text{但 } a \neq 0)$$

问：$G = \{\tau_{(a,b)} \mid 0 \neq a, b \in M\}$ 关于变换乘法是否作成群？是 M 的双射变换群还是非双射变换群？

解

$$\tau_{(a,b)}\tau_{(c,d)}: x \longrightarrow a(cx+d)+b = acx+ad+b$$

即 $\tau_{(a,b)}\tau_{(c,d)} = \tau_{(ac,ad+b)}$，故 G 对变换的乘法封闭。

又当 $a=1, b=0$ 时

$$\tau_{(1,0)}: x \longrightarrow x$$

故 $\tau_{(1,0)}$ 为单位元，当 $c = \dfrac{1}{a}, d = -\dfrac{b}{a}$ 时

$$\tau_{(c,d)}\tau_{(a,b)}: x \longrightarrow cax+cb+d = x$$

即 $\tau_{(a^{-1},-a^{-1}b)}$ 为 $\tau_{(a,b)}$ 的逆元。

综上可知 G 关于变换乘法可作成一个群。

又 $a \neq 0$，故 $\tau_{(a,b)}$ 为 M 的一个单射变换，从而由本章 §5 定理 2 知，G 是 M 的双射变换群（或另取 $y \in M$，则 $x = \dfrac{y-b}{a}$ 是 y 在 $\tau_{(a,b)}$ 下的逆象，即 $\tau_{(a,b)}$ 又是满射，进而 G 是 M 的双射变换群）。

4. 设 $|M|>1$，证明：集合 M 的全体非双射变换关于变换的乘法不能作成群。

证明 反证法。

不妨令 $M = \{a, b, \cdots\}$，且 $\forall x \in M$，有 $\sigma(x) = a, \tau(x) = b$，且

$$\sigma\tau=\sigma,\tau\sigma=\tau$$

若集合M的全体非双射变换关于变换的乘法可作成群，故σ与τ都是此群的单位元，而显见σ与τ为M的两个互异的非双射变换，矛盾，所以M的全体非双射变换关于变换的乘法不能作成群。

---

5. 证明：对任何固定的正整数n，互不同构的n阶群只有有限个。

证明 由Cayley定理的推论：任何n阶有限群都同n次对称群S_n的一个子群同构，而S_n是一个$n!$阶的有限群，它只有有限个子群，因此互不同构的n阶群只有有限个。

§6 置换群(P70)

1. 给出三次对称群S_3的所有真子群，并利用本章§3推论2和§6例3说明理由。

解 S_3的真子群有

$$H_1=\{(1)\},H_2=\{(1),(1,2)\},H_3=\{(1),(1,3)\}$$

$$H_4=\{(1),(2,3)\},H_5=\{(1),(1,2,3),(1,3,2)\}$$

---

2. (1) 设置换$\sigma=\sigma_1\sigma_2\cdots\sigma_k$（每个$\sigma_i$都是对换），问$\sigma^{-1}=$?再由此说明置换$\sigma$与$\sigma^{-1}$有相同的奇偶性。

(2) 证明：循环$(i_1i_2\cdots i_k)$的奇偶性与k的奇偶性相反。

解 (1) 因为$(\sigma_1\sigma_2\cdots\sigma_k)(\sigma_k\sigma_{k-1}\cdots\sigma_1)=(1)$，故$\sigma^{-1}=\sigma_k\sigma_{k-1}\cdots\sigma_1$，由$\sigma\sigma^{-1}=(1)$为偶置换，而奇偶性相异的置换之积为奇置换，故$\sigma$与$\sigma^{-1}$具有相同的奇偶性。

(2) 因为

$$(i_1i_2\cdots i_k)=(i_1i_k)(i_1i_{k-1})\cdots(i_1i_2)$$

即$(i_1i_2\cdots i_k)$为$k-1$个对换之积，故$(i_1i_2\cdots i_k)$的奇偶性与$k-1$的奇偶性相同，即与k的奇偶性相反。

---

3. 证明

(1)$(i_1i_2\cdots i_k)^{-1}=(i_ki_{k-1}\cdots i_1)$；

$$(2)\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}^{-1}=\begin{pmatrix}i_1 & i_2 & \cdots & i_n\\ 1 & 2 & \cdots & n\end{pmatrix}$$

证明 (1) 因为

$$(i_1 i_2 \cdots i_k)(i_k i_{k-1} \cdots i_1)=(1)$$

所以
$$(i_1 i_2 \cdots i_k)^{-1}=(i_k i_{k-1} \cdots i_1)$$

(2) 因为

$$\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}\begin{pmatrix}i_1 & i_2 & \cdots & i_n\\ 1 & 2 & \cdots & n\end{pmatrix}=\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}$$

所以

$$\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}^{-1}=\begin{pmatrix}i_1 & i_2 & \cdots & i_n\\ 1 & 2 & \cdots & n\end{pmatrix}$$

---

4. 试求下列各置换的阶：

$\tau_1=(1\ 3\ 7\ 8)(2\ 4)$；$\tau_2=(1\ 3\ 7\ 2)(2\ 3\ 4)$；

$\tau_3=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 4 & 1 & 5 & 2 & 3\end{pmatrix}$；$\tau_4=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 5 & 7 & 6 & 3 & 1 & 4 & 2\end{pmatrix}$

解 $\tau_3=(1\ 6\ 3)(2\ 4\ 5)$，$\tau_4=(1\ 5)(2\ 7)(3\ 6\ 4)$

则由本章§6定理4可知，τ_1 的阶为4，τ_2 的阶为12，τ_3 的阶为3，τ_4 的阶为6。

---

5. 设 $\tau=(3\ 2\ 7)(2\ 6)(1\ 4)$，$\sigma=(1\ 3\ 4)(5\ 7)$，试求

$$\sigma\tau\sigma^{-1}=?\quad \sigma^{-1}\tau\sigma=?$$

解 $\sigma^{-1}=(7\ 5)(4\ 3\ 1)$，则由本章§6定理5，得

$$\begin{aligned}\sigma\tau\sigma^{-1}&=(\sigma(3)\sigma(2)\sigma(7))(\sigma(2)\sigma(6))(\sigma(1)\sigma(4))\\ &=(4\ 2\ 5)(2\ 6)(3\ 1)=(1\ 3)(2\ 6\ 5\ 4)\\ \sigma^{-1}\tau\sigma&=(\sigma^{-1}(3)\sigma^{-1}(2)\sigma^{-1}(7))(\sigma^{-1}(2)\sigma^{-1}(6)\sigma^{-1}(1)\sigma^{-1}(4))\\ &=(1\ 2\ 5)(2\ 6)(4\ 3)=(1\ 2\ 6\ 5)(3\ 4)\end{aligned}$$

---

6. 证明：$H=\{(1),(1\ 2),(3\ 4),(1\ 2)(3\ 4)\}\leqslant S_4$，又问：$H$ 是否为传递群？

证明 因为 H 中每个元素的阶均有限，且 H 对置换的乘法是封闭的，故

由本章 §3 第 2 题可知 $H \leqslant S_4$，显见 H 没有置换把 1 变成 3，故 H 不是传递群。

7. 先用循环或循环之积写出 6 阶循环群 $G = \langle (1\ 2\ 3\ 4\ 5\ 6) \rangle$ 的全部元素，再指出 G 是一个传递群，但不是 2 重传递群。

解 设 $\tau = (1\ 2\ 3\ 4\ 5\ 6)$，则 G 的元素为

$(1)\tau = (1\ 2\ 3\ 4\ 5\ 6), \tau^2 = (1\ 3\ 5)(2\ 4\ 6)$

$\tau^3 = (1\ 4)(2\ 5)(3\ 6), \tau^4 = (1\ 5\ 3)(2\ 4\ 6), \tau^5 = (1\ 6\ 5\ 4\ 3\ 2)$

又由上可知 $\tau^k(1) = k+1(k = 1,2,3,4,5)$，故 G 为传递群，又 G 中不存在置换 σ，使 $\sigma(1) = 3, \sigma(2) = 5$。

所以 G 不是 2 重传递群。

§7 陪集、指数和 Lagrange 定理（P77）

1. 设 G 为 n 阶有限群。证明：G 中每个元素都满足方程 $x^n = e$。

证明 设 $x \in G$，则由 Lagrange 定理推论 2 可知，$|x| \mid n$，从而 $x^n = e$。

2. 写出三次对称群 S_3 关于子群 $H = \{(1),(2\ 3)\}$ 的所有左陪集和所有右陪集。

解 $S_3 = \{(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$，则 H 的左陪集有

$(1)H = H, (1\ 2)H = \{(1\ 2),(1\ 2\ 3)\}$

$(1\ 3)H = \{(1\ 3),(1\ 3\ 2)\}, (2\ 3)H = \{(2\ 3),(1)\}$

$(1\ 2\ 3)H = \{(1\ 2\ 3),(1\ 2)\}, (1\ 3\ 2)H = \{(1\ 3\ 2),(1\ 3)\}$

H 的右陪集有

$H(1) = H, H(1\ 2) = \{(1\ 2),(1\ 3\ 2)\}$

$H(1\ 3) = \{(1\ 3),(1\ 2\ 3)\}, H(2\ 3) = \{(2\ 3),(1)\}$

$H(1\ 2\ 3) = \{(1\ 2\ 3),(1\ 3)\}, H(1\ 3\ 2) = \{(1\ 3\ 2),(1\ 2)\}$

3. 设 H、K 分别为群 G 的两个 m 与 n 阶子群，证明：若 $(m,n) = 1$，则 $H \cap K = \{e\}$。

证明 显见 $\{e\} \subset H \cap K, H \cap K \neq \varnothing$。任意的 $a,b \in H \cap K$，则 $a,b \in H$ 且 $a,b \in K$，又 H、K 为 G 的子群，故 $ab^{-1} \in H$ 且 $ab^{-1} \in K$。即 $ab^{-1} \in$

$H \cap K$，故 $H \cap K \leqslant H, H \cap K \leqslant K$。从而由 Lagrange 定理知

$$|H \cap K| \mid m \text{ 且 } |H \cap K| \mid n$$

因此 $|H \cap K| \mid (m,n)$，又 $(m,n)=1$，故必有 $|H \cap K|=1$，所以

$$H \cap K = \{e\}$$

---

4. 证明：p^m（p 是素数，m 是正整数）阶群必含有 p 阶元，而且 p 阶元的个数是 $p-1$ 的倍数。

证明　设 G 是 p^m 阶群，任意的 $a(\neq e) \in G$，由 $|G|=p^m$ 及 Lagrange 定理的推论 2 可知

$$|a| \mid p^m$$

又 p 是素数，故存在正整数 $s(\leqslant m)$，使 $|a|=p^s$，因此 $a^{p^s}=e$，$|a^{p^{s-1}}|=p$，即 G 含有 p 阶元。

设 $|b|=p$，$|c|=p$，且 $\langle b\rangle \neq \langle c\rangle$，则

$$\langle b\rangle = \{e,b,b^2,\cdots,b^{p-1}\}, \langle c\rangle = \{e,c,c^2,\cdots,c^{p-1}\}$$

且 $\langle b\rangle \cap \langle c\rangle$ 仅为 $\{e\}$。即 $\langle b\rangle$ 中的 $p-1$ 个元素 $b,b^2,\cdots,b^{p-1}$ 与 $\langle c\rangle$ 中的 $p-1$ 个元素 $c,c^2,\cdots,c^{p-1}$ 不存在相等的元素，而它们都是 G 中的 p 阶元，由此可知，G 中的 p 阶元的个数必是 $p-1$ 的倍数。

---

5. 设 G 是群，$K \leqslant H \leqslant G$。又 $A=\{a_1,a_2,\cdots\}$ 与 $B=\{b_1,b_2,\cdots\}$ 分别为 G 关于 H 和 H 关于 K 的左陪集代表系，证明：

$$AB = \{a_ib_j \mid a_i \in A, b_j \in B\}$$

是 G 关于 K 的一个左陪集代表系。

证明　任取 $x \in G$，因为 A 是 G 关于 H 的左陪集代表系，则存在 i，使

$$x \in a_iH$$

即 $a_i^{-1}x \in H$。又 B 为 H 关于 K 的左陪集代表系，则存在 j，使

$$a_i^{-1}x \in b_jK$$

故 $(a_ib_j)^{-1}x \in K$，$xK=a_ib_jK$，$x \in a_ib_jK$，即 $\forall x \in G$，必有某 $a_ib_j \in AB$，使 $x \in a_ib_jK$。

又若存在 $a_sb_t \in AB$，使 $a_ib_jK = a_sb_tK$，则

$$k = (a_ib_j)^{-1}(a_sb_t) \in K \leqslant H$$

故 $a_i^{-1}a_s = b_jkb_t^{-1} \in H$，进而可知 $a_sH = a_iH$，而 A 是 G 关于 H 的左陪集

代表系，故 $i = s$。从而 $b_jK = b_tK$，由 B 是 H 关于 K 的左陪集代表系知，$j = t$。

综上可知 AB 是 G 关于 K 的一个左陪集代表系。

6. 试求出三次对称群 S_3 的所有子群，并利用 Lagrange 定理说明理由。

解 因为 S_3 的子集

$H_1 = \{(1)\}, H_2 = \{(1),(1\ 2)\}, H_3 = \{(1),(1\ 3)\}$

$H_4 = \{(1),(2\ 3)\}, H_5 = \{(1),(1\ 2\ 3),(1\ 3\ 2)\}, H_6 = S_3$

对置换的乘法都是封闭的，所以这 6 个子集为 S_3 的子群。

利用 Lagrange 定理说明 S_3 只有这 6 个子群。

由 Lagrange 定理可知，S_3 的子群 H 的指数 $|H|$ 为 $|S_3| = 6$ 的因数，故 $|H| = 1,2,3$ 或 6，易得 $|H| = 1$ 时，$H = H_1 = \{(1)\}$；当 $|H| = 6$ 时，$H = S_3$。

当 $|H| = 2$ 时，则子群 H 中除单位元外，另一元素只能是一个二阶元，而 S_3 中的二阶元仅有 $(1\ 2),(1\ 3),(2\ 3)$ 三个，故此时 H 只能为 H_2，H_3 或 H_4。

当 $|H| = 3$ 时，则子群 H 中除单位元外，由 Lagrange 定理知，另两个元素只能为一阶元或三阶元，而 S_3 中除单位元外没有其他一阶元，且仅有两个三阶元 $(1\ 2\ 3)$ 及 $(1\ 3\ 2)$，故此时 $H = H_5$。

综上可知，S_3 有且仅有上述的 6 个子群。

7. 证明：四元数群的真子群只有 4 个：

$$\langle -1\rangle, \langle i\rangle, \langle j\rangle, \langle k\rangle$$

证明 四元数群

$$G = \{1, i, j, k, -1, -i, -j, -k\}$$

（参见本章 §1 例 4），$|G| = 8$，显见 $\langle -1\rangle, \langle i\rangle, \langle j\rangle, \langle k\rangle$ 为 G 的真子群，且 $|\langle -1\rangle| = 2$，$|\langle i\rangle| = |\langle j\rangle| = |\langle k\rangle| = 4$。

若 H 为 G 的真子群，则由 Lagrange 定理知，$|H| = 2$ 或 $|H| = 4$。

当 $|H| = 2$ 时，则又由 Lagrange 定理及 H 为 G 的真子群可知，H 中必有一个二阶元，而 G 中仅有一个二阶元 -1，故必有 $H = \langle -1\rangle$。

当 $|H| = 4$ 时，则 H 中的元素只能是一阶、二阶、四阶元，又 H 为 G

的真子群，且 i,j,k 为四阶元，$i^2=j^2=k^2=-1$，从而若 $i\in H$，必有 $H=\langle i\rangle$，若 $j\in H$，必有 $H=\langle j\rangle$，若 $k\in H$，必有 $H=\langle k\rangle$。

综上可知 G 仅有上述 4 个真子群。

8. 设 A、B、C 是群 G 的三个子集。证明：

$$A(B\cup C)=AB\cup AC$$

问：$A(B\cap C)=AB\cap AC$ 是否成立？当 A、B、C 都是子群时又如何？

证明 ①$\forall x\in AB\cup AC$，则

$$x\in AB \text{ 或 } x\in AC$$

若 $x\in AB$，则存在 $a\in A$，$b\in B$ 使

$$x=ab$$

而 $b\in B$ 当然有 $b\in B\cup C$，故

$$x=ab\in A(B\cup C)$$

同理若 $x\in AC$ 时，也有 $x\in A(B\cup C)$，故由 x 的任意性可得

$$AB\cup AC\subseteq A(B\cup C)$$

$\forall x\in A(B\cup C)$，则存在 $a\in A$，$y\in B\cup C$，使

$$x=ay$$

若 $y\in B$，则 $x=ay\in AB$；若 $y\in C$，则 $x=ay\in AC$，从而 $x=ay\in AB\cup AC$，故

$$A(B\cup C)\subseteq AB\cup AC$$

综上可知 $A(B\cup C)=AB\cup AC$。

②$A(B\cap C)=AB\cap AC$ 未必成立。如四次对称群 S_4，设

$$A=\{(1),(1\ 2)\},B=\{(1),(3\ 4)\}$$

$$C=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$$

可求得

$$A(B\cap C)=\{(1),(1\ 2)\}$$

$$AB\cap AC=\{(1),(1\ 2),(3\ 4),(1\ 2)(3\ 4)\}$$

显见 $$A(B\cap C)\neq AB\cap AC$$

③可验证 A、B、C 均为 S_4 的子群，故由②知 A、B、C 为子群时 $A(B\cap C)=AB\cap AC$ 也未必成立。

9. 设 G 是群，且 $|G| = p^t m$，p 是素数，$p \nmid m$。又 H、K 分别是 G 的 p^t、p^s $(0 < s \leqslant t)$ 阶子群，且 $K \nsubseteq H$。证明：HK 不是 G 的子群。

证明 由

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{p^t \cdot p^s}{|H \cap K|}$$

可得 $|HK| \cdot |H \cap K| = p^{s+t}$，又 p 为素数，故必存在正整数 $r \leqslant s+t$，使得

$$|HK| = p^r \quad (0 < r \leqslant s+t)$$

若 HK 为群 G 的子群，则由 Lagrange 定理及 $|G| = p^t m$ 得

$$|HK| \mid p^t m$$

从而可知 $r \leqslant t$ 且

$$|H \cap K| = p^{s+t-r}$$

又因为

$$|H \cap K| \leqslant |K| \leqslant p^s$$

故 $p^{s+t-r} \leqslant p^s$，由于 $r \leqslant t$，因此 $t = r$，且

$$|H \cap K| = p^s = |K|$$

但由 $H \leqslant G, K \leqslant G$ 可知 $H \cap K \leqslant K$，从而

$$K = H \cap K \subseteq H$$

这同题设中 $K \nsubseteq H$ 矛盾，所以假设 HK 为 G 的子群不成立，即 HK 不是 G 的子群。

---

10. 设 G 为数域 F 上某些 n 阶方阵对于方阵的普通乘法作成的群。证明：G 中的方阵或者全是满秩的，或者全是降秩的。

证法 1 若 G 中的方阵均为降秩的，则结论成立。若 G 中存在一个满秩矩阵 $\boldsymbol{A}$，由于 G 对方阵的普通乘法作成群，故任取 $\boldsymbol{B} \in G$，必存在 $\boldsymbol{C} \in G$，使得

$$\boldsymbol{A} = \boldsymbol{BC}$$

从而 $\boldsymbol{A}$、$\boldsymbol{B}$、$\boldsymbol{C}$ 的矩阵行列式满足

$$|\boldsymbol{A}| = |\boldsymbol{B}||\boldsymbol{C}|$$

由 $\boldsymbol{A}$ 是满秩方阵，可知 $|\boldsymbol{A}| \neq 0$，进而 $|\boldsymbol{B}| \neq 0$，即 $\boldsymbol{B}$ 是满秩方阵，由 $\boldsymbol{B}$ 的任意性可知 G 中的方阵都是满秩的。

证法 2 若 G 中的方阵均为降秩的，则结论成立。若 G 中存在一个满秩矩阵 $\boldsymbol{A}$，则 $\boldsymbol{A}$ 存在逆方阵 $\boldsymbol{A}^{-1}$，使 $\boldsymbol{AA}^{-1} = \boldsymbol{E}$(其中 $\boldsymbol{E}$ 为 n 阶单位方阵)，又 G 对

方阵的普通乘法作成群，不妨设 e 为 G 的单位元，则

$$e\boldsymbol{A}=\boldsymbol{A}\in G,(e\boldsymbol{A})\boldsymbol{A}^{-1}=\boldsymbol{A}\boldsymbol{A}^{-1}\in G$$

故 $\boldsymbol{A}\boldsymbol{A}^{-1}=\boldsymbol{E}\in G$，且

$$e\boldsymbol{E}=\boldsymbol{E}=\boldsymbol{E}\boldsymbol{E}$$

从而 $e=\boldsymbol{E}$，所以 n 阶单位方阵即为 G 中的单位元。任取方阵 $\boldsymbol{B}\in G$，故必存在 G 中的方阵 $\boldsymbol{C}$，使得

$$\boldsymbol{C}\boldsymbol{B}=e=\boldsymbol{E}$$

故 $\boldsymbol{B}$、$\boldsymbol{C}$、$\boldsymbol{E}$ 的矩阵行列式满足

$$|\boldsymbol{C}||\boldsymbol{B}|=|\boldsymbol{E}|=1\neq 0$$

从而 $|\boldsymbol{B}|\neq 0$，$\boldsymbol{B}$ 为满秩方阵，由 $\boldsymbol{B}$ 的任意性可知 G 中的每一方阵均是满秩的。

注 ① 由降秩方阵对普通乘法作成的群存在，如 $n=2$ 时，所有二阶方阵

$$\boldsymbol{A}=\begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix}\text{或 }\boldsymbol{B}=\begin{pmatrix}0 & 0\\ 0 & b\end{pmatrix}$$

(其中 $a\neq 0,b\neq 0,a,b\in\mathbf{R}$)，它们分别对方阵的普通乘法作成群，这两个群的单位元分别为

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\text{及}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$$

元 $\boldsymbol{A}$ 及元 $\boldsymbol{B}$ 在它们各自群中的逆元分别为

$$\begin{bmatrix}\frac{1}{a} & 0\\ 0 & 0\end{bmatrix}\text{及}\begin{bmatrix}0 & 0\\ 0 & \frac{1}{b}\end{bmatrix}$$

② 由证明可知数域 F 上的一些满秩方阵(秩为 n) 对方阵的普通乘法作成群，该群中的单位元即为 n 阶单位方阵，群中每一方阵的逆元为这一方阵的逆方阵。实际上，数域 F 上的所有 n 阶满秩方阵对普通乘法作成的群就是本章 §1 引入的一般线性群 $GL_n(F)$。

---

11. 证明：分式的集合

$$G=\left\{x,\frac{1}{x},1-x,\frac{1}{1-x},\frac{x-1}{x},\frac{x}{x-1}\right\}$$

对运算

$$a \circ b = \text{把} b \text{代入} a \text{中的} x \quad (\forall a, b \in G)$$

作成一个群。

证明 设 $y_1, y_2, \cdots, y_6$ 依次表示 G 中的 6 个元素，对给定的运算"$\circ$"，得乘法表如下

$\circ$	y_1	y_2	y_3	y_4	y_5	y_6
y_1	y_1	y_2	y_3	y_4	y_5	y_6
y_2	y_2	y_1	y_4	y_3	y_6	y_5
y_3	y_3	y_5	y_1	y_6	y_2	y_4
y_4	y_4	y_6	y_2	y_5	y_1	y_3
y_5	y_5	y_3	y_6	y_1	y_4	y_2
y_6	y_6	y_4	y_5	y_2	y_3	y_1

方法 1 由乘法表可知 G 对给定的运算是封闭的，且该运算满足结合律；其中 y_1 是单位元，y_1, y_2, y_3, y_6 的逆元是它们自身，y_4 与 y_5 互为逆元。按群的定义可知 G 对运算 $\circ$ 作成一个群。

方法 2 由乘法表知 G 对给定的运算满足结合律，从而 G 是一个有限半群。又乘法表中各行各列元素互异，故消去律成立，由本章 §1 推论 2 可知 G 对运算 $\circ$ 作成一个群。

---

12. 设 a, b 是群 G 中阶分别为 m 与 n 的两个元素。证明：若 $ab = ba$，则

$$|ab| \mid [m, n]$$

且 G 中有阶为 $[m, n]$（m 与 n 的最小公倍）的元素。

证明 由于 $|a| = m$，$|b| = n$，故

$$a^m = e, b^n = e$$

又 $ab = ba$，故

$$(ab)^{[m,n]} = a^{[m,n]} b^{[m,n]} = e$$

因此

$$|ab| \mid [m, n]$$

设 m, n 的标准分解为

$$m = p_1^{s_1} \cdots p_k^{s_k} p_{k+1}^{s_{k+1}} \cdots p_r^{s_r}$$

$$n = p_1^{t_1} \cdots p_k^{t_k} p_{k+1}^{t_{k+1}} \cdots p_r^{t_r}$$

其中 $s_i, t_i (i = 1, 2, \cdots, r) \geqslant 0$，$p_i (i = 1, 2, \cdots, r)$ 为互异素数，且满足

$$s_i \leqslant t_i \quad (i = 1, 2, \cdots, k)$$

$$s_j \geq t_j \quad (j = k+1, k+2, \cdots, r)$$

从而

$$[m, n] = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k} p_{k+1}^{s_{k+1}} \cdots p_r^{s_r}$$

又由于

$$|a^{p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}}| = p_{k+1}^{s_{k+1}} \cdots p_r^{s_r}, \ |b^{p_{k+1}^{t_{k+1}} \cdots p_r^{t_r}}| = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$$

以及

$$ab = ba, \quad (p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}, p_{k+1}^{s_{k+1}} \cdots p_r^{s_r}) = 1$$

所以

$$|a^{p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}} \cdot b^{p_{k+1}^{t_{k+1}} \cdots p_r^{t_r}}| = [m, n]$$

---

13. 设$\langle a^s \rangle$与$\langle a^t \rangle$是循环群$\langle a \rangle$的两个子群，s与t是自然数。证明：

(1)$\langle a^s \rangle \cap \langle a^t \rangle = \langle a^{[s,t]} \rangle$；

(2)$\langle a^s \rangle \langle a^t \rangle = \langle a^{(s,t)} \rangle$。

其中$[s,t]$是s,t的最小公倍，(s,t)是s,t的最大公约。

证明 (1) 一方面，$\forall x \in \langle a^{[s,t]} \rangle$，存在整数$r$，使

$$x = a^{[s,t]r}$$

由于$[s,t]$为s,t的最小公倍，记$[s,t] = ss' = tt'$，则

$$x = (a^s)^{s'r} = (a^t)^{t'r}$$

故$x \in \langle a^s \rangle$且$x \in \langle a^t \rangle$，即$x \in \langle a^s \rangle \cap \langle a^t \rangle$，由$x$的任意性，有

$$\langle a^{[s,t]} \rangle \subseteq \langle a^s \rangle \cap \langle a^t \rangle$$

另一方面，$\forall x \in \langle a^s \rangle \cap \langle a^t \rangle$，存在整数$r$及$p$，使得

$$x = a^{sr} = a^{tp}$$

设$(s,t) = d$，则

$$s = dm, t = dn$$

其中m,n为正整数且$(m,n) = 1$，从而存在整数u,v，使

$$mu + nv = 1, [s,t] = dmn$$

从而

$$x^{mu} = (a^{tp})^{mu} = a^{dnpmu}$$

$$x^{nv} = (a^{sr})^{nv} = a^{dmrnv}$$

$$x = x^{mu+nv} = a^{dmn(pu+rv)} = (a^{[s,t]})^{pu+rv} \in \langle a^{[s,t]} \rangle$$

即 $x \in \langle a^{[s,t]} \rangle$，由 x 的任意性，有

$$\langle a^s \rangle \cap \langle a^t \rangle \subseteq \langle a^{[s,t]} \rangle$$

综上有 $$\langle a^s \rangle \cap \langle a^t \rangle = \langle a^{[s,t]} \rangle$$

(2) 设 $(s,t) = d$，则存在整数 u,v，使

$$su + tv = d$$

一方面，$\forall x \in \langle a^{(s,t)} \rangle = \langle a^d \rangle$，存在整数 p，使

$$x = a^{dp} = a^{(su+tv)p} = (a^s)^{up} \cdot (a^t)^{vp} \in \langle a^s \rangle \langle a^t \rangle$$

从而 $$\langle a^{(s,t)} \rangle = \langle a^d \rangle \subseteq \langle a^s \rangle \langle a^t \rangle$$

另一方面，$\forall x \in \langle a^s \rangle \langle a^t \rangle$，则存在整数 m、n，使

$$x = a^{sm} \cdot a^{tn} = a^{sm+tn}$$

由 $(s,t) = d$ 可知，存在正整数 u、v，且 $(u,v) = 1$，使

$$s = du, t = dv$$

从而

$$x = a^{dum+dvn} = a^{d(mu+nv)} = (a^d)^{mu+nv} \in \langle a^d \rangle$$

所以 $$\langle a^s \rangle \langle a^t \rangle \subseteq \langle a^{(s,t)} \rangle$$

综上可知 $$\langle a^s \rangle \langle a^t \rangle = \langle a^{(s,t)} \rangle$$

---

14. 证明：群 G 是有限群当且仅当 G 只有有限个子群。

证明 必要性是显然的，这是因为若 G 为有限群，则其子集个数有限，从而其子群个数也是有限的。

充分性 当群 G 只有有限个子群时，则由无限循环群有无限个子群可知 G 中每一元素的阶都是有限的，任取 $a_1 \in G$，则 $\langle a_1 \rangle$ 为 G 的一个有限子群。取

$$a_2 \in G - \langle a_1 \rangle$$

则 $\langle a_2 \rangle$ 是 G 的一个异于 $\langle a_1 \rangle$ 的一个有限子群，再取

$$a_3 \in G - (\langle a_1 \rangle \cup \langle a_2 \rangle)$$

则 $\langle a_3 \rangle$ 是 G 的一个异于 $\langle a_1 \rangle$ 与 $\langle a_2 \rangle$ 的有限子群，如此下去，但由于 G 仅有有限个子群，从而上述的过程不能无限地继续下去，从而存在 r，使得

$$G = \langle a_1 \rangle \cup \langle a_2 \rangle \cup \cdots \langle a_r \rangle$$

而 $\langle a_i \rangle (i = 1,2,\cdots,r)$ 都是有限的，所以 G 为一个有限群。

15. 设 H,K 是群 G 的子群,证明:

(1)$(H:H\cap K)\leqslant(G:K)$;

(2) 当$(G:K)$有限时,则$(H:H\cap K)=(G:K)$当且仅当$G=HK$。

证明 (1) 设 $A=\{h(H\cap K)\mid h\in H\}$,$B=\{xK\mid x\in G\}$

由于 $H\subset G$,定义

$$\varphi:h(H\cap K)\longrightarrow hK$$

则 φ 为 A 到 B 的映射。

再证 φ 为单射。若

$$h_1K=h_2K\quad(h_1,h_2\in H)$$

则存在 $k_1,k_2\in K$,使

$$h_1k_1=h_2k_2$$

故由 $K\leqslant G$ 知

$$h_1^{-1}h_2=k_1k_2^{-1}\in K$$

由 $H\leqslant G$ 知

$$h_1^{-1}h_2\in H$$

从而

$$h_1^{-1}h_2\in H\cap K,h_1(H\cap K)=h_2(H\cap K)$$

所以 φ 为集合 A 到集合 B 的一个单射,因此 $|A|\leqslant|B|$,即

$$(H:H\cap K)\leqslant(G:K)$$

(2)"$\Rightarrow$" 若$(H:H\cap K)=(G:K)$,可由$(G:K)$有限及上述证明可知 φ 为集合 A 到集合 B 的双射,从而 $\forall x\in G$,存在 $h\in H$,使得

$$x\in xK=hK\subseteq HK$$

即有 $G\subseteq HK$。又显见 $HK\subseteq G$,所以 $G=HK$。

"$\Leftarrow$" 若 $G=HK$,则 $\forall x\in G$,存在 $h\in H,k\in K$,使

$$x=hk$$

从而

$$xK=hkK=hK$$

所以 φ 是集合 A 到集合 B 的双射,故

$$(H:H\cap K)=(G:K)$$

---

16. 设 G 是一个 $2n$ 阶有限交换群,其中 n 是一个奇数。证明:G 有且只有一

个 2 阶元素。

证明 依题意，问题可化为证明 G 有且仅有一个 2 阶子群。

先证 2 阶子群的存在性。由 $|G| = 2n$，及本章 §2 第 4 题可知 G 中阶等于 2 的元素，必存在且有奇数个。不妨设 a 为 G 的一个 2 阶元素，则 $H = \{e,a\}$ 为 G 的一个 2 阶子群。

下证 2 阶子群的惟一性。若 $b \in G$，$|b| = 2$ 且 $b \neq a$，则 $K = \{e,b\}$ 为 G 的一个异于 H 的 2 阶子群。又 G 为交换群，故

$$HK = \{e,a,b,ab\}$$

为 G 的一个 4 阶子群，从而由 Lagrange 定理可知

$$|HK| \mid |G|$$

即 $4 \mid 2n$，$2 \mid n$，这与 n 是一个奇数相矛盾，故 $b = a$，$H = K$，即 G 只能有一个 2 阶子群。

---

17. 设 H 是群 G 的一个周期子群，且 $(G:H)$ 有限。证明：G 是周期群。

证明 任意的 $a \in G$，$a,a^2,a^3,\cdots$，不可能属于 G 的不同陪集，否则指数 $(G:H)$ 无限与题设矛盾，从而存在 s 与 t（不妨设 $s > t$），使

$$a^sH = a^tH$$

故 $a^{-t}a^s = a^{s-t} \in H$。又 H 是周期群，因此 a^{s-t} 的阶有限，设 $|a^{s-t}| = m$，则

$$(a^{s-t})^m = a^{(s-t)m} = e$$

$$|a| \leqslant (s-t)m$$

即 a 的阶有限，由 a 的任意性可知 G 是周期群。

---

18. 证明：15 阶交换群必为循环群。

证法 1 不妨设 G 是一个 15 阶交换群，在 G 中任取 $a \neq e$，设 $|a| = m$，则由 Lagrange 定理知，$m \mid 15$，故 $m = 3,5$ 或 15。

下证 G 中除单位元 e 外，其他元素的阶不可能都是 3。否则，设 a、$b \in G$ 满足

$$|a| = |b| = 3, b \notin \langle a\rangle$$

则 $H = \langle a\rangle$，$K = \langle b\rangle$ 是 G 的两个不同的 3 阶子群，且 $H \cap K = \{e\}$，故

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = 3 \cdot 3 = 9$$

又 G 为交换群，故 $HK \leqslant G$，从而由 Lagrange 定理有

$$|HK| \mid |G|\text{，即 } 9 \mid 15$$

矛盾，所以 G 必有 5 阶或 15 阶元素。

若 G 中有 5 阶元素，则由本章 §7 推论 3 知 G 最多有一个 5 阶子群，所以一定有元素的阶为 3 或 15。若有元素的阶为 3，则由于 $(3,5)=1$ 及 G 为交换群可知，G 一定有 15 阶元素。从而无论 G 有 3 阶元还是 5 阶元，G 总有 15 阶元。即 G 为循环群。

证法 2 类似于证法 1，$\forall a \in G, a \neq e$，

$$|a| = m = 3,5 \text{ 或 } 15$$

若 $m = 15$，则 $G = \langle a \rangle$ 为循环群；

若 $m = 3$，则 $\langle a \rangle$ 为 G 的 3 阶循环群。又 G 可换，故

$$|G/\langle a \rangle| = 15/3 = 5$$

又 5 为素数，故 $G/\langle a \rangle$ 为循环群，记

$$\langle \bar{b} \rangle = G/\langle a \rangle, b \in G, |\langle \bar{b} \rangle| = 5$$

由 $|b| \neq 1$ 且 $|b| \neq 3$（否则由 Lagrange 定理 $3 \mid 5$，矛盾），故 $|b| = 5$ 或 $|b| = 15$，若 $|b| = 15$，则 $G = \langle b \rangle$ 为循环群；

若 $|b| = 5$，则由于 $|a| = 3$，G 可换，$|ab| = 15$，$G = \langle ab \rangle$ 为循环群。

---

19. 设 e 是幺半群 S 的单位元，又 $a,b \in S$。证明：a 是以 b 为逆元的可逆元当且仅当

$$aba = a, ab^2a = e$$

证明 “$\Leftarrow$” 若 $aba = a, ab^2a = e$，则

$$ab = (aba)b = (ab)(ab) = (ab)^2$$

$$ba = b(aba) = (ba)(ba) = (ba)^2$$

从而

$$(ab)(ba) = (ab)^2ba = (ab)(ab)ba = ab(ab^2a) = abe = ab$$

$$(ab)(ba) = ab(ba)^2 = (ab)(ba)(ba) = (ab^2a)(ba) = eba = ba$$

又因为 $(ab)(ba) = ab^2a = e$，所以

$$ab = ba = e$$

即 a 是以 b 为逆元的可逆元。

"⇒" 设 a 是以 b 为逆元的可逆元，则

$$ab = ba = e$$

从而

$$aba = a(ba) = ae = a$$
$$ab^2a = (ab)(ba) = ee = e$$

---

20. 证明：无限循环群的非 e 子群的指数均有限。

证明 依题意记 $G = \langle a \rangle$ 为无限循环群，H 为 G 的非 e 子群，即

$$H \neq \{e\}, H = \langle a^s \rangle \leqslant G$$

其中 s 为 H 中所含元素的最小正指数，下证明

$$G = a^0H \cup aH \cup \cdots \cup a^{s-1}H \text{ 且 } a^iH \cap a^jH = \varnothing$$

其中 $i \neq j(i,j = 0,1,\cdots,s-1)$。

任取 $a^k \in G$，则由 $G = \langle a \rangle$ 可知存在 q 及 $r(0 \leqslant r < s)$，使 $k = sq + r$，又 $H = \langle a^s \rangle$，故

$$a^k = a^{sq+r} = a^r(a^s)^q \in a^rH$$

由 a^k 的任意性可知

$$G \subseteq a^0H \cup aH \cup \cdots \cup a^{s-1}H$$

又显见有

$$a^0H \cup aH \cup \cdots \cup a^{s-1}H \subseteq G$$

故
$$G = a^0H \cup aH \cup \cdots \cup a^{s-1}H$$

若 $a^iH \cap a^jH \neq \varnothing$，则存在 $x \in a^iH \cap a^jH$ $(i \neq j, i,j = 0,1,\cdots, s-1)$。不妨设 $i < j$，则存在 $h_i \in H, h_j \in H$，使

$$x = a^ih_i = a^jh_j$$

又 $H \leqslant G$，故

$$a^{j-i} = h_ih_j^{-1} \in H$$

其中 $0 < j - i < s$，这与假设 s 为 H 中所含元素的最小正指数相矛盾，故

$$a^iH \cap a^jH = \varnothing \quad (i \neq j, i,j = 0,1,\cdots,s-1)$$

从而

$$G = a^0H \cup aH \cup \cdots \cup a^{s-1}H$$

是 G 关于子群 H 的左陪集分解，所以 H 在 G 中的指数 $(G:H)$ 有限。

21. 举出一个无限群，其任何真子群的指数均无限。

解 有理数加群 Q_+ 的任何真子群在 Q_+ 中的指数均无限。

设 H 为 Q_+ 的任一真子群，则 $H \subset Q_+$。当 $H = \{0\}$ 时，显见 H 在 Q_+ 中的指数是无限的，下设 $H \neq \{0\}$。

① 先证存在有理数 $a \notin H$ 及素数 p，使 $pa \in H$。

由 $H \neq \{0\}$ 及 $H \subset G$ 可知，存在有理数 $\frac{c}{b} \in H$ 且 $\frac{c}{b} \neq 0$，从而 $b \cdot \frac{c}{b} = c \in H$，即 H 中含有整数 c，不妨设 $c > 0$，且 c 的标准分解为

$$c = p_1 p_2 \cdots p_m \in H \quad (p_i \text{ 为素数})$$

下取 $a \notin H$，若 a 为一整数，则 $ac \in H$，即

$$p_1 p_2 \cdots p_m a \in H$$

由此可逐次考查 $p_m a, p_{m-1} p_m a, \cdots$ 是否属于 H，进而可得所要结论。

若 a 为一分数，设 q_i 为素数，

$$a = \frac{t}{q_1 q_2 \cdots q_n}$$

当 $t \notin H$ 时，则类似的由于 $tc \in H$ 可得素数 q，使 $qa \in H$。

当 $t \in H$ 时，则由于

$$q_1 q_2 \cdots q_n a = t \in H$$

逐步考查 $q_n a, q_{n-1} q_n a, \cdots$ 是否属于 H 即可得所要结论。

综上可知，存在有理数 $a \notin H$ 及素数 p，使 $pa \in H$。

② 由于 $a \notin H$，而 $H \leqslant Q_+$，故显然有

$$a, \frac{a}{p}, \frac{a}{p^2}, \cdots, \frac{a}{p^n}, \cdots$$

都不在 H 中，下证它们关于子群 H 属于不同的陪集。若

$$\frac{a}{p^m} = \frac{a}{p^n} + h \quad (h \in H, m > n)$$

则
$$a = p^{m-n} a + p^m h$$

但由 ① 知 $pa \in H$，所以 $p^{m-n} a \in H$，又 $p^m h \in H$，从而由 $a = p^{m-n} a + p^m h$ 知 $a \in H$，与 $a \notin H$ 矛盾。

由上可知有无限个有理数是属于 Q_+ 关于 H 的不同左陪集，故 H 在 Q_+ 中的指数无限。

22. 证明:4 次交代群 A_4 无 6 阶子群。

证明 4 次交代群 A_4 是 4 次对称群 S_4 中全体偶置换作成的一个 12 阶子群,下用反证法证明 A_4 无 6 阶子群。

假设 A_4 有 6 阶子群 H,则由 Lagrange 定理知 H 中除了单位元恒等置换(1) 外,其他元素可能为 2 阶元或 3 阶元(A_4 中有 1 个单位元,3 个 2 阶元,8 个 3 阶元)。

由于 A_4 中 2 阶元仅有(1 2)(3 4),(1 3)(2 4),(1 4)(2 3)3 个,因此 H 中的置换不可能全是 2 阶元。又由于 A_4 中 3 阶元有

$$\sigma_1 = (1\ 2\ 3), \sigma_2 = (1\ 3\ 2), \sigma_3 = (1\ 2\ 4), \sigma_4 = (1\ 4\ 2)$$

$$\sigma_5 = (1\ 3\ 4), \sigma_6 = (1\ 4\ 3), \sigma_7 = (2\ 3\ 4), \sigma_8 = (2\ 4\ 3)$$

共 8 个,其中 σ_1 与 σ_2,σ_3 与 σ_4,σ_5 与 σ_6,σ_7 与 σ_8 分别互逆,因此 H 中也不可能全是 3 阶元,故 H 中 2 阶元与 3 阶元(与其逆元成对出现)必同时存在。

设 H 中含有 1 个 2 阶元,4 个 3 阶元,如

$$H = \{(1), (1\ 2)(3\ 4), \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

则由 $H \leqslant A_4$ 可知

$$(1\ 2)(3\ 4) \cdot \sigma_1 = \sigma_8 \in H, \sigma_1 \cdot (1\ 2)(3\ 4) = \sigma_5 \in H$$

这与 $|H| = 6$ 矛盾。

H 的其他情形与此类似,所以 A_4 无 6 阶子群。

---

23. 设 G 是集合 $M = \{1,2,\cdots,n\}$ 上的一个置换群,又 $i \in M$,令

$$G_i = \{\tau \mid \tau \in G, \tau(i) = i\}, G(i) = \{\tau(i) \mid \tau \in G\}$$

证明:(1)$G_i \leqslant G$;

(2) 若 s、$t \in G(i)$,则有 $\sigma \in G$ 使 $\sigma(s) = t$;

(3) $|G| = |G_i| \cdot |G(i)|$。

证明 (1) 因为恒等置换(1) $\in G_i$,故 $G_i \neq \varnothing$。又任意的 $\tau_1, \tau_2 \in G_i$,则

$$\tau_1\tau_2(i) = \tau_1(i) = i, \tau_1^{-1}(i) = \tau_1^{-1}(\tau_1(i)) = i$$

故 $\tau_1\tau_2 \in G_i$,$\tau_1^{-1} \in G_i$,从而 $G_i \leqslant G$。

(2) 设 s、$t \in G(i)$,由 $G(i)$ 定义,则存在 $\tau_1, \tau_2 \in G$,使得

$$s = \tau_1(i), t = \tau_2(i)$$

令 $\sigma = \tau_2\tau_1^{-1}$,则 $\sigma \in G$,且有

$$\sigma(s)=\tau_2\tau_1^{-1}(s)=\tau_2(i)=t$$

(3) 设 $G(i)=\{\tau_1(i),\tau_2(i),\cdots,\tau_m(i)\}$ 是 M 中 m 个互异的元素，则 $|G(i)|=m$。

一方面，若 $\tau_s^{-1}\tau_t\in G_i$，

$$\tau_s^{-1}\tau_t(i)=i,\tau_t(i)=\tau_s(i)$$

则只有 $s=t$。

另一方面，任意 $\tau\in G$，则 $\tau(i)\in G(i)$，故存在 $\tau_k(1\leqslant k\leqslant m)$，使

$$\tau(i)=\tau_k(i),\tau_k^{-1}\tau(i)=i$$

所以 $\tau_k^{-1}\tau\in G_i,\tau\in\tau_kG_i$，从而

$$G=\tau_1G_i\cup\tau_2G_i\cup\cdots\cup\tau_mG_i$$

是 G 关于子群 G_i 的一个左陪集分解。

因此

$$(G:G_i)=|G(i)|=m$$

所以由 Lagrange 定理

$$|G|=|G_i|\cdot(G:G_i)=|G_i|\cdot G(i)$$

---

24. 设 G,M 如上题，又令 $A\subseteq M$，且

$$G_A=\{\tau\mid\tau\in G,\text{对每个 } i\in A \text{ 都有 } \tau(i)=i\}$$

$$G^A=\{\tau\mid\tau\in G,\text{对每个 } i\in A \text{ 都有 } \tau(i)\in A\}$$

证明：$G_A\leqslant G^A\leqslant G$。

证明 恒等置换$(1)\in G_A$，故 $G_A\neq\varnothing$。又任 $\tau_1,\tau_2\in G_A$，$\forall i\in A$，有

$$\tau_1(i)=i,\tau_2(i)=i$$

从而

$$\tau_1\tau_2(i)=i,\tau_1^{-1}(i)=\tau_1^{-1}\tau_1(i)=i$$

故 $\tau_1\tau_2\in G_A,\tau_1^{-1}\in G_A$，所以 $G_A\leqslant G$。

恒等置换$(1)\in G^A$，故 $G^A\neq\varnothing$，又 $\forall\tau_1,\tau_2\in G^A$，$\forall i\in A$，有

$$\tau_1(i)\in A,\tau_2(i)\in A$$

且存在 $k\in A$，使 $i=\tau_1(k)$，从而

$$\tau_1\tau_2(i)=\tau_1(j)\in A,\tau_1^{-1}(i)=\tau_1^{-1}\tau_1(k)=k\in A$$

其中 $j=\tau_2(i)\in A$，即

$$\tau_1\tau_2\in A,\tau_1^{-1}\in A$$

故 $G^A \leqslant G$，又显见 $G_A \leqslant G^A$，所以

$$G_A \leqslant G^A \leqslant G$$

---

25. 证明：以下的 M_1 与 M_2 都是 n 次对称群 S_n 的生成系：

(1)$M_1 = \{(1\ 2),(1\ 3),\cdots,(1\ n)\}$；

(2)$M_2 = \{(1\ 2),(1\ 2\cdots n)\}$。

证明 (1) 因为每个置换都可表为对换之积(参见教材本章§6定理2)及对换

$$(i\ j) = (1\ i)(1\ j)(1\ i)$$

所以每个置换都可表为若干个含1的对换之积，从而

$$M_1 = \{(1\ 2),(1\ 3),\cdots,(1\ n)\}$$

是 S_n 的一个生成系。

(2) 令 $\tau = (1\ 2)$，$\sigma = (1\ 2\cdots n)$，对 i 用归纳法可以证明

$$\sigma^{1-i}\tau\sigma^{i-1} = (i,i+1) \in \langle\tau,\sigma\rangle \quad (1 \leqslant i \leqslant n-1)$$

当 $j > i+1$ 即 $i < j-1$ 时，有

$$(j,j-1)\cdots(i+2,i+1)(i,i+1)(i+1,i+2)\cdots(j-1,i)$$
$$= (i,j) \in \langle\tau,\sigma\rangle$$

从而 $\langle\tau,\sigma\rangle$ 包含一切对换，所以 $\langle\tau,\sigma\rangle = S_n$，即 $M_2 = \{\tau,\sigma\}$ 也是 S_n 的一个生成系。

---

26. 设有一个正三角形 ABC，如图2-1所示，中心为 O，现使它在空间中运动，但运动前后仍占有同一空间位置。问：这样的运动(包括正三角形不动的运动)共有多少个？它与 $M = \{A,B,C\}$ 上的三次对称群有何关系？

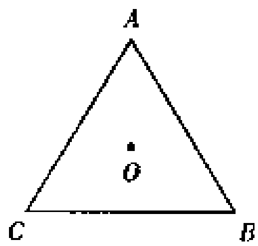

图 2-1

解 这样的运动共有6个。

第一类是 $\triangle ABC$ 不动或 $\triangle ABC$ 绕中心 O 旋转 $2n\pi$ 弧度的运动(运动后 A、B、C 三点仍分别变为 A、B、C)，记该运动为 σ_0，即 σ_0 是 A、B、C 三点的恒等交换。

第二类是分别以 OA、OB、OC 为轴在空间各旋转 π 弧度的运动，此时，$\triangle ABC$ 旋转前后占同一位置。

以 OA 为轴旋转 π 弧度时，A 点不动，B、C 两点位置互换，记这一运动为 σ_1，即

$$\sigma_1=\begin{pmatrix}A & B & C\\ A & C & B\end{pmatrix}$$

以 OB 为轴旋转 π 弧度时，B 点不动，A、C 两点位置互换，记这一运动为 σ_2，即

$$\sigma_2=\begin{pmatrix}A & B & C\\ C & B & A\end{pmatrix}$$

以 OC 为轴旋转 π 弧度时，C 点不动，A、B 两点位置互换，记这一运动为 σ_3，即

$$\sigma_3=\begin{pmatrix}A & B & C\\ B & A & C\end{pmatrix}$$

第三类是在 $\triangle ABC$ 所在平面内，$\triangle ABC$ 绕中心 O 按逆时针旋转 $\frac{\pi}{3}$ 或 $\frac{2\pi}{3}$ 弧度，这两个运动前后 $\triangle ABC$ 仍占同一位置，A、B、C 三点分别变为 B、C、A 和 C、A、B，分别记这两个运动为 σ_4，σ_5，即

$$\sigma_4=\begin{pmatrix}A & B & C\\ B & C & A\end{pmatrix},\sigma_5=\begin{pmatrix}A & B & C\\ C & A & B\end{pmatrix}$$

使 $\triangle ABC$ 运动前后仍占同一空间位置的其他运动，都是以这三类 6 个运动中某些运动连续施行的结果，且仍在这 6 个运动之中。即使正 $\triangle ABC$ 占同一空间位置的运动共有 6 个，且它们关于运动的运算（即置换的乘法）作成一个群，实际上，它就是 $M=\{A、B、C\}$ 上的三次对称群。

第三章 正规子群和群的同态与同构

导读

一、基本要求

1. 理解并掌握群的同态与同构及其性质。

2. 掌握正规子群和商群的概念，能够熟练判定一个子群是否构成正规子群，掌握相关结论。

3. 掌握群的同态基本定理的结论及证明。

4. 理解群的同构定理与自同构群。

5. 了解共轭关系与正规化子的概念。

6. 了解群的直积和有限交换群。

7. 理解 Sylow 定理。

二、重点与难点

1. 同态的性质与同态基本定理。

2. 正规子群和商群。

知识点考点精要

一、群的同态与同构

1. 定义

① 同态映射

设 G 与 $\overline{G}$ 是两个群，如果有一个 G 到 $\overline{G}$ 的映射 φ 满足

$$\varphi(ab)=\varphi(a)\varphi(b)\quad(\forall a,b\in G)$$

则称 φ 为群 G 到群 $\overline{G}$ 的一个同态映射。

② 同态

若群 G 到群 $\overline{G}$ 的同态映射 φ 为满射，则称群 G 与群 $\overline{G}$ 同态，记作 $G\sim\overline{G}$。

③ 同构映射与同构

若存在群 G 到群 $\overline{G}$ 的一个同态双射 φ，则称 φ 为同构映射，群 G 与群 $\overline{G}$ 同构，记作 $G\cong\overline{G}$。

④ 自同态与自同构

群 G 到自身的同态映射与同构映射，分别称为群 G 的自同态映射与自同构映射，简称为群 G 的自同态与自同构。

2. 同态与同构的性质

(1) 设 G 是一个群，$\overline{G}$ 是一个有代数运算（也称为乘法）的集合。若 $G\sim\overline{G}$，则 $\overline{G}$ 也是群（要求同态映射为满射）。

(2) 设 φ 是群 G 到群 $\overline{G}$ 的一个同态映射（不一定是满射）。则群 G 的单位元的象是群 $\overline{G}$ 的单位元；G 的元素 a 的逆元的象是 a 的象的逆元，即

$$\overline{a^{-1}}=\overline{a}^{-1}\text{ 或 }\varphi(a^{-1})=\varphi(a)^{-1}$$

(3) 若 G 与 $\overline{G}$ 为各有一个代数运算的代数系统，且 $G\cong\overline{G}$，则当 G 与 $\overline{G}$ 中有一个是群时，另一个也必然是群。

(4) 设 φ 为群 G 到群 $\overline{G}$ 的一个同态映射（不一定是满射），则

① 当 $H\leqslant G$ 时，有 $\varphi(H)\leqslant\overline{G}$ 且 $H\sim\varphi(H)$；

② 当 $\overline{H}\leqslant\overline{G}$ 时，有 $\varphi^{-1}(\overline{H})\leqslant G$，且在 φ 之下诱导出 $\varphi^{-1}(\overline{H})$ 到 $\overline{H}$ 的一个同态映射。

(5) 群 G 到群 $\overline{G}$ 的同态映射 φ 是单射的充要条件是群 $\overline{G}$ 的单位元 $\overline{e}$ 的逆象只有 e。

三、正规子群、商群与单群

1. 正规子群

(1) 定义

正规子群

设 N 是群 G 的一个子群，如果对 G 中每个元素 a 都有

$$aN=Na$$

即

$$aNa^{-1} = N$$

则称 N 是群 G 的一个正规子群(或不变子群),记为 $N \trianglelefteq G$。

若 N 不是群 G 的一个正规子群,则记为 $N \ntrianglelefteq G$。

若 $N \trianglelefteq G$ 且 $N \neq G$,则记为 $N \triangleleft G$。

G 的平凡子群 $\{e\}$ 与 G 均为 G 的正规子群,称为 G 的平凡正规子群;其他正规子群若存在的话,则称为 G 的非平凡正规子群。

(2) 正规子群的简单性质

① 交换子群均为正规子群。

② 若 $N \trianglelefteq G$,且 $N \leqslant H \leqslant G$,则 $N \trianglelefteq H$。

③ 群 G 的中心 $C(G)$ 是 G 的一个正规子群,即 $C(G) \trianglelefteq G$。

④ 正规子群的任何一个左陪集都是一个右陪集(由此可简称为陪集)。

(3) 正规子群的判定

① 设 G 是群,$N \leqslant G$,则

$$N \trianglelefteq G \Leftrightarrow aNa^{-1} \subseteq N \quad (\forall a \in G)$$

② 设 G 是群,$N \leqslant G$,则

$$N \trianglelefteq G \Leftrightarrow axa^{-1} \in N \quad (\forall a \in G, \forall x \in N)$$

(4) 同态满射下的正规子群

设 φ 是群 G 到群 $\overline{G}$ 的一个同态满射,则在 φ 之下 G 的正规子群的象是 $\overline{G}$ 的一个正规子群,$\overline{G}$ 的正规子群的逆象是 G 的一个正规子群。

(5) 正规子群的乘积

① 群 G 的一个正规子群与一个子群的乘积是一个子群;

② 两个正规子群的乘积仍是一个正规子群。

(6) 哈密顿群

设 G 是一个非交换群。若 G 的每个子群都是 G 的正规子群,则称 G 是一个哈密顿群。

2. 商群

(1) 陪集的乘法

设 N 是群 G 的一个正规子群,则任取二陪集 aN 与 bN,有

$$(aN)(bN) = (ab)N$$

称之为陪集的乘法。

注 $N \lhd G$ 时，陪集的乘法是 N 的全体陪集的一个代数运算。

(2) 商群的定义

群 G 的正规子群 N 的全体陪集对于陪集的乘法作成一个群，称为 G 关于 N 的商群，记作 G/N。

(3) 商群的阶

① $|G/N| = (G : H)$

这由商群 G/N 中的元素就是 N 在 G 中的陪集可知。

② 若 G 为有限群，则

$$|G/N| = \frac{|G|}{|N|}$$

这由 Lagrange 定理可知。

(4) 商群的应用

①Cauchy 定理

设 G 是一个 pn 阶有限交换群，其中 p 是一个素数，则 G 有 p 阶元素，从而有 p 阶子群。

②pq 阶交换群必为循环群，其中 p、q 为互异素数。

3. 单群

(1) 定义

阶大于 1 且只有平凡正规子群的群称为单群。

(2) 有限交换单群的判定

有限交换群 G 为单群 $\Leftrightarrow |G|$ 为素数。

三、群同态基本定理

1. 相关定义

(1) 自然同态

群 G 到其商群 G/N 的同态满射

$$\tau : a \longrightarrow aN$$

称为 G 到商群 G/N 的自然同态。

(2) 核

设 φ 是群 G 到群 $\overline{G}$ 的一个同态映射，$\overline{G}$ 的单位元在 φ 之下所有逆象作成的集合称为 φ 的核，记作 $\mathrm{Ker}\varphi$。

(3) 象集

集合 $\{\varphi(a) \mid \forall a \in G\}$（其中 G 为群）称为 φ 的象集，记作 $\mathrm{Im}\varphi$。

注 ①$\mathrm{Ker}\varphi \leqslant G$，$\mathrm{Im}\varphi \leqslant \overline{G}$。

② 自然同态 τ 的核为 N。

2. 群与其商群间的关系

设 G 为群，$N \trianglelefteq G$，则

$$G \sim G/N$$

即任何群 G 均与其商群同态。

3. 群同态基本定理

设 φ 是群 G 到群 $\overline{G}$ 的一个同态满射。则 $N = \mathrm{Ker}\varphi \trianglelefteq G$，且

$$G/N \cong \overline{G}$$

注 ① 在同构意义下，每个群能且只能同它的商群同态。

② 设 G 与 $\overline{G}$ 是两个有限群，若 $G \sim \overline{G}$，则

$$|\overline{G}| \mid |G|$$

但其逆不真，即若有限群 $\overline{G}$ 的阶整除群 G 的阶，未必有 $G \sim \overline{G}$。如 $\overline{G} = S_3$，即三次对称群；$G = U_{12}$，即 12 次单位根群。

4. 循环群的同态象

(1) 设 G 与 $\overline{G}$ 是两个群且有 $G \sim \overline{G}$。若 G 是循环群，则 $\overline{G}$ 也是循环群。

注 当 G 与 $\overline{G}$ 间的同态映射不是满射时，若 G 为循环群，则 G 的同态象 $\varphi(G)$ 为循环群。

(2) 循环群的商群也是循环群。

5. 同态映射下两个群的子群间的关系

(1) 设 φ 是群 G 到群 $\overline{G}$ 的一个同态映射，又 $H \leqslant G$，如果 $H \supseteq \mathrm{Ker}\varphi$，则

$$\varphi^{-1}[\varphi(H)] = H$$

(2) 设 φ 是群 G 到群 $\overline{G}$ 的一个同态满射，K 是核。则 G 的含 K 的所有子群与 $\overline{G}$ 的所有子群间可建立一个保持包含关系的双射。

四、 群同构定理

1. 第一同构定理

设 φ 是群 G 到群 $\overline{G}$ 的一个同态满射，又 $\mathrm{Ker}\varphi \subseteq N \trianglelefteq G, \overline{N} = \varphi(N)$，则

$$G/N \cong \overline{G}/\overline{N}$$

推论　设 G 为群，$H \trianglelefteq G, N \trianglelefteq G$，且 $N \subseteq H$，则

$$G/H \cong G/N/H/N$$

2. 第二同构定理

设 G 为群，$H \leqslant G, N \trianglelefteq G$，则

$$H \cap N \trianglelefteq H \text{ 且 } HN/N \cong H/(H \cap N)$$

3. 第三同构定理

设 G 为群，$N \trianglelefteq G, \overline{H} \leqslant G/N$，则

(1) 存在 G 的惟一子群 $H \supseteq N$，且 $\overline{H} = H/N$；

(2) 又当 $\overline{H} \trianglelefteq G/N$ 时，有惟一的 $H \trianglelefteq G$，使

$$\overline{H} = H/N \text{ 且} G/H \cong G/N/H/N$$

注　① 商群 G/N 的子群仍为商群，呈 H/N 形，其中 H 是 G 的含 N 的子群，且商群的商群可类似于普通分数那样进行约分。

② $H \trianglelefteq G \Leftrightarrow (H/N) \trianglelefteq (G/N)$。

五、 群的自同构群

1. 自同构群及性质

(1) 定义

① 自同构群

设 M 是一个有代数运算(叫做乘法)的集合。则 M 的全体自同构关于变换的乘法作成一个群，称之为 M 的自同构群。

群 G 的全体自同构关于变换的乘法作成一个群。这个群称为群 G 的自同构群，记作 $\mathrm{Aut}G$。

② 内自同构

设 G 是一个群，$a\in G$，定义

$$\sigma_a: x \longrightarrow axa^{-1} \quad (x\in G)$$

则 σ_a 是 G 的一个自同构，称为 G 的一个内自同构。

③ 内自同构群

群 G 的全体内自同构关于变换的乘法作成一个群，称为群 G 的内自同构群，记作 $\mathrm{Inn}G$。

(2) 自同构群的简单性质

① 无限循环群的自同构群是一个 2 阶循环群；

n 阶循环群的自同构群是一个 $\varphi(n)$ 阶群，其中 $\varphi(n)$ 为 Euler 函数。

② 无限循环群的自同构群与 3 阶循环群的自同构群同构。

③$\mathrm{Inn}G \trianglelefteq \mathrm{Aut}G$。

④ 设 G 为群，则 $N\trianglelefteq G \Leftrightarrow N$ 对 G 的所有内自同构都不变。

⑤ 设 C 是群 G 的中心，则

$$\mathrm{Inn}G\cong G/C$$

2. 特征子群与全特征子群

(1) 定义

① 特征子群

对群 G 的所有自同构都不变的子群，即对 G 的任何自同构 σ 都有

$$\sigma(N)\subseteq N$$

的子群 N，称为群 G 的特征子群。

注 a. 群 G 与 $\{e\}$ 是 G 的特征子群。

b. 群 G 的中心 $C(G)$ 是 G 的特征子群。

② 全特征子群

设 G 为群，$H\leqslant G$，若 H 对 G 的每个自同态都不变，即对 G 的每个自同态映射 Ψ 都有

$$\Psi(H)\subseteq H$$

则称 H 为群 G 的一个全特征子群。

(2) 全特征子群、特征子群与正规子群(不变子群)的关系

$$\text{全特征子群}\subset\text{特征子群}\subset\text{正规子群}$$

注 正规子群不具有传递性，但特征子群与全特征子群具有传递性，

即群的(全)特征子群的(全)特征子群仍为原群的(全)特征子群。

六、共轭关系与正规化子

1. 共轭关系与正规化子

(1) 定义

① 共轭

设 a,b 为群 G 的两个元素,若存在元素 $c \in G$,使

$$a = cbc^{-1}$$

则称 a 与 b 共轭,也称 a 是 b 的共轭元素。

注 a. 共轭是一个等价关系。

b. $a \in G$,则 a 与自身共轭 $\Leftrightarrow a \in C(G)$。

② 类等式

设 G 为有限群,C 为 G 的中心,$c_0 = |C|$,G 中其他共轭类(若存在的话,每类中元素的个数都大于 1) 设为 $C_1, C_2, \cdots, C_m$,且其元素的个数分别表示为 $c_1, c_2, \cdots, c_m$,则

$$|G| = c_0 + c_1 + \cdots + c_m$$

并称这一等式为群 G 的类等式或类方程(也称为群等式或群方程)。

③ 正规化子

设 S 是群 G 的一个子集,称

$$N(S) = \{x \mid x \in G, xS = Sx \text{ 即 } xSx^{-1} = S\}$$

为 S 在 G 中的正规化子。

元素 a 的正规化子记为 $N(a)$。

④ 共轭子集与共轭子群

设 S 是群 G 的一个非空子集,则称 $xSx^{-1}(x \in G)$ 为 S 的一个共轭子集。

当 S 是子群时,称 xSx^{-1} 为 S 的一个共轭子群。

注 a. 子集(子群) 的共轭关系是一个群的所有非空子集(所有子群) 间的一个等价关系,因此可将一个群的所有非空子集(子群) 按是否共轭来进行分类,每个这样的类称为一个共轭子集(子群) 类。

b. 设 G 为群,$H \leqslant G$,则 H 只与自身共轭(即此共轭子群类只含有一个子群)$\Leftrightarrow H \trianglelefteq G$。

(2) 正规化子的性质

① 设 S 是群 G 的任一非空子集，则

a. $N(S) \leqslant G$；

b. 当 $S = H \leqslant G$ 时，$H \subseteq N(H)$ 且 $H \trianglelefteq N(H)$。

② 设 G 为群，$H \leqslant G$，则 $N(H)$ 是 G 中以 H 作为其正规子群的最大子群。

③ 设 G 为群，$H \leqslant G$，则 $N(H) = G \Leftrightarrow H \trianglelefteq G$。

(3) 共轭子集类中子集的个数

① 设 S 是群 G 的一个非空子集，$N(S)$ 为 S 在 G 中的正规化子，则 G 中与 S 共轭的子集数等于 $(G : N(S))$，即 S 的所有共轭子集与 G 关于 $N(S)$ 的所有陪集间可建立双射。

② 群 G 中与元素 a 共轭的元素个数为 $(G : N(a))$。

③ 群 G 中与子群 H 共轭的子群个数为 $(G : N(H))$。

注 若 G 为有限群，则 G 中每个共轭子群类中子群个数都是 $|G|$ 的一个因数。

(4) 类等式的应用

①(A. L. Cauchy 定理) 设 G 是一个有限群，且 $|G| = pn$，其中 p 是一个素数，则 G 有 p 阶子群。

注 这一结论在一定意义下是 Lagrange 定理的逆定理。

② pq 阶群有惟一的 q 阶正规子群，其中 p,q 为素数且 $p < q$。

(5) 共轭元素类与共轭子群类间的关系

① 设 S,T 是群 G 的两个共轭子集，且 $T = cSc^{-1}$，$c \in G$，则

$$N(T) = cN(S)c^{-1}\text{，即 } N(cSc^{-1}) = cN(S)c^{-1}$$

② 设 C_1 是群 G 的一个共轭元素类，则 C_1 中各元素的正规化子作成的集合恰好是 G 的一个共轭子群类。

(6) 共轭子群的指数

① 共轭子群在群中有相同的指数。

② 若群 G 中有一个具有有限指数(大于 1) 的子群，则在 G 中必有一个具有有限指数(大于 1) 的正规子群。

2. 中心化子与相关性质

(1) 定义

设 S 是群 G 的一个非空子集，记

$$C(S) = \{x \mid x \in G, x \text{与} S \text{中每个元素可换}\}$$

称 $C(S)$ 为 S 在 G 中的中心化子。

(2) 性质

设 G 为群，$H \leqslant G$，则

$$C(H) \trianglelefteq N(H)$$

注　若 H 为群 G 的任意非空子集，该结论仍成立。

七、群的直积

1. 直积的定义及性质

(1) 定义

① 加氏积

设 $A_1, A_2, \cdots, A_n$ 为任意 n 个集合，则称集合

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in A_i\}$$

为这 n 个集合的加氏积，其中

$$(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n) \Leftrightarrow a_i = b_i \quad (i = 1, 2, \cdots, n)$$

② 外直积

设 $A_i(i = 1, 2, \cdots, n)$ 为任意 n 个群，则加氏积 $A_1 \times A_2 \times \cdots \times A_n$ 对运算

$$(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n)$$

作成一个群，称为群 $A_1, A_2, \cdots, A_n$ 的外直积，而称每个 A_i 为这个直积的一个直积因子。

注　a. 外直积是交换群(有限群)$\Leftrightarrow$ 每个直积因子为交换群(有限群)。

b. $A_i(i = 1, 2, \cdots, n)$ 为有限群时

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|$$

③ 内直积

设 G 为群，$G_i \leqslant G(i = 1, 2, \cdots, n)$，若满足

a. $G_i \trianglelefteq G(i = 1, 2, \cdots, n)$；

b. $G = G_1 G_2 \cdots G_n$，即 G 中每个元素都可表为 $G_1, G_2, \cdots, G_n$ 中元素的

积；

c. $G_1G_2\cdots G_{i-1}\cap G_i=e(i=2,3,\cdots,n)$。

则称 G 是子群 $G_1,G_2,\cdots,G_n$ 的内直积。

(2) 外直积的性质

设 $A_1,A_2,\cdots,A_n$ 是 n 个群，

$$G=A_1\times A_2\times\cdots\times A_n$$

$$G_i=\{(e_1,\cdots,e_{i-1},a_i,e_{i+1},\cdots,e_n)\mid a_i\in A_i\}\quad(i=1,2,\cdots,n)$$

则 $G_i\leqslant G(i=1,2,\cdots,n)$ 且 $G_i(i=1,2,\cdots,n)$ 与 G 有如下关系：

① $G_i\trianglelefteq G(i=1,2,\cdots,n)$；

②$G=G_1G_2\cdots G_n$，即 G 中每个元素都可表为 $G_1,G_2,\cdots,G_n$ 中元素的积；

③$G_1G_2\cdots G_{i-1}\cap G_i=e(i=2,3,\cdots,n)$。

(3) 内直积的性质

设 G 为群，$G_i\leqslant G(i=1,2,\cdots,n)$，则 G 是这 n 个子群的内直积的充要条件是：

①$G=G_1G_2\cdots G_n$，且 G 中每个元素的表示法是惟一的；

②G_i 中任意元素同 $G_j(i\neq j)$ 中任意元素可换。

注 a. 由外直积的结论知外直积可导出内直积。另一方面，内直积也可导出外直积，因此，若对同构的群不加区分，则外直积与内直积就是一致的，一般情况下，均称为直积。

b. 在直积中，可在直积因子间添加括号或去掉括号，且直积因子也可任意交换次序。

2. 直积的应用

(1) 由直积定义的两个群

①(不) 可分解群

一个群若能够分解成其真子群的直积，则称这个群为可分解群；否则称为不可分解群。

② 完全可分解群

一个群若能够分解成其真子群且为单群的直积，则称为完全可分解群。

(2) 不可分解群的例子与判定

① 无限循环群及 n 次对称群、有理数加群都是不可分解群；

②n 阶循环群是不可分解群的充要条件是 n 为素数的方幂。

(3) 完全可分解群的性质

① 设 G 是完全可分解群，且 $N \trianglelefteq G$，则有 $H \trianglelefteq G$，使

$$G = N \times H$$

即完全可分解群的任何正规子群都是其直积因子。

注　该结论对非完全分解群不再成立，如三次对称群 S_3 只有一个非平凡正规子群

$$N = \{(1),(123),(132)\}$$

N 不是 S_3 的直积因子。

② 完全可分解群的正规子群及商群都是完全可分解群。

八 Sylow 定理

1. Sylow 定理

(1) 定义

①Sylow p- 子群

设 G 是有限群，且 $|G| = p^s m$，其中 p 是素数，s 是非负整数，$p \nmid m$，则称 G 的 p^s 阶子群为 G 的一个 Sylow p- 子群，也简称为 Sylow 子群。

② 重陪集

设 H,K 是群 G(未必有限) 的两个子群，$x \in G$，则称 G 的子集

$$HxK = \{hxk \mid h \in H, k \in K\}$$

为群 G 关于子群 H,K 的一个重陪集，并称 HxH 为关于 H 的一个重陪集。

(2) 重陪集的性质

① 设 HxK 与 HyK 是群 G 的任意两个重陪集，若

$$HxK \cap HyK \neq \varnothing$$

则必 $HxK = HyK$。

注　由这一性质可知，可将 G 分解成互不相交的若干个重陪集的并。这种分解称为群 G 关于子群 H,K 的重陪集分解。

② 在群 G 的重陪集 HxK 中：

a. 含子群 H 的右陪集的个数等于$(K : K \cap x^{-1}Hx)$；

b. 含子群 K 的左陪集的个数等于$(H : H \cap xKx^{-1})$。

(3) 三个 Sylow 定理

① 第一 Sylow 定理 —— 存在性和包含性

设 G 是有限群，且 $|G| = p^s m$，其中 p 是素数，s 是正整数，$p \nmid m$。则对 G 的每个 $p^i(i = 0, 1, \cdots, s-1)$ 阶子群 H，总存在 G 的 p^{i+1} 阶子群 K 使 $H \trianglelefteq K$。

② 第二 Sylow 定理 —— 共轭性(即相互关系)

设 G 是有限群，p 是素数，则 G 的所有 Sylow p- 子群恰好是群 G 的一个共轭子群类。

③ 第三 Sylow 定理 —— 计数定理

设 G 是有限群，且 $|G| = p^s m$，其中 p 是素数，$p \nmid m$。若 G 的 Sylow p- 子群共有 k 个，则 $k \mid |G|$，且

$$k \equiv 1 \pmod{p}$$

(4)Sylow 定理的应用

① 循环群的一个判定

设 G 是有限群，$|G| = pq$，其中 p, q 是互异的素数，且 $p \nmid (q-1)$，$q \nmid (p-1)$，则 G 是一个循环群。

② 有限群是其 Sylow 子群直积的判定

a. 设 G 是有限群，且 $|G| = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ 为标准分解式，则 G 是其 Sylow p_i- 子群 $P_i(i = 1, 2, \cdots, m)$ 的直积的充要条件是：$P_i \trianglelefteq G(i = 1, 2, \cdots, m)$。

b. 任何有限交换群都是其所有 Sylow 子群的直积(由此可将对有限交换群的讨论转化为对素幂交换群的讨论)。

③Lagrange 定理的逆定理(对有限交换群成立)

设 G 是有限交换群，如果 $d \mid |G|$，则 G 有 d 阶子群。

注 Sylow 定理还可用于确定一些群不是单群(参见本章 §8 第 7 题)。

2. p- 群的定义及性质

(1) 定义

若群 G 中每个元素的阶都有限，且都是素数 p 的方幂，则称 G 是一个 p- 群。

(2) 性质

有限群 G 是 p- 群 $\Leftrightarrow |G|$ 是 p 的方幂。

九、有限交换群

1. 有限交换群基本定理

任何阶大于 1 的有限交换群 G 都可以惟一地分解为素幂阶循环群（从而为不可分解群）的直积

$$G = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_n \rangle$$

其中 $\langle a_i \rangle$ 是 $p_i^{\alpha_i}$（p_i 为素数，$i = 1,2,\cdots,n$）阶循环群。

注 每个 $p_i^{\alpha_i}(i=1,2,\cdots,n)$ 称为群 G 的初等因子，$\{p_1^{\alpha_1},p_2^{\alpha_2},\cdots,p_n^{\alpha_n}\}$ 称为群 G 的初等因子组。

2. 有限交换群的不变因子定理

任何阶大于 1 的有限交换群 G 都可以惟一地分解为

$$G = \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \times \langle b_m \rangle$$

其中 $|b_i| > 1(i = 1,2,\cdots,m)$，且 $|b_i| \mid |b_{i+1}|\ (i = 1,2,\cdots,m-1)$。

注 每个 $|b_i|$ 称为群 G 的不变因子，$\{|b_1|,|b_2|,\cdots,|b_m|\}$ 称为 G 的不变因子组。

3. 有限交换群同构的判定

(1) 两个阶大于 1 的有限交换群同构当且仅当二者有相同的初等因子组。

(2) 两个阶大于 1 的有限交换群同构当且仅当二者有相同的不变因子组。

4. 初等交换群的定义

初等因子组为 $\{p,p,\cdots,p\}$（p 为素数）的有限交换群，称为初等交换群。

释疑解惑

一、对群同态与同构的理解

1. 群 G 与群 $\overline{G}$ 满同态，记作 $G \sim \overline{G}$，是指存在一个从 G 到 $\overline{G}$ 的满射 φ，且保持运算关系，即

$$\varphi(ab) = \varphi(a)\varphi(b) \quad (\forall a,b \in G)$$

此时 $\overline{G}$ 为 G 的同态象。

若 φ 仅是从 G 到 $\overline{G}$ 的一个同态映射(不是满射),不能使用"$G \sim \overline{G}$"的记号,此时 G 的同态象 $\varphi(G) \subset \overline{G}$,显见 $\varphi(G) \leqslant \overline{G}$。

2. 群 G 与群 $\overline{G}$ 同态(同构)及不是同态(同构)的证明

要证两个群 G 与 $\overline{G}$ 同态(同构),只需证明存在一个 G 到 $\overline{G}$ 的满射(双射)φ,使

$$\varphi(ab) = \varphi(a)\varphi(b) \quad (\forall a, b \in G)$$

这样的同态(同构)映射可能不止一个。

在建立这种映射时,必须使 G 的单位元 e 对应 $\overline{G}$ 的单位元 $\overline{e}$,互相对应的元素的逆元也互相对应。一般地,G 的特殊元素与 $\overline{G}$ 相应的特殊元素对应。

要证明群 G 与群 $\overline{G}$ 不是同态(同构)的,则需证明不存在 G 到 $\overline{G}$ 的满同态(同构)映射。为证明这一点,常采用反证法,即证明若有一个满同态(同构)映射存在,使 $G \sim \overline{G}(G \cong \overline{G})$,必可导出矛盾。为此,也常从特殊元素入手。

3. 群 G 与 $\overline{G}$ 同构,只是说二者代数性质完全相同,因而二者有相同的代数结构。但同构的群与相同的群是有区别的,例如整数加群 Z 与所有偶数作成的加群是同构的,而后者为前者的子群,即同构群不相同。实际上此例也说明一个群可以同自己的一个真子群同构。

4. 同态与同构的比较

(1) 若群 $G \sim \overline{G}$,则群 G 的代数性质完全传递给它的同态象,但反之未必。

若群 $G \cong \overline{G}$,则群 G 与 $\overline{G}$ 的代数性质完全相同。

(2) 同构映射必须是单射,而同态映射不一定是单射(可多对一)。

(3) 群的同态象不能像群的同构象那样完全刻画群,但由于同态象有时与原群相比可能具有某些特殊性及某种便利,讨论可能比研究原群更容易些,而从一个群的同态象的代数性质又常可部分地推测原群的性质,因此,研究群的同态比研究群的同构更灵活,运用也更广泛。

5. 一个反例

G 与 $\overline{G}$ 是各有代数运算的集合且 $G \sim \overline{G}$,若 G 为群,则 $\overline{G}$ 为群,反之不真。即若 $G \sim \overline{G}$,$\overline{G}$ 为群,未必有 G 为群。如 $G = \{$所有正负奇数$\}$,代数运算

为普通乘法；$\overline{G}=\{1,-1\}$，代数运算也为普通乘法，定义

$$\varphi:\begin{array}{l}正奇数\longrightarrow 1\\ 负奇数\longrightarrow -1\end{array}$$

则 φ 为 G 到 $\overline{G}$ 的同态满射，即 $G\sim\overline{G}$。又 $\overline{G}$ 对普通乘法作成群，但 G 不是群。

二、对正规子群的理解

1. 概念的理解

正规子群是一种特殊的子群，其特殊性在于它的每一左陪集和相应的右陪集相等。定义中的 $aN=Na$ 的 a 是对群 G 中任意元素来说的，而不是对某些 a 来说的。

另外 $aN=Na$ 是指用 a 左乘子群 N 所得的子集与用 a 右乘子群 N 所得的子集是相等的。这并不是说 a 可同 N 中的每一元素可交换。

2. 正规子群的不可传递性，即正规子群的正规子群未必是原群的正规子群，这同子群不同。反例参见本章 §2 例 3。

3. 关于正规子群的等价条件

设 G 为群，$N\leqslant G$，则下列四个条件等价：

①$N\lhd G$；

②$aN=Na(\forall a\in G)$；

③$aNa^{-1}\subseteq N(\forall a\in G)$；

④$ana^{-1}\in N(\forall a\in G,\forall n\in N)$。

一般地，要验证 $N\lhd G$，用 ④ 较为方便。

4. 正规子群和商群是紧密联系的两个概念，正规子群 N 的特殊性导致了它的商群 G/N 的特殊性，即可自然地规定某运算，使商集 G/N 作成一个群，其关键就是所规定运算的合理性。在第二章指出若 N 仅是 G 的子群，则 $aN\cdot bN$ 未必是一个左陪集（参见第二章释疑解惑七），但 N 为 G 的正规子群时则有

$$aN\cdot bN=abN\quad(\forall a,b\in G)$$

且这个条件也是充分的（参见本章 §9 第 7 题）。因此，在商集 G/N 中可自然地规定一种运算并使之作成群。

三、对满同态核及正规子群的认识

G 到 $\overline{G}$ 满同态 φ 的核 $\mathrm{Ker}\varphi$ 是指

$$\mathrm{Ker}\varphi = \{a \mid \varphi(a) = \bar{e}, a \in G, \bar{e} \in \overline{G}\}$$

其中 $\bar{e}$ 为 $\overline{G}$ 的单位元。实际上它是群 G 的正规子群，证明如下：

先证 $K = \mathrm{Ker}\varphi$ 为 G 的子群。$\forall a, b \in K$，由 $\varphi(a) = \bar{e}, \varphi(b) = \bar{e}$ 可知

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

故 $ab^{-1} \in K$，即 $K \leqslant G$。

再证 $K \trianglelefteq G$。$\forall k \in K, a \in G$，在 φ 之下有

$$\varphi(aka^{-1}) = \varphi(a)\varphi(k)\varphi(a^{-1}) = \varphi(a)\bar{e}\varphi(a)^{-1} = \bar{e}$$

因此 $aka^{-1} \in K$，所以 $K \trianglelefteq G$。

要证明 G 的一个子集 K 是满同态 φ 的核时，一般需证明 $K \subseteq \mathrm{Ker}\varphi$ 且 $\mathrm{Ker}\varphi \subseteq K$，即需证明 $\forall k \in K$，有 $\varphi(k) = \bar{e}$，即 $k \in \mathrm{Ker}\varphi, K \subseteq \mathrm{Ker}\varphi$；反之，$\forall k \in \mathrm{Ker}\varphi$，即 $\varphi(k) = \bar{e}$，只需证 $k \in K$，$\mathrm{Ker}\varphi \subseteq K$。

由本章 §3 第 1 题知，$\forall a, b \in G, \varphi(a) = \varphi(b) \Leftrightarrow a$ 与 b 在 K 的同一陪集中(其中 φ 为从 G 到 $\overline{G}$ 的同态映射，$K = \mathrm{Ker}\varphi$)，即把 G 的元以 K 为分类标准后，G 中同类元映成 $\overline{G}$ 中同类元。核 K 越大，分类越粗，映的象元越少，即 G 的这一同态象比较“粗糙”。核越小，分类越细，映的象元越多，即这一同态象比较精细。同态核 K 的大小完全刻画了同态映射 φ 的精细过程。由下面的典型题精讲第 1 题可知 $K = \{e\}$ 时，$G \cong \overline{G}$，即 G 与 $\overline{G}$ 完全等同；$K = G$ 时，则 $\overline{G} = \{\bar{e}\}$，即整个 G 映成了一个元。

在本章 §3 定理 1 中，G 与 G/N 同态的核就是 N，即 G 的任一正规子群必为 G 的某个满同态的核(这一映射从证明可知就是 G 到 G/N 的自然同态)。这是因为：N 是 G/N 的单位元，$\forall n \in N$，有 $\tau(n) = nN = N$，即 $N \subseteq \mathrm{Ker}\tau$。反之，$\forall x \in \mathrm{Ker}\tau$，即 $\tau(x) = xN = N$，故 $x \in N$，即 $\mathrm{Ker}\tau \subseteq N$。因此 $N = \mathrm{Ker}\tau$。又由前面指出同态映射的核为 G 的正规子群，从而有：G 的正规子群且只有正规子群，才能是 G 的满同态的核。这进一步指出了正规子群与一般子群不同的特征。

由于 G 的正规子群 N 完全确定商群 G/N，因此完全确定 G 的同态象(本章 §3 定理 2)。所以作为同态核的正规子群在群构造的研究中具有重

要地位。

四、三个群 $G,\overline{G},G/N$ 的关系

其中 $G \overset{\varphi}{\sim} \overline{G}, N = \mathrm{Ker}\varphi$，由

(1)$G \overset{\varphi}{\sim} \overline{G}, N = \mathrm{Ker}\varphi \trianglelefteq G$(参见本章释疑解惑三)。

(2)$G \overset{\sigma}{\sim} G/N$，$\sigma$ 为自然同态(参见本章 §3 定理 1)。

(3)$G/N \overset{\tau}{\cong} \overline{G}$(参见本章 §3 定理 2)

可知任 $a \in G$

$$\varphi: a \xrightarrow{\sigma} aN \xrightarrow{\tau} \overline{a} = \varphi(a)$$

因此 $\varphi = \tau\sigma$。

三者的这种关系说明群 G 的任一商群都是 G 的同态象，在同构的意义下 G 的任一同态象也只能是它的商群。因此，G 的同态象只需从它的商群中找，又 G 的商群完全由 G 和 G 的正规子群 N 所决定，所以，掌握了 G 的所有正规子群就掌握了 G 的所有商群，进而掌握了 G 的所有同态象。但应当注意，虽然正规子群和同态映射是一一对应的，但正规子群和 G 的同态象(不同构)之间可能不是一一对应的。可能由群 G 的几个不同的正规子群得到同一商群，但正规子群能够决定群 G 的所有同态象。

五、对有限群相关阶的讨论

若群 G 的阶为 n，则其任一同态象的阶必为 n 的约数。这是因为其同态象的阶等于某一商群 G/N 的阶，而 $|G/N|$ 为 N 在 G 中的指数，进而由 Lagrange 定理知 $|G/N|$ 为 $|G|$ 的约数。

由此可知 4 阶群不会和 3 阶群同态，7 阶群只能同 7 阶群或单位元群同态。

六、正规子群、特征子群与全特征子群的关系

三者之间的关系是：

$$\text{全特征子群} \subset \text{特征子群} \subset \text{正规子群}$$

1. 是正规子群但不是特征子群的例子

Klein 四元群

$$K_4 = \{(1),(12)(34),(13)(24),(14)(23)\}$$

中的子群

$$N = \{(1),(12)(34)\} \trianglelefteq K_4$$

且

$$\begin{aligned} \sigma:(1) &\longrightarrow (1) \\ (12)(34) &\longrightarrow (13)(24) \\ (13)(24) &\longrightarrow (12)(34) \\ (14)(23) &\longrightarrow (14)(23) \end{aligned}$$

是 K_4 的一个自同构，但

$$\sigma(N) = \{(1),(13)(24)\} \not\subseteq N$$

故 N 不是特征子群。

2. 是特征子群但不是全特征子群的例子

如 Q 上的 2 阶线性群 $G = GL_2(Q)$ 的中心（Q 上的全体 2 阶纯量矩阵）是 $GL_2(Q)$ 的特征子群，但不是全特征子群（参见本章 §5 例 2、例 3）。

一般地，正规子群不具有传递性，但在特殊情况下具有这一特性，即

若 $K \trianglelefteq H \trianglelefteq G$，$|K| = n$，$(H:K) = m$，若 $(n,m) = 1$，则必有

$$K \trianglelefteq G$$

证明如下：

$\forall k \in K, g \in G$，由 $H \trianglelefteq G$ 知 $g^{-1}kgK$ 为 m 阶群 H/K 的某一元素，设其阶为 x，则 $x \mid m$。

又由 $|K| = n$ 知 $k^n = e$，故

$$((g^{-1}kg)K)^n = (g^{-1}kg)^n K = g^{-1}k^n gK = K$$

K 为 H/K 中的单位元，从而 $x \mid n$，因此由 $(m,n) = 1$ 知 $x = 1$，于是

$$g^{-1}kgK = K, g^{-1}kg \in K$$

故 $K \trianglelefteq G$。

另外，在完全分解群中，子群的正规性也具有传递性，即若 G 为完全分解群，且 $K \trianglelefteq H \trianglelefteq G$，则 $K \trianglelefteq G$。

事实上，可令

$$G = H \times H'$$
$$H = K \times K'$$

则有 $G = KxK'xH'$，从而 $K \trianglelefteq G$。

七、关于元素共轭的一个说明

两个元素是否共轭，按定义可知同此两元素所在的群的范围有关，即若 $a,b \in H \leqslant G$，且 a,b 在 H 中共轭，则必在 G 中共轭，但若在 G 中共轭，未必在 H 中共轭。

八、本章 §2 定理 5，§6 定理 3，§8 定理 1 的比较

这三个定理均涉及到 pm 阶群(p 为素数)，群 G 必有 p 阶子群，三者的关系是

§2 定理 5(pm 阶交换群必有 p 阶子群)

$\Rightarrow$ §6 定理 3(pm 阶群必有 p 阶子群)

$\Rightarrow$ §8 定理 1(p^{sm} 阶群必有 $p^i(i = 0,1\cdots,s)$ 阶子群)。

其中 §2 定理 5 中要求 G 为交换群，§6 定理 3 中 G 是一般性的群，在其证明中用到了 §2 定理 5，§8 定理 1 的证明中用到了 §6 定理 3。

九、直积的意义

群的直积在群论研究中占有重要地位：提供了由已知群构造新群的方法；把研究群 G 的结构转化为其若干子群的结构(可把一个群 G 分解成一些(正规) 子群的直积，那么群 G 的结构决定于每个直积因子的结构。只要将每个直积因子研究清楚，则群 G 就会很清楚)。

十、p- 群的一些主要性质

除教材中给出的有限群 G 是 p- 群 $\Leftrightarrow |G|$ 是 p 的方幂这一性质外，p-群还具有其他一些重要性质。

(1) 阶大于 1 的有限 p- 群必包含 $\{e\}$。

(2) p^2 阶群必为交换群。

(3) 若有限 p- 群 G 仅有一个指数为 p 的子群，则 G 必为循环群。

(4) p^n 阶群对每个 $i(i = 1,2,\cdots,n-1)$ 都至少有一个 p^i 阶正规子群。

十一、有限交换群与 λ- 矩阵的比较

有限交换群与高等代数中的 λ- 矩阵类似。有限交换群中的不变因子、不变因子分解式、初等因子、同构及同构的充要条件，分别与 λ- 矩阵中的不变因子、标准形、初等因子、等价及等价的充要条件相对应。关于有限交换群的结构及相关结论，可对应于 λ- 矩阵的相应结果来理解。

典型题精讲

1. 设 φ 是群 G 到群 $\overline{G}$ 的满同态。证明：φ 是群 G 到群 $\overline{G}$ 的同构映射的充要条件是其核 $\varphi^{-1}(\bar{e})=\{e\}$。其中 $e,\bar{e}$ 分别是群 G 和群 $\overline{G}$ 的单位元。

证明　依题设，φ 是群 G 到群 $\overline{G}$ 的满同态映射，因此

$$\varphi \text{ 是群 } G \text{ 到群 } \overline{G} \text{ 的同构映射} \Leftrightarrow \varphi \text{ 为单射}$$

"$\Leftarrow$"　设 φ 为单射，即若 $\varphi(a)=\varphi(b)$ 则必有 $a=b$。$\forall x\in\varphi^{-1}(\bar{e})$，则

$$\varphi(x)=\bar{e}=\varphi(e)$$

故 $x=e$，即 $\varphi^{-1}(\bar{e})=\{e\}$。

"$\Rightarrow$"　设 $\varphi^{-1}(\bar{e})=\{e\}$，$\forall a,b\in G$，若 $\varphi(a)=\varphi(b)$，则

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

故 $ab^{-1}\in\varphi^{-1}(\bar{e})=\{e\}$，即 $ab^{-1}=e$，从而 $a=b$，φ 为单射。

---

2. 设 G 与 $\overline{G}$ 是两个有限循环群，它们的阶分别是 m 和 n。证明：G 与 $\overline{G}$ 同态 $\Leftrightarrow n\mid m$。

证明　"$\Rightarrow$"　设 G 与 $\overline{G}$ 同态，则由第三章 §3 定理2(群同态基本定理)知

$$G/N\cong\overline{G}$$

其中 N 为 G 到 $\overline{G}$ 的同态满射的核，且 $N\trianglelefteq G$，故 $|G/N|=|\overline{G}|=n$，但 $|G/N|=(G:N)$，故由 Lagrange 定理知，它能整除 $|G|$，即 $n\mid m$。

"$\Leftarrow$"　若 $n\mid m$，不妨设 $G=\langle a\rangle$，$\overline{G}=\langle\bar{a}\rangle$，定义

$$\varphi: a^k\longrightarrow\bar{a}^k$$

若 $a^h = a^k$，则 $m \mid (h-k)$，从而由 $n \mid m$ 得 $n \mid (h-k)$，故 $\overline{a}^h = \overline{a}^k$。故 φ 为 G 到 $\overline{G}$ 的映射，又易于验证 φ 是 G 到 $\overline{G}$ 的一个同态满射，因此 G 与 $\overline{G}$ 同态。

---

3. 设群 $N \trianglelefteq G$，且 $|N| = 2$，证明：$N \subseteq C(G)$，其中 $C(G)$ 为群 G 的中心。

证明 由于 $|N| = 2$，不妨设 $N = \{e, n\}$，其中 e 为 G 的单位元。$\forall a \in G$，由于 $N \trianglelefteq G$，故 $aN = Na$，即

$$\{a, an\} = \{a, na\}$$

故 $an = na$，因此，N 的两个元 e 与 n 均可同 G 中的任意元素 a 可换，所以

$$N \subseteq C(G)$$

---

4. 设 G 为有限交换群，$|G| = n$，p 为素数且 $p \mid n$。证明：G 中存在阶为 p 的元素。

证明 用数学归纳法证明。

$n = 2$ 时，结论显然成立。

设 $m < n$ 时结论成立，下证 $m = n$ 时结论也成立。

$\forall a \in G, a \neq e$，设 $|a| = k$，则由 Lagrange 定理知，$k \mid n$。

若 $p \mid k$，则元素 $b = a^{\frac{k}{p}}$ 的阶为 p，故结论成立。

若 $p \nmid k$，则由 G 为交换群知 $\langle a \rangle$ 为 G 的正规子群。$\overline{G} = G/\langle a \rangle$ 为交换群，$\overline{G}$ 的阶数 $m < n$ 且 $m \mid n$。设 $n = mk$，又由 $p \mid n$，设 $n = ps$，故 $mk = n = ps$，$p \mid mk$，而 $p \nmid k$，故必有 $p \mid m$。由归纳假设，$\overline{G}$ 中存在阶为 p 的元 $\overline{c}$，由 $\overline{c}^p = \overline{c^p} = \overline{e}$（$\overline{e}$ 为 $\overline{G}$ 的单位元）可知 $c^p \in \langle a \rangle$。又 $\langle a \rangle$ 为 k 阶循环群，故 $(c^p)^k = e$，即 $(c^k)^p = e$。又 p 为素数，故 c^k 的阶或为 p 或为 1。若 $c^k = e$，有 $\overline{c^k} = \overline{e}$，即 $\overline{c}^k = \overline{e}$，而 $\overline{c}$ 的阶为 p，故有 $p \mid k$，这与 $p \nmid k$ 矛盾，从而 c^k 的阶为 p，即命题对任意 n 均成立。

---

5. 设 φ 是群 G 到群 $\overline{G}$ 的一个满同态。证明：G 的中心 $C(G)$ 中的元素在 φ 之下的象是 $\overline{G}$ 的中心 $C(\overline{G})$ 中的元素。

证明 $\forall a \in C(G)$，$\varphi(a) = \overline{a} \in \overline{G}$，下面证明 $\overline{a} \in C(\overline{G})$。

$\forall \overline{x} \in \overline{G}$，由于 φ 为满射，故存在 $x \in G$，使 $\varphi(x) = \overline{x}$。又 $a \in C(G)$，

故有 $ax = xa$。又 φ 是 G 到 $\overline{G}$ 的同态映射，故

$$\overline{a}\,\overline{x} = \varphi(a)\varphi(x) = \varphi(ax) = \varphi(xa) = \varphi(x)\varphi(a) = \overline{x}\,\overline{a}$$

于是 $$\overline{a} \in C(\overline{G})$$

---

6. 证明：群 G 为交换群 $\Leftrightarrow \varphi: a \longrightarrow a^{-1}$ 是群 G 的自同构。

证明 "$\Rightarrow$" 设群 G 为交换群。$\forall a \in G$，有 $a^{-1} \in G$，使

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

故 φ 为满射。

又若 $\forall a, b \in G, a \neq b$，则 $a^{-1} \neq b^{-1}$，即 $\varphi(a) \neq \varphi(b)$，故 φ 为单射。

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

故 φ 是群 G 的自同构映射。

"$\Leftarrow$" 设 φ 是群 G 的自同构映射。$\forall a, b \in G$，有 $a^{-1}, b^{-1} \in G$，使

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

又 $$\varphi(a^{-1}b^{-1}) = \varphi((ba)^{-1}) = ba$$

故 $ab = ba$，所以群 G 为可换群。

---

7. 证明：单群的同态象是单群或单位元群。

证明 设 G 是单群，$\overline{G}$ 是 G 的同态象，N 是同态核，则 $N \trianglelefteq G$。又 G 为单群，故 N 为 G 或单位元群。

若 $N = G$，则 $\{e\} = G/G \cong \overline{G}$，故 $\overline{G}$ 为单位元群。

若 $N = \{e\}$，则 $G = G/\{e\} \cong \overline{G}$，故 $\overline{G}$ 为单群。

---

8. 设群 H 是群 G 的子群，$N \trianglelefteq G$。证明 G/N 的任一子群均具有 H/N 的形式。

证明 设 $\overline{H}$ 为 G/N 的任一子群，φ 为 G 到 G/N 的自然同态，则其核为 N。则

$$H = \varphi^{-1}(\overline{H}) \leqslant G \text{ 且 } H \supseteq N$$

显见 N 也是 H 的正规子群，且 $\overline{H} = \varphi(H) = \{aN \mid a \in H\} = H/N$。即 G/N 的任一子群均具有 H/N 的形式。

9. 设 G 为群，$H \trianglelefteq G$，且 $(G : H) = m$，$|H| = n$，$(m,n) = 1$，证明：H 是 G 的惟一一个 n 阶子群。

证明　设 N 是 G 的一个 n 阶子群，下面证明 $H = N$。考虑商群 HN/H，因 $H \trianglelefteq G$，HN 是 G 中包含 H 的子群，故 HN/H 有意义。若能证明 $|HN/H| = 1$，则 $HN = H$，即 $N \subseteq H$，而 $|N| = |H|$，所以 $H = N$。

记 $|HN/H| = l$，由于 HN/H 是 G/H 的子群，而

$$|G/H| = (G : H) = m$$

故 $l \mid m$，又由第三章 §4 定理 2 知

$$HN/H \cong N/(H \cap N)$$

即

$$|N/(H \cap N)| = |HN/H| = l$$

但

$$\begin{aligned} n = |N| &= (N : (H \cap N)) \cdot |H \cap N| \\ &= |N/(H \cap N)| \cdot |H \cap N| \\ &= l \cdot |H \cap N| \end{aligned}$$

故 $l \mid n$，由于 $(m,n) = 1$，所以有 $l = 1$。

综上可知有 $H = N$，即 H 是 G 的惟一一个 n 阶子群。

---

10. 设群 G 的阶为 n，$p \mid n$，p 为素数。若方程 $x^p = e$ 在 G 内恰有 p 个解，则由这 p 个解组成的集合 H 必为 G 的正规子群。

证明　因 p 为素数，故方程 $x^p = e$ 在 G 中的任一非单位元解 a 必为 p 阶元。易知

$$H = \{e, a, a^2, \cdots, a^{p-1}\} = \langle a \rangle \leqslant G$$

又 $\forall g \in G$，由

$$(gag^{-1})^p = e$$

知 $gag^{-1} \in H$，因此 $H \trianglelefteq G$。

---

11. 设 C_n 表示 n 阶循环群，试证明 $C_3 \times C_5 \cong C_{15}$。

证明 由

$$|C_3 \times C_5| = |C_3| \cdot |C_5| = 3 \cdot 5 = 15$$

可知，要证 $C_3 \times C_5 \cong C_{15}$，据第2章 §4定理3可知，只需证明 $C_3 \times C_{15}$ 为一个15阶循环群，再据第2章 §4定理1，即需证 $C_3 \times C_5$ 中含有一个15阶的元素。

不妨设

$$C_3 = \langle a \rangle, C_5 = \langle b \rangle$$

则 $|a| = 3$，$|b| = 5$，考虑元素 $(a,b) \in C_3 \times C_5$，有

$$(a,b)^{15} = (a^{15}, b^{15}) = (e_1, e_2)$$

其中 e_1, e_2 分别为 C_3 与 C_5 的单位元。

另一方面，若 $|(a,b)| = n$，则

$$(a,b)^n = (a^n, b^n) = (e_1, e_2)$$

即有 $a^n = e_1, b^n = e_2$，故 $3 \mid n, 5 \mid n$，从而 $15 \mid n$，所以 $|(a,b)| = 15$，故

$$C_3 \times C_5 \cong C_{15}$$

注 这一结果可推广到一般的情况，即若 $(m,n) = 1$，则

$$C_m \times C_n \cong C_{mn}$$

---

12. 证明36阶群不是单群。

证明 设群 G 的阶为36。$36 = 2^2 \cdot 3^2$，若 G 的Sylow-3子群的个数大于1，则任取 G 的两个互异的9阶子群 H_1、H_2，由

$$|H_1 \cap H_2| < 9$$

$$|H_1 \cdot H_2| < 36$$

$$|H_1 H_2| \cdot |H_1 \cap H_2| = |H_1| \cdot |H_2|$$

知 $|H_1 \cap H_2| \neq 1$、9，故 $H = H_1 \cap H_2$ 必为3阶子群。考虑 H 在 G 中的正规化子 $N(H)$，由 H_1 与 H_2 均为交换群知

$$|N| = |N(H)| \geqslant 2 \cdot 6 + 3 = 15$$

因此 $|N| = 18$ 或 36，若 $|N| = 18$，则 $N \trianglelefteq G$；若 $|N| = 36$，则 $N = G, H \trianglelefteq G$，所以 G 不是单群。

习题全解

§1　群同态与同构的简单性质(P86)

1. 设 H 是群 G 的一个子群，$a \in G$。证明：

$$aHa^{-1} \leqslant G，且\ H \cong aHa^{-1}$$

证明　任意 $ah_1a^{-1}, ah_2a^{-1} \in aHa^{-1}$，其中 $h_1, h_2 \in H$，因为 $H \leqslant G$，从而

$$(ah_1a^{-1})(ah_2a^{-1}) = a(h_1h_2)a^{-1} \in aHa^{-1}$$

故

$$aHa^{-1} \leqslant G$$

$\forall h \in H$，定义映射 $\varphi: h \longrightarrow aha^{-1}$，则 $\forall h_1, h_2 \in H$，有

$$\varphi(h_1h_2) = a(h_1h_2)a^{-1} = (ah_1a^{-1})(ah_2a^{-1}) = \varphi(h_1)\varphi(h_2)$$

故 φ 为 H 到 aHa^{-1} 的同态映射，又显见 φ 为双射，故

$$H \cong aHa^{-1}$$

---

2. 在群的同态映射下，一个元素与其象的阶是否一定相等？在同构映射下如何？

解　在同态映射下，一个元素与其象的阶未必相等。例如，令

$$D(x_1, \cdots, x_n) = \prod_{i<j}(x_i - x_j)$$

则对于 $\sigma \in S_n$，有

$$\begin{aligned}\sigma D(x_1, \cdots, x_n) &= D(x_{\sigma_{(1)}}, \cdots, x_{\sigma_{(n)}}) \\ &= \prod_{i<j}(x_{\sigma_{(i)}} - x_{\sigma_{(j)}}) = \pm D(x_1, \cdots, x_n)\end{aligned}$$

定义

$$\sigma D(x_1, \cdots, x_n) = \mathrm{sgn}(\sigma) D(x_1, \cdots, x_n)$$

sgn 就是由 S_n 到乘法群 $G = \{1, -1\}$ 的一个映射。显见 sgn 是 S_n 到 G 的一个同态，G 中的元 1 是 1 阶的，元 -1 是 2 阶的。若取 $n = 4$，由第二章 §7 习题 22 证明可知 S_4 中存在 8 个 3 阶元，因此 S_4 中元素与其象的阶未必相等。又如取 S 为非零有理数乘群，G 仍为上述的乘法群，$\forall x \in S$，定义

$$\sigma_1(x) = 1$$

$$\sigma_2(x) = \begin{cases} 1, & x \text{为正有理数} \\ -1, & x \text{为负有理数} \end{cases}$$

则 σ_1 与 σ_2 均为 S 到 G 的映射，且 σ_2 为满射，而 σ_1 与 σ_2 显见是 S 到 G 的一个同态，S 中元素除 1 的阶为 1，-1 的阶为 2 外，其余均为无穷，因此，S 与 G 中元素的阶未必相等。

但如果两个群 S 与 G 是同构的，设同构映射为 φ，任意 $x \in S$，若 $|x| = m$，即 $x^m = e$，则 $\varphi(x^m) = \bar{e} = \varphi^m(x)$，即 $|\varphi(x)| = m = |x|$；反之，若 $|\varphi(x)| = m$，亦有 $|x| = m$，因此 S 中任何元素与其象的阶都相同。

---

3. 问：$\varphi(\boldsymbol{A}) = \boldsymbol{A}^T$（$\boldsymbol{A}$ 的转置方阵）是否为一般线性群 $GL_n(F)$ 的自同构？又 $\sigma(\boldsymbol{A}) = (\boldsymbol{A}^{-1})^T$ 呢？

解 由 $(\boldsymbol{A}^T)^T = \boldsymbol{A}$ 可知 φ 是一般线性群的双射变换，但由转置的性质可知

$$(\boldsymbol{AB})^T = \boldsymbol{B}^T\boldsymbol{A}^T \neq \boldsymbol{A}^T\boldsymbol{B}^T$$

故 $\varphi(\boldsymbol{AB}) \neq \varphi(\boldsymbol{A}) \cdot \varphi(\boldsymbol{B})$。因此 φ 不是群 $GL_n(F)$ 的自同构。

由 $\boldsymbol{A}$ 与 $\boldsymbol{A}^{-1}$ 是互逆矩阵，$\boldsymbol{A}^{-1}$ 与 $(\boldsymbol{A}^{-1})^T$ 是互为转置矩阵，故 $\sigma(\boldsymbol{A}) = (\boldsymbol{A}^{-1})^T$ 是 $GL_n(F)$ 的双射变换。又 $\forall \boldsymbol{A}, \boldsymbol{B} \in GL_n(F)$

$$\sigma(\boldsymbol{AB}) = [(\boldsymbol{AB})^{-1}]^T = (\boldsymbol{B}^{-1}\boldsymbol{A}^{-1})^T = (\boldsymbol{A}^{-1})^T \cdot (\boldsymbol{B}^{-1})^T = \sigma(\boldsymbol{A}) \cdot \sigma(\boldsymbol{B})$$

所以 σ 是群 $GL_n(F)$ 的自同构。

---

4. 先证明本节例 3 中 6 阶群 G 的元素 $ba = ab^2$，再各给出 G 与 S_3 的乘法表，并由此指出 φ 是群 G 到三次对称群 S_3 的同构映射。

证明 由例 3 可知非循环群

$$G = \{e, a, b, b^2, ab, ab^2\}$$

其中 $|a| = 2$，$|b| = 3$。从而如果 $ba = ab$，则有 $|ab| = 6$，故 G 为 6 阶循环群，与 G 不是循环群矛盾。又显见 ba 不等于 e, a, b, b^2，故只有 $ba = ab^2$。又由于

$$\begin{aligned} b^2a &= b(ba) = b(ab^2) = (ba)b^2 = ab^4 \\ &= a(b^3)b = ab \end{aligned}$$

$$(ab)a = a(ba) = aab^2 = a^2b^2 = b^2$$

$$(ab^2)a = a^2b^4 = b$$

$$b^2(ab) = b(ab^2)b = ab^5 = ab^2$$

$$(ab)(ab) = a(ab^2)b = a^2b^3 = e$$

$$(ab^2)(ab) = a^2b^5 = b^2$$

$$b^2(ab^2) = ab^6 = a$$

$$(ab)(ab^2) = a^2b^4 = b$$

$$(ab^2)(ab^2) = a^2b^6 = e$$

因此得 G 的乘法表如下：

$\cdot$	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab^2	b^2	e	a	ab
b^2	b^2	ab	e	b	ab^2	a
ab	ab	b^2	ab^2	a	e	b
ab^2	ab^2	b	a	ab	b^2	e

参见第一章 §3 第 4 题可知 S_3 的乘法表如下：

$\cdot$	(1)	(12)	(123)	(132)	(23)	(13)
(1)	(1)	(12)	(123)	(132)	(23)	(13)
(12)	(12)	(1)	(23)	(13)	(123)	(132)
(123)	(123)	(13)	(132)	(1)	(12)	(23)
(132)	(132)	(23)	(1)	(123)	(13)	(12)
(23)	(23)	(132)	(13)	(12)	(1)	(123)
(13)	(13)	(123)	(12)	(23)	(132)	(1)

由 G 与 S_3 的乘法表即可知

$$\varphi: e \longrightarrow (1), a \longrightarrow (12), b \longrightarrow (123)$$
$$b^2 \longrightarrow (132), ab \longrightarrow (23), ab^2 \longrightarrow (13)$$

为 G 到 S_3 的同构映射。

---

5. 证明：4 阶群 G 若不是循环群则必与 Klein 四元群同构。

证明　因为 4 阶群 G 不是循环群，故 G 没有 4 阶元，从而由 Lagrange 定理知，G 中除单位元外，其余三个元的阶均为 2，由此可设

$$G = \{e, a, b, c\}$$

其中 $|a| = |b| = |c| = 2$，定义

$$\varphi: e \longrightarrow (1), a \longrightarrow (12)$$

$$b \longrightarrow (34),c \longrightarrow (12)(34)$$

则 φ 是 G 到 Klein 四元群 $K_4=\{(1),(12),(34),(12)(34)\}$ 的同构映射，所以

$$G \cong K_4$$

---

6. 设 G 是正有理数乘群，$\overline{G}$ 为整数加群。证明：

$$\varphi: 2^n \frac{b}{a} \longrightarrow n$$

是 G 到 $\overline{G}$ 的一个同态满射，其中 a 与 b 是互素的正奇数，n 是整数。

证明 设 a 与 b 及 c 与 d 分别是互素的正奇数，则存在互素的正奇数 h,k，

$$\frac{bd}{ac}=\frac{k}{h}$$

从而

$$\varphi\left(2^n \frac{b}{a}\cdot 2^m \frac{d}{c}\right)=\varphi\left(2^{n+m}\frac{bd}{ac}\right)=\varphi\left(2^{n+m}\frac{k}{h}\right)=n+m$$

$$=\varphi\left(2^n \frac{b}{a}\right)\cdot\varphi\left(2^m \frac{d}{c}\right)$$

故 φ 是 G 到 $\overline{G}$ 的一个同态映射，又显见 φ 是 G 到 $\overline{G}$ 的满射，所以是 G 到 $\overline{G}$ 的一个同态满射。

§ 2 正规子群和商群(P95)

1. 证明：群 G 的任意个正规子群的交还是 G 的一个正规子群。

证明 只需证明 G 的任两个正规子群的交还是正规子群。

设 $N_1 \trianglelefteq G_1$，$N_2 \trianglelefteq G$，则由第二章 §3 第 1 题知 $N_1 \cap N_2 \leqslant G$。$\forall a \in G$，$\forall x \in N_1 \cap N_2$，则 $x \in N_1$ 且 $x \in N_2$，但 $N_1 \trianglelefteq G$，$N_2 \trianglelefteq G$，故 $axa^{-1} \in N_1$，$axa^{-1} \in N_2$，所以

$$axa^{-1} \in N_1 \cap N_2$$

由本节定理 1 可知 $N_1 \cap N_2 \trianglelefteq G$。从而群 G 的任意个正规子群的交还是 G 的一个正规子群。

---

2. 指数是 2 的子群必是正规子群。

证明 设群 N 是群 G 的一个子群，且 $(G:N)=2$。

若 $x \in N$，则显见有 $xN = Nx$。

设 $b \in G, b \notin N$，由于 $(G:N) = 2$，故 G 被分成两个左陪集 N 和 bN，G 也被分成两个右陪集 N 与 Nb，因此 $bN = Nb$，从而对任意 $a \in G$，均有 $aN = Na$，故 $N \trianglelefteq G$。

3. 证明：若群 G 的 n 阶子群有且只有一个，则此子群必为 G 的正规子群。

证明 设群 H 是群 G 的 n 阶子群，则 $\forall a \in G$，由 §1 第 1 题可知 aHa^{-1} 也是 G 的一个 n 阶子群。由于 G 的 n 阶子群是惟一的，故 $aHa^{-1} = H \subseteq H$，所以 H 为 G 的正规子群。

4. 设 $H \trianglelefteq G$，且 $(G:H) = m$。证明：对群 G 中任意元素 a 有 $a^m \in H$。

证明 由 $(G:H) = m$ 可知商群 G/H 是一个 m 阶群，商群 G/H 的单位元 $\bar{e} = H$，又对任意 $a \in G, aH \in G/H$，故 $(aH)^m = \bar{e} = H$，又因为 $H \trianglelefteq G$，所以

$$(aH)^m = a^m H$$

因此
$$a^m H = H$$

故
$$a^m \in H$$

5. 设 H, K 是群 G 的两个正规子群，且二者的交为 $\{e\}$。证明：H 与 K 中的元素相乘时可换。

证明 由于 $H \trianglelefteq G$，故 $\forall a \in H, \forall b \in K \subseteq G$，有 $bab^{-1} \in H$，又 $(bab^{-1})^{-1} = ba^{-1}b^{-1}$，故 $ba^{-1}b^{-1} \in H$，从而 $aba^{-1}b^{-1} \in H$。

又由于 $K \trianglelefteq G$，则对上述的 a 与 b，有

$$aba^{-1} \in K$$

又 $b^{-1} \in K$，故有 $aba^{-1}b^{-1} \in K$，从而

$$aba^{-1}b^{-1} \in H \cap K$$

又由题设 $H \cap K = \{e\}$，从而

$$aba^{-1}b^{-1} = e, ab = ba$$

即 H 与 K 中的元素相乘时可换。

6. 设 H 是包含在群 G 的中心内的一个子群。证明：当 G/H 是循环群时，G 是交换群。

证明 由第二章 §3 中心的定义可知 $H \trianglelefteq G$。

若 G/H 是循环群，设 aH 为 G/H 的生成元，即 $G/H = \langle aH \rangle$，则 G 中任意两个元 x, y 必有

$$x \in (aH)^s = a^sH, y \in (aH)^t = a^tH$$

故存在 $h_1, h_2 \in H$，使

$$x = a^sh_1, y = a^th_2$$

注意到 H 中的元与 G 中的元可交换，a^s 与 a^t 可交换，故

$$xy = (a^sh_1)(a^th_2) = (a^th_2)(a^sh_1) = yx$$

即 G 是交换群。

---

7. 设 G 是群，$N \trianglelefteq G$。证明：如果 N 及商群 G/N 都是周期群，则 G 也是周期群。

证明 对任意的 $a \in G$，由 $N \trianglelefteq G$ 知 $aN \in G/N$。又由于 G/N 是周期群，所以存在正整数 m 使

$$(aN)^m = a^mN = N$$

其中 N 为商群 G/N 中的单位元，因此 $a^m \in N$。

又因为 N 也是周期群，所以存在正整数 n，使

$$(a^m)^n = a^{mn} = e$$

其中 e 为群 N 的单位元。从而 G 中任一元素的阶有限，故 G 是一个周期群。

---

8. 设 G 是群，$G_i(0 \leqslant i \leqslant k)$ 为其子群，且

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{k-1} \trianglelefteq G_k \trianglelefteq G \qquad ①$$

则称此为群 G 的正规群列。若群 G 有正规群列 ① 且诸商群

$$G_1/G_0, G_2/G_1, \cdots, G_k/G_{k-1}$$

又都是交换群时，则称 G 为可解群。证明：对称群 S_2, S_3 及 S_4 都是可解群。

证明 由 $\{e\} \trianglelefteq S_2, S_2/\{e\} \cong S_2$ 为交换群可知 S_2 为可解群。

令 $H = \{(1), (123), (132)\}$，则由本节例 1 可知

$$\{e\} \trianglelefteq H \trianglelefteq S_3$$

且 $H/\{e\}$ 及 S_3/H 均为交换群，所以 S_3 也是可解群。

又由本节例 3 可知

$$\{e\} \trianglelefteq K_4 \trianglelefteq A_4 \trianglelefteq S_4$$

且 $K_4/\{e\}, A_4/K_4, S_4/A_4$ 都是交换群，所以 S_4 也是可解群。

§3　群同态基本定理(P100)

1. 设群 $G \sim \overline{G}$，且同态核是 K。证明：G 中二元素在 $\overline{G}$ 中有相同的象当且仅当它们在 K 的同一陪集中。

证明　设 φ 是 G 到 $\overline{G}$ 的一个同态映射，其同态核 $K = \varphi^{-1}(e')$，其中 e' 为 $\overline{G}$ 中的单位元。

"$\Rightarrow$"　任意 $a,b \in G$，若 $\varphi(a) = \varphi(b)$，则由本章 §1 定理 1 推论知

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

故 $ab^{-1} \in K$，即 a,b 在 K 的同一陪集中。

"$\Leftarrow$"　若 a,b 在 K 的同一陪集中，即 $ab^{-1} \in K$，则

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

故 $\varphi(a) = \varphi(b)$，即 a 与 b 在 $\overline{G}$ 中有相同的象。

---

2. 证明：单群的同态象是单群或单位元群（即只含有一个元素的群）。

证明　设 G 是单群，$\overline{G}$ 是 G 的同态象，K 是同态核，则由群同态基本定理知 $K \trianglelefteq G$。又 G 是单群，故 $K = G$ 或 $K = \{e\}$。

若 $K = G$，则$\{e\} = G/G \cong \overline{G}$，即 $\overline{G}$ 为单位元群；

若 $K = \{e\}$，则 $G = G/\{e\} \cong \overline{G}$，即 $\overline{G}$ 为单群。

---

3. 设 N 是群 G 的一个正规子群，又 $N \subseteq H \leqslant G$。证明：$H$ 在自然同态

$$G \sim G/N$$

之下的象是 H/N。

证明　设 φ 为 $G \sim G/N$ 下的自然同态，则任意 $x \in G$，有

$$\varphi(x) = xN$$

又由 $N \leqslant G$ 及 $N \subseteq H$ 可知 $N \leqslant H$。再由 $N \trianglelefteq G$，故 $\forall a \in H \subseteq G, x \in N$，有 $axa^{-1} \in N$，所以 $N \trianglelefteq H$。

因此若 $a \in H$，则

$$\varphi(a) = aN \in H/N$$

故 $\varphi(H) \subseteq H/N$。另一方面，显见有 $H/N \subseteq \varphi(H)$，从而 $\varphi(H) = H/N$。

---

4. 证明：

(1) 无限循环群与任何循环群同态；

(2) 两个有限循环群 G 与 $\overline{G}$ 同态，当且仅当 $|\overline{G}| \mid |G|$。

证明　(1) 设 $G = \langle a \rangle$ 为无限循环群，$\overline{G} = \langle b \rangle$ 为任一循环群，则 $|a| = \infty$，故 $a^k = a^l$ 当且仅当 $k = l$。定义

$$\varphi: G \longrightarrow \overline{G}$$
$$a^k \longrightarrow b^k$$

其中 k,l 均为整数。则当 $a^k = a^l$ 时，有 $\varphi(a^k) = \varphi(a^l)$，即 φ 是 G 到 $\overline{G}$ 的映射。又由 $|a| = \infty$ 可知 φ 为满射且

$$\varphi(a^s)\varphi(a^t) = b^s b^t = b^{s+t} = \varphi(a^{s+t})$$

即 φ 保持运算，故 $G \sim \overline{G}$。

(2) 设 $G \sim \overline{G}$，$|G| = m$，$|\overline{G}| = n$。则由群同态基本定理知 $G/K \cong \overline{G}$，其中 K 为 G 到 $\overline{G}$ 的同态满射的核。因此 $|G/K| = n$，又 $|G/K| = (G:K)$，从而由 Lagrange 定理知 $n \mid m$，即 $|\overline{G}| \mid |G|$。

反之若 $|\overline{G}| \mid |G|$，$n \mid m$，则 $m = nt$，由于 G 为循环群，故 G 有 t 阶子群 H。显见 G 为交换群，从而其子群 H 为正规子群，即 $H \trianglelefteq G$。又 G/H 为 n 阶循环群及 $\overline{G}$ 为 n 阶循环群，故有

$$\varphi: G/H \cong \overline{G}$$

又存在 G 到 G/H 的自然同态 $f: G \sim G/H$，令 $\psi = \varphi f$，则 $\psi: G \sim \overline{G}$。

---

5. 证明：有理数加群 Q_+ 与非零有理数乘群 Q^* 不同构。

证法 1　若 Q_+ 与 Q^* 间存在一个同构映射，设为 φ，令 $\varphi(0) = \overline{a} \in Q^*$，则由于 φ 为同构映射，故

$$\varphi(0) = \varphi(0+0) = \varphi(0)\varphi(0) = \overline{a}^2$$

从而由 φ 为单射得 $\overline{a} = \overline{a}^2$，故 $\overline{a} = 0$ 或 $\overline{a} = 1$。又 $\overline{a} \in Q^*$，故 $\overline{a} \neq 0$，$\overline{a} = 1$，即 $\varphi(0) = 1$。

又 φ 为满射，故必存在 $a \in Q_+$，使

$$\varphi(a)=-1\in Q^*$$

故 $\varphi(2a)=\varphi(a+a)=\varphi(a)\varphi(a)=(-1)^2=1$。从而由 φ 是单射得 $2a=0$，即 $a=0$，因此 $\varphi(0)=-1$。这与前面的 $\varphi(0)=1$ 相矛盾，故 Q_+ 与 Q^* 不同构。

证法 2 反证法 设 Q_+ 与 Q^* 同构且 φ 为其一同构映射，则由 φ 为双射可得，对于 $2\in Q^*$，存在惟一的 $a\in Q_+$ 且 $a\neq 0$，使 $\varphi(a)=2$。从而

$$\varphi\left(\frac{a}{2}\right)^2=\varphi\left(\frac{a}{2}\right)\varphi\left(\frac{a}{2}\right)=\varphi\left(\frac{a}{2}+\frac{a}{2}\right)=\varphi(a)=2$$

故 $\varphi\left(\frac{a}{2}\right)^2=2$，$\varphi\left(\frac{a}{2}\right)$ 为无理数 $-\sqrt{2}$ 或 $\sqrt{2}$，这与 φ 的定义相矛盾，所以 Q_+ 与 Q^* 不同构。

证法 3 由 $\varphi(a)=\varphi\left(\frac{a}{2}\right)^2\geqslant 0$ 知 φ 不是满射，故同构映射 φ 不存在。

证法 4 易知 Q_+ 中无二阶元(若 $2a=0$，则 $a=0$)，Q^* 中有 2 阶元 -1，而同构映射是保阶的，故同构映射 φ 不存在。

§4 群的同构定理(P104)

1. 设群 $G\sim\overline{G}$，$\overline{N}\trianglelefteq\overline{G}$，$N$ 是 $\overline{N}$ 的逆象。证明：

$$G/N\cong\overline{G}/\overline{N}$$

证明 设 φ 是群 G 到群 $\overline{G}$ 的同态满射，则由题设知 $N=\varphi^{-1}(\overline{N})$，又 $\overline{N}\trianglelefteq\overline{G}$，故

$$\mathrm{Ker}\varphi\subseteq N=\varphi^{-1}(\overline{N})\trianglelefteq G$$

又因为 $\varphi(N)=\varphi(\varphi^{-1}(\overline{N}))=\overline{N}$，所以由第一同构定理即可得

$$G/N\cong\overline{G}/\overline{N}$$

---

2. 设 H,K 是群 G 的两个子群，$K'\trianglelefteq K$，证明：

(1) $H\cap K'\trianglelefteq H\cap K$；

(2) $H\cap K/H\cap K'$ 与 K/K' 的一个子群同构。

证明 (1) 任 $a,b\in H\cap K'$，则 $a\in H$，$a\in K'$，$b\in H$，$b\in K'$，又 $K'\leqslant K$，$H\leqslant G$，则 $b^{-1}\in H$，$b^{-1}\in K'$，进而 $ab^{-1}\in H$ 且 $ab^{-1}\in K'$。即 $ab^{-1}\in$

$H \cap K'$，因此 $H \cap K' \leqslant H \cap K$。

又任 $x \in H \cap K$，任 $a \in H \cap K'$，则 $x \in H$ 且 $x \in K$，$a \in H$ 且 $a \in K'$ 故由 $H \leqslant G$ 及 $a \in H$ 可知

$$xax^{-1} \in H$$

又由于 $a \in K'$，$x \in K$ 以及 $K' \trianglelefteq K$，故又有 $xax^{-1} \in K'$。

从而任 $a \in H \cap K'$，任 $x \in H \cap K$，均有 $xax^{-1} \in H \cap K'$，所以

$$H \cap K' \trianglelefteq H \cap K$$

(2) 定义

$$\varphi: x(H \cap K') \longrightarrow xK'$$

其中 $x \in H \cap K$，则 φ 是群 $H \cap K/H \cap K'$ 到 K/K' 的满同态，则由同态基本定理有

$$H \cap K/H \cap K' \cong \varphi(H \cap K/H \cap K') \leqslant K/K'$$

---

3. 设 G 是群，又 $K \leqslant H \trianglelefteq G$，$K \trianglelefteq G$。证明：若 G/K 是交换群，则 G/H 也是交换群。

证明 要证 G/H 可交换，只需证明对任意 $x, y \in G$

$$xH \cdot yH = yH \cdot xH$$

亦即

$$xyH = yxH, (xy)^{-1}(yx) \in H \qquad (*)$$

而 $K \leqslant H$，若有

$$(xy)^{-1}(yx) \in K, xyK = yxK$$

则有式(*)成立。又由题设条件 G/K 是交换群，当然有

$$xK \cdot yK = yK \cdot xK$$

即 $xyK = yxK$。综上可知 G/H 也是交换群。

---

4. 题设如定理1。证明：$\sigma: x \longrightarrow \varphi(x)\overline{N}$ 是群 G 到商群 $\overline{G}/\overline{N}$ 的满同态，且其核 $\mathrm{Ker}\sigma = N$。从而 $G/N \cong \overline{G}/\overline{N}$。

证明 定理1中设 φ 是群 G 到群 $\overline{G}$ 的一个同态满射，且 $\mathrm{Ker}\varphi \subseteq N \trianglelefteq G$，$\overline{N} = \varphi(N)$，则由 φ 是同态满射可知 σ 为群 G 到商群 $\overline{G}/\overline{N}$ 的满射，且任 $a, b \in G$，有

$$\sigma(ab) = \varphi(ab)\overline{N} = \varphi(a)\varphi(b)\overline{N} = \varphi(a)\overline{N} \cdot \varphi(b)\overline{N} = \sigma(a)\sigma(b)$$

从而 σ 是群 G 到商群 $\overline{G}/\overline{N}$ 的一个满同态，$G \sim \overline{G}/\overline{N}$。

下证核 $\mathrm{Ker}\sigma = N$。任 $x \in N$，由 $\overline{N} = \varphi(N)$ 知 $\varphi(x) \in \overline{N}$，故此时

$$x \xrightarrow{\sigma} \varphi(x)\overline{N} = \overline{N}$$

故 $x \in \mathrm{Ker}\sigma$，所以有 $N \subseteq \mathrm{Ker}\sigma$。又在定理 1 题设中，$\mathrm{Ker}\varphi \subseteq N$，而由题意知 $\mathrm{Ker}\sigma \subseteq \mathrm{Ker}\varphi$，故 $\mathrm{Ker}\,\sigma \subseteq N$，因此有 $\mathrm{Ker}\sigma = N$，即 N 是同态 $G \sim \overline{G}/\overline{N}$ 的核，由群同态基本定理（§3 定理 2）知

$$G/N \cong \overline{G}/\overline{N}$$

---

5. 设 G 是一个群，又 $H_1 \leqslant G, H_2 \trianglelefteq G, N \trianglelefteq G$。证明：如果 $|H_1|, |H_2|$ 与 $(G : N)$ 均有限，且

$$(|H_i|, (G : N)) = 1 \quad (i = 1, 2)$$

则

$$H_1 H_2 \leqslant N$$

证明 由题设及第二同构定理可得

$$H_i/(H_i \cap N) \cong H_i N/N \leqslant G/N \quad (i = 1, 2)$$

从而 $(H_i N : N) = (H_i : H_i \cap N)$ 且整除 $(G : N)$。由 Lagrange 定理可知

$$|H_i| = |H_i \cap N|(H_i : H_i \cap N)$$

因此 $(H_i N : N)$ 也整除 $|H_i|$。从而 $(H_i N : N)$ 整除 $(|H_i|, (G : N))$，而题设中 $(|H_i|, (G : N)) = 1$，故必有 $(H_i N : N) = 1$，即 $H_i N = N$，因此

$$H_i \leqslant N, H_1 H_2 \leqslant N$$

---

6. 设 G 是群，$N \triangleleft G$。如果当 $N \leqslant H \triangleleft G$ 时必有 $N = H$，则称 N 是 G 的一个极大正规子群。证明：

$$N \text{ 是 } G \text{ 的极大正规子群} \Leftrightarrow G/N \text{ 是单群}$$

证明 不妨设 φ 为群 G 到商群 G/N 的自然同态。

“$\Leftarrow$” 设 G/N 为单群。由于 $N \triangleleft G$，故设 $N \subset K \trianglelefteq G$，则

$$\varphi(K) \trianglelefteq G/N$$

且 $\varphi(K) \neq \{N\}$。又 G/N 为单群，故有 $\varphi(K) = G/N = \varphi(G)$。

因此任意 $a \in G$，存在 $k \in K$，使

$$\varphi(a) = \varphi(k)，\text{即 } \varphi(ak^{-1}) = N$$

所以 $ak^{-1} \in \mathrm{Ker}\varphi = N \subset K$，$a = ak^{-1} \cdot k \in K$，故 $G \subseteq K$，又 $K \subseteq G$，所以 $K = G$，即 N 为 G 的极大正规子群。

"⇒"　设 N 为 G 的极大正规子群，下证 G/N 只有平凡正规子群。

任取 $K/N \trianglelefteq G/N$ 且 $K/N \neq \{N\}$，则 $\varphi^{-1}(K/N) \trianglelefteq G$。进而由 φ 为自然同态及 N 为 K/N 的单位元可知 $\varphi^{-1}(N) = N$，故

$$N \subseteq \varphi^{-1}(K/N)$$

又由 $K/N \neq \{N\}$ 可得 $N \subset \varphi^{-1}(K/N)$。而 N 为群 G 的极大正规子群，所以

$$\varphi^{-1}(K/N) = G, \quad K/N = G/N$$

因此 G/N 仅有平凡正规子群，即为单群。

§5　群的自同构群(P110)

1. 证明：阶数 $\leqslant 7$ 的循环群的自同构群都是循环群。

证明　由定理 2，n 阶循环群的自同构群是一个 $\varphi(n)$ 阶群，其中 $\varphi(n)$ 为 Euler 函数($\varphi(n)$ 即为不超过 n 且与 n 互素的正整数的个数)，又

$$\varphi(1) = \varphi(2) = 1, \varphi(3) = \varphi(4) = \varphi(6) = 2$$

故 1 阶、2 阶、3 阶、4 阶、6 阶循环群的自同构群为循环群。

$n = 5$ 时，$\varphi(5) = 4$，故 5 阶循环群 $\langle a \rangle$ 的自同构群是一个 4 阶群。又任 $x \in \langle a \rangle$，定义

$$\sigma : x \longrightarrow x^3$$

则 σ 是 $\langle a \rangle$ 的一个自同构，显见 σ 与置换 $\tau = (1342)$ 同构，而 $\tau^4 = (1)$，从而 $|\sigma| = 4$，即 4 阶群中含有 4 阶元，由第二章 §4 推论 1 可知该自同构群是一个循环群。

$n = 7$ 时，$\varphi(7) = 6$，故 7 阶循环群 $\langle b \rangle$ 的自同构群是一个 6 阶群，又任 $y \in \langle b \rangle$，定义

$$\pi : y \longrightarrow y^5$$

则 π 是 $\langle b \rangle$ 的一个自同构，显见 π 与置换 $\tau = (154623)$ 同构，而 $\tau^6 = (1)$，从而 $|\pi| = 6$，即 6 阶群中含有 6 阶元，由第二章 §4 推论 1 知该自同构群是一个循环群。

---

2. 证明：非交换群的自同构群不能是循环群。

证法 1　设 G 为一个非交换群，C 为 G 的中心，则由本章 §5 定理 4 知

$$\mathrm{Inn}G \cong G/C$$

其中 $\mathrm{Inn}G$ 为群 G 的内自同构群，由本章 §2 第 6 题及 G 为非交换群可知，G/C 不是循环群，由本章 §3 定理 3 可知 $\mathrm{Inn}G$ 也不是循环群，又由本章 §5 定理 3，$\mathrm{Inn}G \trianglelefteq \mathrm{Aut}G$，以及由第二章 §4 定理 4 可知 $\mathrm{Aut}G$ 也不是循环群，即非交换群 G 的自同构群不能是循环群。

证法 2　设 G 为一个非交换群，C 为 G 的中心，$\mathrm{Inn}G$ 为 G 的内自同构群，$\mathrm{Aut}G$ 为 G 的自同构群，则由本章 §5 定理 3 及定理 4 有

$$\mathrm{Inn}G \trianglelefteq \mathrm{Aut}G, \mathrm{Inn}G \cong G/C$$

若 $\mathrm{Aut}G$ 是循环群，则 $\mathrm{Inn}G$ 也是循环群，进而 G/C 也是循环群。从而由本章 §2 第 6 题可知 G 为交换群，这与题设中 G 为非交换群矛盾，所以 $\mathrm{Aut}G$ 不是循环群。

---

3. 证明：若群 G 的自同构群是一个单位元群(即 G 只有恒等自同构)，则 G 必为交换群且每个元素都满足方程 $x^2 = e$。

证明　设 C 为群 G 的中心，$\mathrm{Inn}G$ 为 G 的内自同构群，$\mathrm{Aut}G$ 为 G 的自同构群，则由本章 §5 定理 3 及定理 4 有

$$\mathrm{Inn}G \trianglelefteq \mathrm{Aut}G, \quad \mathrm{Inn}G \cong G/C$$

又 $|\mathrm{Aut}G| = 1$，故 $|\mathrm{Inn}G| = 1$，进而 $|G/C| = 1$，故由本章 §2 第 6 题知 $G = C$ 为交换群。

又任 $x \in G$，定义

$$\tau: x \longrightarrow x^{-1}$$

则 τ 为 G 的自同构，进而依题意知其为 G 的恒等同构，故任 $x \in G$ 均有 $x^{-1} = x$，从而 $x^2 = xx^{-1} = e$。

---

4. 证明：任何非交换单群 G 必与其内自同构群 $\mathrm{Inn}G$ 同构。

证明　设 C 为群 G 的中心，则 $C \trianglelefteq G$。又 G 为非交换单群，故 $C = \{e\}$，$G/C \cong G$，又由本章 §5 定理 4 可知

$$\mathrm{Inn}G \cong G/C$$

从而有

$$G \cong \mathrm{Inn}G$$

5. 设 N 是群 G 的一个子群。证明：N 是 G 的特征子群，当且仅当对 G 的每个自同构 σ 都有 $\sigma(N)=N$。

证明　"⇒"　设 N 是群 G 的特征子群，σ 为群 G 的任一自同构，则由特征子群定义有

$$\sigma(N)\subseteq N$$

显然 σ^{-1} 也是群 G 的自同构，故又有

$$\sigma^{-1}(N)\subseteq N$$

从而有

$$\sigma(\sigma^{-1}(N))\subseteq\sigma(N),\text{即 } N\subseteq\sigma(N)$$

所以

$$\sigma(N)=N$$

"⇐"　若对 G 的每一自同构 σ 都有 $\sigma(N)=N$，显见有 $\sigma(N)\subseteq N$，依特征子群定义即可知 N 为 G 的特征子群。

---

6. 证明：若 G 是一个无中心群，则其自同构群 $\mathrm{Aut}G$ 也是一个无中心群。

证明　任意的 $\tau\in\mathrm{Aut}G$ 且 τ 不是恒等自同构，则存在 $a\in G$，使

$$\tau(a)=b\neq a$$

若 τ 为 $\mathrm{Aut}G$ 中心元素，则 τ 与群 G 的任一自同构可换，从而与群 G 的内自同构 σ_a 可换，即

$$\tau\sigma_a=\sigma_a\tau$$

又任意 $x\in G$，存在 $y\in G$，使 $x=\tau(y)$，于是有

$$\tau\sigma_a(y)=\sigma_a\tau(y),\tau(aya^{-1})=\sigma_a(x)$$

即
$$\tau(a)\tau(y)\tau(a)^{-1}=axa^{-1},bxb^{-1}=axa^{-1}$$

故 $(a^{-1}b)x=x(a^{-1}b)$，即 $a^{-1}b$ 为 G 的中心元素。又题设中 G 为无中心群，故 $a^{-1}b=e,a=b$，这与前面的结论相矛盾。所以 $\mathrm{Aut}G$ 也是一个无中心群。

§6　共轭关系与正规化子(P118)

1. 试分别写出四次单位根乘群 U_4 和四次对称群 S_4 的类等式。

解　因为四次单位根群 $U_4=\langle i\rangle=\{1,-1,i,-i\}$ 为交换群，故其类等式为 $|\langle i\rangle|=c_0=4$。

S_4 的元素有 5 个共轭类，即

(1)；

(12)，(13)，(14)，(23)，(24)，(34)；

(123)，(132)，(124)，(142)，(134)，(143)，(234)，(243)；

(1234)，(1243)，(1324)，(1342)，(1423)，(1432)；

(12)(34)，(13)(24)，(14)(23)。

从而 S_4 的类等式为

$$|S_4| = 1 + 6 + 8 + 6 + 3 = 24$$

---

2. 证明：群中子集的共轭关系是一个等价关系。

证明 设 S 为群 G 的非空子集，则 xSx^{-1} 为 S 的共轭子集，其中 $x \in G$。则 S 与自身共轭当且仅当 S 为 G 的中心。

又若 H 为 S 的共轭子集，则 $H = xSx^{-1}$，其中 $x \in G$，则

$$S = x^{-1}Hx = x^{-1}H(x^{-1})^{-1}$$

故 S 为 H 的共轭子集。

若 H 为 S 的共轭子集，T 为 H 的共轭子集，则

$$H = xSx^{-1}, T = yHy^{-1}$$

其中 $x,y \in G$，则 $xy \in G$ 且

$$T = yxSx^{-1}y^{-1} = (yx)S(yx)^{-1}$$

即 T 也是 S 的共轭子集。

综上可知群 G 中子集的共轭关系是一个等价关系。

---

3. 证明：

(1) 若 C_1, C_2 是群 G 的两个共轭元素类，则 C_1C_2 是 G 的一些共轭元素类的并集。

(2) 若 C_1 是群 G 的一个共轭元素类，则 $C_1^{-1} = \{x^{-1} \mid x \in C_1\}$，更一般地 C_1^m（m 为任意整数）也是 G 的一个共轭元素类。

证明 (1) 任意的 $x \in C_1C_2$，则存在 $x_1 \in C_1, x_2 \in C_2$ 使 $x = x_1x_2$。设 G 中有元素 y 与 x 共轭，则

$$x = aya^{-1} \quad (a \in G)$$

又 C_1, C_2 都是 G 的共轭元素类，故 $a^{-1}x_1a \in C_1, a^{-1}x_2a \in C_2$，从而

$$y = a^{-1}xa = a^{-1}(x_1x_2)a = (a^{-1}x_1a)(a^{-1}x_2a) \in C_1C_2$$

即与 C_1C_2 中元素共轭的元素均在 C_1C_2 中，所以 C_1C_2 是 G 中一些共轭元素类的并集。

(2) 只需证任意整数 m 的情形。任意 $x,y \in C_1^m$，则存在 $x_1,y_1 \in C_1$，使

$$x = x_1^m, y = y_1^m$$

又 C_1 为 G 的一个共轭元素类，故存在 $a \in G$，使

$$x_1 = ay_1a^{-1}$$

$$x_1^m = (ay_1a^{-1})^m = ay_1^m a^{-1}$$

即

$$x = aya^{-1}$$

所以 C_1^m 中任意两个元素均共轭。

下证所有与 C_1^m 中元素共轭的元素均属于 C_1^m。再设 y 为 G 中与上述 x 共轭的元素，则 $x = cyc^{-1}$，其中 $c \in G$。又 C_1 为 G 的一个共轭元素类，故

$$y = c^{-1}xc = c^{-1}x_1^m c = (c^{-1}x_1c)^m \in C_1^m$$

综上可知，C_1^m 是群 G 的一个共轭元素类。

---

4. 设 a 是群 G 的一个元素，证明：

$$\langle a\rangle \trianglelefteq N(a) \leqslant N(\langle a\rangle)$$

证明 由于任意 $x \in N(a)$，有

$$xa^mx^{-1} = a^m \in \langle a\rangle$$

以及 $\langle a\rangle \subseteq N(a)$，从而可得 $\langle a\rangle \trianglelefteq N(a)$。又显见 $N(a) \subseteq N(\langle a\rangle)$，进而 $N(a) \leqslant N(\langle a\rangle)$，所以有

$$\langle a\rangle \trianglelefteq N(a) \leqslant N(\langle a\rangle)$$

---

5. 证明：S_n 的所有对换构成一个共轭类。

证明 对 S_n 中的任意一个对换 (ij)，$\pi(ij)\pi^{-1}$ 为与 (ij) 共轭的任一置换，其中 π 为 S_n 中的一个 n 次置换，由第二章 §6 定理 5 可知

$$\pi(ij)\pi^{-1} = (\pi(i)\pi(j))$$

也是 S_n 的一个对换。

再设 (st) 为 S_n 中的另一个对换，并在 S_n 中取置换 π，使

$$\pi(i) = s, \pi(j) = t$$

则有
$$\pi(ij)\pi^{-1} = (\pi(i)\pi(j)) = (st)$$

从而得(ij)与(st)共轭，即S_n的全体对换构成一个共轭类。

---

6. 设G是有限群，且$H < G$，证明

$$G \neq \bigcup_{x\in G} xHx^{-1}$$

证明 因为G是有限群，故存在正整数k，使$(G : N(H)) = k$，又$H < G$，故$k > 1$，并且由推论2知与H共轭的全部子群为

$$x_1Hx_1^{-1}, x_2Hx_2^{-1}, \cdots, x_kHx_k^{-1}$$

所以
$$\bigcup_{x\in G} xHx^{-1} = \bigcup_{i=1}^{k} x_iHx_i^{-1}$$

如果结论不成立，即有$G = \bigcup\limits_{x\in G} xHx^{-1}$，则由$H \leqslant N(H)$可得

$$|G| = |\bigcup_{x\in G} xHx^{-1}| = |\bigcup_{i=1}^{k} x_iHx_i^{-1}| < k|H|$$
$$\leqslant (G : N(H))|N(H)| = |G|$$

矛盾，所以结论$G \neq \bigcup\limits_{x\in G} xHx^{-1}$成立。

*§7 群的直积(P125)

1. 设$G = G_1 \times \cdots \times G_n$，证明：当$i \neq j$时

$$G_i \cap G_j = \{e\}$$

证明 不妨设$i < j$，则

$$G_i \cap G_j \subseteq G_1G_2\cdots G_i\cdots G_{j-1} \cap G_j$$

故由本章§7定理2可知$G_i \cap G_j \subseteq \{e\}$，从而$G_i \cap G_j = \{e\}$。

---

2. 证明：定理3中的“每个元素表示法惟一”可改为“单位元表示法惟一”。

证明 只需证明“每个元素表示法惟一”与“单位元表示法惟一”等价。

“$\Leftarrow$” 设单位元e表示法惟一。

对任意的$a \in G$，若存在$a_i \in G_i$及$b_i \in G_i (i = 1, 2, \cdots, n)$均有

$$a = a_1a_2\cdots a_n \text{ 且 } a = b_1b_2\cdots b_n$$

则$a_1a_2\cdots a_n = b_1b_2\cdots b_n$，且

$$(a_1a_2\cdots a_n)(b_1b_2\cdots b_n)^{-1}=a_1b_1^{-1}\cdot a_2b_2^{-1}\cdot\cdots\cdot a_nb_n^{-1}=e$$

但由于单位元 e 表示法惟一，故

$$a_ib_i^{-1}=e_i,a_i=b_i\quad(i=1,2,\cdots,n)$$

即 G 中任一元素的表示法均惟一。

"$\Rightarrow$"若 G 中每个元素的表示法惟一，当然有单位元表示法惟一。

---

3. 设 $G=G_1\times G_2,G=G_1'\times G_2$。证明

$$G_1\cong G_1'$$

证明　由 $G=G_1\times G_2$ 可得 $G/G_2=\{aG_2\mid a\in G_1\}$，从而可定义

$$\varphi:G_1\longrightarrow G/G_2$$
$$a\longrightarrow aG_2$$

又由本章 §7 第 1 题可知 $G_1\cap G_2=\{e\}$，故任 $a,b\in G_1$，有

$$a=b\Leftrightarrow a^{-1}b=e\Leftrightarrow a^{-1}b\in G_1\cap G_2\Leftrightarrow a^{-1}b\in G_2$$
$$\Leftrightarrow aG_2=bG_2$$

另一方面有

$$\varphi(ab)=abG_2=aG_2\cdot bG_2=\varphi(a)\varphi(b)$$

所以 φ 为 G_1 到 G/G_2 的同构映射，即 $G/G_2\cong G_1$，同理可证 $G/G_2\cong G_1'$，于是有

$$G_1\cong G_1'$$

---

4. 设 $G=G_1\times G_2\times\cdots\times G_n$，证明：

$$\varphi_i:a_1a_2\cdots a_n\longrightarrow a_i\quad(a_j\in G_j)$$

是群 G 到 G_i 的满同态。

证明　由定理 3，直积中 G_i 与 $G_j(i\neq j)$ 的元素可换，故任 $a_i,b_i\in G_i(i=1,2,\cdots,n)$

$$\begin{aligned}&\varphi_i(a_1a_2\cdots a_i\cdots a_n\cdot b_1b_2\cdots b_i\cdots b_n)\\=&\varphi_i(a_1b_1\cdot a_2b_2\cdot\cdots\cdot a_ib_i\cdot\cdots\cdot a_nb_n)\\=&a_ib_i\\=&\varphi_i(a_1a_2\cdots a_n)\cdot\varphi_i(b_1b_2\cdots b_n)\end{aligned}$$

又显见 φ_i 为群 G 到 $G_i(i=1,2,\cdots,n)$ 的满射，从而有 $G\sim G_i$。

5. 设 G_1,G_2 是两个群，证明：

$$G_1\times G_2\cong G_2\times G_1$$

证明　设 $G=G_1\times G_2$，任 $a_1\in G_1,a_2\in G_2$，定义

$$\varphi:G_1\times G_2\longrightarrow G_2\times G_1$$

$$a_1a_2\longrightarrow a_2a_1$$

由定理3知，G 中每个元素的表示法惟一，从而 φ 为 $G_1\times G_2$ 到 $G_2\times G_1$ 的同构映射，故 $G_1\times G_2\cong G_2\times G_1$。

6. 设群 $G=G_1\times G_2$。证明：

$$G/G_1\cong G_2,G/G_2\cong G_1$$

证法1　类似于上面第3题证明即可得证。

证法2　由定理2，$G_i\lhd G(i=1,2)$，又由上面第1题知 $G_1\cap G_2=\{e\}\lhd G_1$，且 $G_1\cap G_2\lhd G_2$，故由本章§4第二同构定理知

$$G_1G_2/G_2\cong G_1/(G_1\cap G_2)=G_1/\{e\}\cong G_1$$

又 $G/G_2=G_1G_2/G_2$，故 $G/G_2\cong G_1$，同理可得 $G/G_1\cong G_2$。

7. 设群 $G=G_1\times G_2,N\lhd G_1$。证明：$N\lhd G$。

证明　任意 $(a_1,e_2)\in N,(x_1,x_2)\in G,(x_1,e_2)\in G_1,(e_1,x_2)\in G_2$，其中 $e_i\in G_i(i=1,2)$。则

$$(x_1,x_2)(a_1,e_2)(x_1,x_2)^{-1}=(x_1a_1x_1^{-1},e_2)=(x_1,e_2)(a_1,e_2)(x_1,e_2)^{-1}$$

又 $N\lhd G_1$，故 $(x_1,e_2)(a_1,e_2)(x_1,e_2)^{-1}\in N$，从而

$$(x_1,x_2)(a_1,e_2)(x_1,x_2)^{-1}\in N$$

则任 $x\in G$，任 $a\in N$，记 $x=(x_1,x_2),a=(a_1,e_2)$，均有

$$xax^{-1}\in N$$

所以 $N\lhd G$。

8. 设 $G_1,G_2,\cdots,G_n$ 是群 G 的正规子群且 $G=G_1G_2\cdots G_n$，证明：

$$G_1G_2\cdots G_{i-1}\cap G_i=\{e\}\Leftrightarrow G\text{ 中每个元素的表示法惟一}$$

证明　类似于定理3的证明。

“$\Rightarrow$”　若 G 中每个元素的表示法不惟一，令

$$g=a_1\cdots a_{i-1}a_i\cdots a_n=b_1\cdots b_{i-1}b_i\cdots b_n$$

其中 $a_j,b_j\in G_j(j=1,2,\cdots,n)$，$a_i\neq b_i$，$a_{i+1}=b_{i+1},\cdots,a_n=b_n$

由题设 $G_j\lhd G(j=1,2,\cdots,n)$，故由本章 §2 定理 3 知

$$G_1G_2\cdots G_n\lhd G$$

从而

$$(b_1\cdots b_{i-1})^{-1}(a_1\cdots a_{i-1})=b_ia_i^{-1}\in G_1\cdots G_{i-1}\cap G_i$$

而 $b_ia_i^{-1}\neq e$ 这与 $G_1G_2\cdots G_{i-1}\cap G_i=\{e\}$ 矛盾，故 G 中每一个元素的表示法惟一。

"$\Leftarrow$" 若 $G_1G_2\cdots G_{i-1}\cap G_i\neq\{e\}$，则有

$$e\neq a_i=a_1a_2\cdots a_{i-1}\in G_1G_2\cdots G_{i-1}\cap G_i$$

其中 $a_j\in G_j(j=1,2,\cdots,i-1)$，这同 G 中每一元素的表示法惟一矛盾，所以

$$G_1G_2\cdots G_{i-1}\cap G_i=\{e\}$$

* §8 Sylow 定理（P135）

1. 求出 4 次交代群 A_4 的所有 Sylow 子群。

解 $|A_4|=12=2^2\cdot 3$，故 A_4 有 Sylow2- 子群（4 阶）和 Sylow3- 子群（3 阶），又 Klein 四元群

$$K_4=\{(1),(12)(34),(13)(24),(14)(23)\}$$

显然是 A_4 的一个 Sylow 2- 子群，又由本章 §2 例 3 知 $K_4\lhd A_4$，因此 K_4 是 A_4 惟一的 Sylow 2- 子群。

由 A_4 的所有 3- 循环生成的子群为 A_4 的全部 Sylow3- 子群，分别是

$$\langle(123)\rangle,\langle(124)\rangle,\langle(134)\rangle,\langle(234)\rangle,$$

共 4 个。

---

2. 设 G 是 np 阶群（p 是素数），证明：若 $n<p$，则 G 有 p 阶正规子群。

证明 由 $n<p$ 知 G 的 Sylow p- 子群为 p 阶群。又 p 为素数，故该 Sylow p- 子群为循环群，记为 C_p，设这样的子群共有 k_p 个，则由 Sylow 第三定理得

$$k_p=ps+1,k_p\mid np,\text{即}(ps+1)\mid np$$

又$(ps+1,p)=1$，从而$(ps+1)\mid n$，由题设$n<p$，故有$s=0$，进而$k_p=1$，所以C_p是G的正规子群。

3. 设G是一个有限群，P是G的一个Sylow$p$-子群，H是G的一个p-子群。证明：若$H\subseteq N(P)$，则$H\subseteq P$。

证明 由$H\subseteq N(P)$及正规化子定义，对任意$a\in H$，都有$aP=Pa$，故$HP=PH$，从而

$$HP\leqslant G\text{ 且 }a^{-1}Pa=P$$

任取$ab\in HP$，其中$b\in P$，由$a^{-1}ba\in P$知

$$(ab)^2=(ab)(ab)=a^2(a^{-1}ba)b=a^2b_1b=a^2b_2$$

即$(ab)^2=a^2b_2$，其中$b_1=a^{-1}ba$，$b_2=b_1b\in P$，如此下去由数学归纳法可证

$$(ab)^m=a^mb_m$$

其中$b_m\in P$。又因为H为G的一个p-子群，故$|a|=p^r$，从而有

$$(ab)^{p^r}=a^{p^r}b_0=eb_0=b_0\in P$$

又P为p-子群，故$|b_0|$也为p的方幂，因此$|ab|$为p的方幂，即HP为p-子群，又显见子群$P\subseteq HP$及P为G的p-子群，故必有$HP=P$，进而

$$H\subseteq P$$

4. 设K是群G的一个有限正规子群，P是K的一个Sylow$p$-子群，证明：

$$G=N(P)K$$

证明 任意$x\in G$，由$K\lhd G$及$P\leqslant K$可得

$$xPx^{-1}\leqslant xKx^{-1}=K$$

又P为有限群K的Sylow$p$-子群，故xPx^{-1}也是K的一个Sylow$p$-子群。从而由第二Sylow定理知，P与xPx^{-1}在K中共轭。所以存在$k\in K$，使

$$xPx^{-1}=kPk^{-1},(k^{-1}x)P=P(k^{-1}x)$$

故$k^{-1}x\in N(P)$，于是

$$x\in KN(P),G\subseteq KN(P),G=KN(P)$$

又因为$K\lhd G$及$KN(P)=N(P)K$，从而有$G=N(P)K$。

5. 设 P 是有限群 G 的一个 Sylow$p$- 子群。证明：若 G 有子群 H 包含 $N(P)$，则 $N(H)=H$。

证明 由 $P\leqslant G, H\leqslant G$ 及本章 §6 定理 1 知 $H\subseteq N(H)$，且

$$P\trianglelefteq N(P)\subseteq H$$

又任意 $a\in N(H)$，有 $aHa^{-1}=H$，故

$$aPa^{-1}\subseteq aHa^{-1}=H$$

因此 P 与 aPa^{-1} 也是 H 的 Sylow$p$- 子群，故在 H 中共轭，即存在 $h\in H$，使

$$h(aPa^{-1})h^{-1}=P \text{ 或}(ha)P(ha)^{-1}=P\text{，即}(ha)P=P(ha)$$

故有 $ha\in N(P)\subseteq H$，所以 $a\in H$。由 a 的任意性得 $N(H)\subseteq H$，从而由 $H\subseteq N(H)$ 可得

$$N(H)=H$$

---

6. 证明：有限群 G 必有一个最大的正规 p- 子群 H。即 H 是 G 的正规 p- 子群，又若 K 也是 G 的正规 p- 子群，则必 $K\subseteq H$。

证明 若 G 不存在阶数大于 1 的正规 p- 子群，则 G 的单位元群就是 G 的最大正规 p- 子群。

若 G 存在阶数大于 1 的正规 p- 子群，不妨设两个（多于两个情况可归纳证明），记为 H,K，则 HK 仍为 G 的正规子群，即 $HK\trianglelefteq G$，从而由群同构定理可知

$$H/(H\cap K)\cong HK/K$$

但 H 为 p- 子群，故 $H/(H\cap K)$ 为 p- 子群，于是 HK/K 为 p- 子群，任意的 $a\in HK$，则 $aK\in HK/K$，若 aK 的阶为 p^s，则有

$$a^{p^s}K=(aK)^{p^s}=K, a^{p^s}\in K$$

而 K 也为 p- 子群，设 a^{p^s} 的阶为 p^t，故

$$(a^{p^s})^{p^t}=a^{p^{s+t}}=e$$

即 a 的阶也是 p 的方幂，因此 HK 也是 p- 子群，又显见子群 $H\subseteq HK$，$K\subseteq HK$，从而 HK 是 G 的最大正规 p- 子群。

---

7. 证明：196 阶群 G 必有一个阶大于 1 的 Sylow 子群，它是 G 的一个正规

子群。

证明　只需证明群 G 有惟一的阶大于 1 的 Sylow 子群。

$|G| = 196 = 2^2 \cdot 7^2$，设 P 是 G 的一个 Sylow 7-子群，与 P 共轭的子群个数 $k = 7q + 1$ 应是 196 的正因数，而 196 的正因数只有

$$1,2,4,7,14,28,49,98,196$$

所以必有 $q = 0$，故 $k = 1$，即 P 是 G 的惟一的 Sylow 7-子群，进而又是 G 的正规子群。

---

8. 设 H,K 是群 G（不一定有限）的两个 p-子群，且 $K \trianglelefteq G$。证明：HK 也是 G 的一个 p-子群。

证法 1　由上面第 6 题的证明过程即可得到。

证法 2　由 $H \leqslant G$ 及 $K \trianglelefteq G$ 可得 $HK \leqslant G$ 且任 $x \in G$，均有

$$xK = Kx$$

对任意 $hk \in HK$，其中 $h \in H, k \in K$，由于 H 为 p-子群，不妨设 $|H| = p^s$，从而若 $p^s = 2$ 时，有

$$(hk)^2 = (hk)(hk) = h(hk_1)k = h^2k_2 = k_2$$

其中 $k_1,k_2 \in K$。于是一般地有

$$(hk)^{p^s} = h^{p^s}k' = k' \in K$$

又 K 也是 p-子群，不妨令 $|k'| = p^t$，故

$$(hk)^{p^{s+t}} = (k')^{p^t} = e$$

即 $|hk|$ 也是 p 的方幂，故 HK 也是 G 的 p-子群。

* §9　有限交换群(P144)

1. 证明：对任意素数 $p_1,p_2,\cdots,p_m$ 和任意正整数 $k_1,k_2,\cdots,k_m$，总存在有限交换群 G，其初等因子组为

$$\{p_1^{k_1},p_2^{k_2},\cdots,p_m^{k_m}\}$$

证明　设 $t_i = p_i^{k_i}(i = 1,2,\cdots,m)$，令

$$G = C_{t_1} \times C_{t_2} \times \cdots \times C_{t_m}$$

其中 C_{t_i} 为 t_i 阶循环群，则群 G 即为初等因子组为 $\{p_1^{k_1},p_2^{k_2},\cdots,p_m^{k_m}\}$ 的有限交换群。

2. 设 p 是素数。试给出同构意义下的所有 p^4 阶交换群。

解 p^4 阶交换群的初等因子共有

$$\{p^4\},\{p,p^3\},\{p^2,p^2\},\{p,p,p^2\},\{p,p,p,p\}$$

5 种,因此互不同构的所有 p^4 阶交换群共有 5 个,如下

$$C_{p^4},C_p\times C_{p^3},C_{p^2}\times C_{p^2},C_p\times C_p\times C_{p^2},C_p\times C_p\times C_p\times C_p$$

其中 C_k 表示 k 阶循环群。

---

3. 给出同构意义下的所有 108 阶交换群。

解 $108=2^2\cdot 3^3$,故 108 阶交换群的初等因子共有

$$\{2^2,3^3\},\{2^2,3,3^2\},\{2^2,3,3,3\}$$

$$\{2,2,3^3\},\{2,2,3,3^2\},\{2,2,3,3,3\}$$

6 种,因此互不同构的所有 108 阶交换群共有六个,如下

$$C_4\times C_{27},C_4\times C_3\times C_9,C_4\times C_3\times C_3\times C_3$$

$$C_2\times C_2\times C_{27},C_2\times C_2\times C_3\times C_9,C_2\times C_2\times C_3\times C_3\times C_3$$

其中 C_k 表示 k 阶循环群。

---

4. 设 G 是阶大于 1 的有限群。证明:若除 e 外其余元素的阶均相同,则 G 为素幂阶群。

证明 假设存在互异素数 p,q,使 $pq\mid|G|$,则由本章 §2 定理 5 知群 G 有 p 阶元素及 q 阶元素,这与题设中除 e 外其余元素的阶相同相矛盾,故 $|G|$ 为素数 p 的方幂。

---

5. 设 G 是有限交换群。证明:G 是循环群的充要条件是,$|G|$ 是 G 中所有元素阶的最小公倍数。

证明 "$\Rightarrow$" 由 Lagrange 定理即可得 $|G|$ 是 G 中所有元素的阶的公倍数,又 n 阶循环群中必有 n 阶元素,所以 $|G|$ 为 G 中所有元素的阶最小公倍数。

"$\Leftarrow$" 由第二章 §7 第 12 题可知在 n 阶群 G 中含有 n 阶元素,因此 G 是循环群。

---

6. 用 C_k 表示 k 阶循环群,证明

$$C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}\cong C_{m_1m_2\cdots m_n}$$

当且仅当正整数 $m_1,m_2,\cdots,m_n$ 两两互素。

证明 “$\Rightarrow$” 若 $C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}\cong C_{m_1m_2\cdots m_n}$，则由本章 §3定理3知 $C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}$ 为 $m_1m_2\cdots m_n$ 阶的循环群，从而其中含有阶为 $m_1m_2\cdots m_n$ 的元素 $(a_1,a_2,\cdots,a_n)$。

如果 $m_1,m_2,\cdots,m_n$ 中存在两个不互素的正整数，不妨设其为 m_1,m_2，则

$$(m_1,m_2)=d>1,m_1=dm_1',m_2=dm_2'$$

故

$$dm_1'm_2'm_3\cdots m_n<m_1m_2m_3\cdots m_n$$

$$(a_1,a_2,\cdots,a_n)^{dm_1'm_2'm_3\cdots m_n}=(e_1,e_2,\cdots,e_n)$$

这与 $(a_1,a_2,\cdots,a_n)$ 的阶为 $m_1m_2\cdots m_n$ 相矛盾，所以 $m_1,m_2,\cdots,m_n$ 两两互素。

“$\Leftarrow$” 利用数学归纳法证明。

$n=1$ 时，由同构的反身性即得。

$n=2$ 时，m_1 与 m_2 互素，若 $C_{m_1}\times C_{m_2}$ 为 m_1m_2 阶循环群，则 $C_{m_1}\times C_{m_2}\cong C_{m_1m_2}$。故只需证 $C_{m_1}\times C_{m_2}$ 中含有 m_1m_2 阶元素，令 $C_{m_1}=\langle a\rangle$，$C_{m_2}=\langle b\rangle$，e_1,e_2 分别为 C_{m_1},C_{m_2} 中的单位元，则

$$(a,b)\in C_{m_1}\times C_{m_2}\text{ 且}(a,b)^{m_1m_2}=(a^{m_1m_2},b^{m_1m_2})=(e_1,e_2)$$

另一方面，若存在正整数 s，使

$$(a,b)^s=(e_1,e_2)$$

则 $(a^s,b^s)=(e_1,e_2)$，$a^s=e_1$，$b^s=e_2$，从而 $m_1\mid s$，$m_2\mid s$，又 m_1 与 m_2 互素，故 $m_1m_2\mid s$，于是 (a,b) 的阶为 m_1m_2。

因此可知 $C_{m_1}\times C_{m_2}$ 为 m_1m_2 阶的循环群，而由已知 $C_{m_1m_2}$ 也为 m_1m_2 阶的循环群，所以

$$C_{m_1}\times C_{m_2}\cong C_{m_1m_2}$$

设结论对 $n-1$ 成立，即

$$C_{m_1}\times C_{m_2}\times\cdots\times C_{m_{n-1}}\cong C_{m_1m_2\cdots m_{n-1}}$$

从而

$$\begin{aligned}C_{m_1}\times C_{m_2}\times\cdots\times C_{m_{n-1}}\times C_{m_n}&=(C_{m_1}\times C_{m_2}\times\cdots\times C_{m_{n-1}})\times C_{m_n}\\&\cong C_{m_1m_2\cdots m_{n-1}}C_{m_n}\end{aligned}$$

又由 $m_1,m_2,\cdots,m_n$ 两两互素可知 $(m_1,m_2,\cdots,m_{n-1},m_n)=1$，故由上述

$n=2$ 时的情况便有

$$C_{m_1m_2\cdots m_{n-1}}\times C_{m_n}\cong C_{m_1m_2\cdots m_n}$$

所以

$$C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}\cong C_{m_1m_2\cdots m_n}$$

---

7. 设 G 是群，$H\leqslant G$。证明：如果关于 H 的任意两个左陪集的乘积仍是一个左陪集，则 $H\trianglelefteq G$。

证明 设 aH,bH 为 H 的任两个左陪集，先证 $aH\cdot bH=abH$。

依题设 $aH\cdot bH$ 仍为一个左陪集，不妨令 $aH\cdot bH=cH$，而

$$ab=ae\cdot be\in aH\cdot bH$$

从而 $ab\in cH$，故 $abH=cH$，故 $aH\cdot bH=abH$。

任 $h\in H,a\in G$，因为

$$(aha^{-1})h=ah\cdot a^{-1}h\in aH\cdot a^{-1}H=(aa^{-1})H=H$$

所以 $aha^{-1}\in H$，故 $H\trianglelefteq G$。

---

8. 举例指出，存在群 G，C 为其中心，而商群 G/C 的中心的阶大于 1。

解 例如，第二章 §1 例 4 中的四元数群

$$G=\{1,i,j,k,-1,-i,-j,-k\}$$

其中心 $C=\{1,-1\}$，而

$$G/C=\{C,iC,jC,kC\}$$

且 G/C 为交换群，故其中心就是自身，其阶为 4，大于 1。

---

9. 设 $N\trianglelefteq G$，$|N|=m$，$(m,n)=1$，证明：若 $|a|=n$，则 aN 的阶也是 n；反之，若 aN 的阶是 n，则在 G 中有 n 阶元 b 使 $aN=bN$。

证明 ① 若 $|a|=n$，则由 $N\trianglelefteq G$ 知

$$(aN)^n=a^nN=eN=N$$

若存在正整数 s，使 $(aN)^s=N$，则 $a^sN=N$，$a^s\in N$，又 $|N|=m$，故 $a^{sm}=e$，于是 $n\mid sm$。而题设中 $(m,n)=1$，故 $n\mid s$，即得 $|aN|=n$。

② 因为 $(m,n)=1$，所以存在整数 s,t，使

$$ms+nt=1$$

令 $b=a^{ms}=a^{1-nt}=a\cdot a^{-nt}$，又由题设中 $|aN|=n$ 知

$$(aN)^n=a^nN=N,a^n\in N$$

从而

$$a^{-1}b=a^{-1}\cdot a\cdot a^{-nt}=a^{-nt}=(a^n)^{-t}\in N$$

故

$$bN=aN$$

又因为题设中 $|N|=m$，所以由已证 $a^n\in N$ 知

$$(a^n)^m=e,b^n=(a^{ms})^n=e$$

另一方面，若存在正整数 r，使 $b^r=a^{msr}=e$，则

$$(aN)^{msr}=eN=N$$

又 $|aN|=n$，故 $n\mid msr$，而由 $ms+nt=1$ 可知 $(n,ms)=1$，因此 $n\mid r$，所以 $|b|=n$，即存在 n 阶元 b，使 $aN=bN$。

---

10. 称群 G 中元素 $a^{-1}b^{-1}ab$ 为元素 a 与 b 的换位元，证明：

(1) 由 G 中所有换位元生成的子群 K 是 G 的一个正规子群；

(2) G/K 是交换群；

(3) 若 $N\trianglelefteq G$，且 G/N 可换，则 $N\supseteq K$。

证明 (1) K 中两个元的乘积仍是有限个换位元的乘积，因而仍是 K 的一个元。一个换位元的逆仍是一个换位元，故 K 的一个元的逆仍是 K 的一个元。故 K 为 G 的一个子群。

任 $a\in G,k\in K$，由于

$$aka^{-1}=(aka^{-1}k^{-1})k\in K$$

故 K 为 G 的一个正规子群。

(2) 任 $a,b\in G$，则 $a^{-1}b^{-1}ab=k\in K$，从而

$$ab=bak,abK=bakK=baK$$

所以 $(aK)(bK)=(bK)(aK)$，故 G/K 为交换群。

(3) 因为 G/N 可换，所以对任意 $a,b\in G$

$$(aN)(bN)=(bN)(aN),abN=baN$$

由此得 $ab=ban$，其中 $n\in N$，即

$$a^{-1}b^{-1}ab=n\in N$$

这样 N 含有一切换位元，故有 $K\subseteq N$。

11. 设 H,K 是群 G 的两个有限正规子群，且 $(|H|,|K|)=1$。证明：如果商群 G/H 与 G/K 都是交换群，则 G 也是交换群。

证明 易知 $H\cap K\leqslant H$，$H\cap K\leqslant K$，而 $|H|$ 与 $|K|$ 均有限，故

$$|H\cap K|\mid|H|$$

$$|H\cap K|\mid|K|$$

于是 $|H\cap K|\mid(|H|,|K|)$，而 $(|H|,|K|)=1$，故

$$|H\cap K|=1$$

$$H\cap K=\{e\}$$

任意 $a,b\in G$，因为商群 G/H 与 G/K 均可交换，所以

$$abH=baH,abK=baK$$

即 $a^{-1}b^{-1}ab\in H$，$a^{-1}b^{-1}ab\in K$，从而由已证 $H\cap K=\{e\}$ 可知

$$a^{-1}b^{-1}ab=e$$

即 $ab=ba$，所以 G 也是交换群。

---

12. 设 k 是一个奇数。证明：$2k$ 阶群 G 必有 k 阶子群。

提示：在 G 中取一个 2 阶元 a，可先证

$$G=\{x_1,x_2,\cdots,x_k,ax_1,ax_2,\cdots,ax_k\};$$

再由 Cayley 定理，$G\cong\overline{G}$ 且

$$(x_1,ax_1)(x_2,ax_2)\cdots(x_k,ax_k)\in\overline{G}$$

再利用第二章 §6 例 3 即得。

证明 由 Cayley 定理可知 $2k$ 阶群 G 与其上的一个 $2k$ 阶的 $2k$ 次置换群 $\overline{G}$ 同构。

由于任一有限群中阶大于 2 的元必成对出现，故偶数阶群 G 中必有某 2 阶元 a 存在，且 $a=a^{-1}$。故任 $x_1\in G$，有

$$x_1\neq ax_1$$

再取 $x_2\in G$ 且 $x_2\notin\{x_1,ax_1\}$，则由 $a^{-1}=a$ 知

$$x_2\neq ax_2,x_1\neq ax_2,ax_1\neq ax_2$$

如此下去，而 $|G|=2k$，故可继续到第 k 步，且

$$G=\{x_1,x_2,\cdots,x_k,ax_1,ax_2,\cdots,ax_k\}$$

因为

$$a^2=e,a(ax_i)=a^2x_i=x_i\quad(i=1,2,\cdots,k)$$

所以可令置换

$$\tau_a = \begin{pmatrix} x_1 & x_2 & \cdots & x_k & ax_1 & ax_2 & \cdots & ax_k \\ ax_1 & ax_2 & \cdots & ax_k & x_1 & x_2 & \cdots & x_k \end{pmatrix}$$

且 $\tau_a = (x_1, ax_1)(x_2, ax_2)\cdots(x_k, ax_k) \in \overline{G}$，由题设 k 为奇数，故 $\overline{G}$ 中有奇置换，从而由第二章 §6 例 3 知 $\overline{G}$ 中奇偶置换各占一半。

又由于 $G \cong \overline{G}$，故 $|\overline{G}| = 2k$，从而其 k 个偶置换作成 $\overline{G}$ 的一个子群。因此，G 也有 k 阶子群存在。

---

13. 设 G 是一个有限 p- 群。证明：G 的中心 C 的阶大于 1。

证明 设 p 为某素数，$|G| = p^m$，将 G 进行共轭元素类分解，则

$$G = G_1 \cup G_2 \cup \cdots \cup G_n$$

其中 $G_i \cap G_j = \varnothing (i \neq j)$，$G_1 = \{e\}$，$|G_i|$ 为 p^m 的因数$(i = 1, 2, \cdots, n)$，从而每个 $|G_i|$ 必为 1 或素数 p 的方幂。又由 $|G_1| = 1$ 以及 $|G_1| + |G_2| + \cdots + |G_n| = |G| = p^m$，$|G_2| + |G_3| + \cdots + |G_n| = p^m - 1$，故必存在 $i \geqslant 2$ 使 $|G_i| = 1$，即 $G_i = \{a\}$ 且 $a \neq e$，从而

$$a \in C，又\ e \in C，故\ |C| > 1$$

---

14. 证明：p^2 阶群必是交换群，其中 p 是一个素数。

证法 1 设群 G 的阶为 p^2，其中心为 C。若 G 不是交换群，则由 C 为 G 的可换子群可知 $C \neq G$，从而由上题结果及 Lagrange 定理知 $|C| = p$。

任取非中心元 a，因为 C 中元素与 a 都可交换，所以 a 在 G 中的中心化子 $N(a) = C$，这又说明 $a \in C$，矛盾。故 G 为交换群。

证法 2 若群 G 不是交换群，由证法 1 可知 $|C| = p$，故 G/C 为 p 阶循环群。令

$$G/C = \langle \overline{a}_0 \rangle$$

其中 $\overline{a}_0 = a_0C$。任取 $a_1, a_2 \in G$，则据 $\overline{a}_1 = \overline{a}_0^m, \overline{a}_2 = \overline{a}_0^n$，可设

$$a_1 = a_0^m c_1, a_2 = a_0^n c_2，其中\ c_1, c_2 \in C$$

故由 c_1, c_2 为中心元可知 $a_1a_2 = a_2a_1$，即 G 为交换群，矛盾，故 G 为交换群。

---

15. 证明：群 G 的子集 S 的中心化子等于 S 中各元素的正规化子的交。

证明 由

$$C(S)=\{x \mid x\in G, xs=sx, s\in S\}$$
$$N(a)=\{y \mid y\in G, ya=ay, a\in S\}$$

可知

$$\bigcap_{a\in S} N(a)=\{z \mid z\in G, za=az\}\subseteq C(S)$$

另一方面，任 $x\in C(S)$，必有 $x\in\bigcap_{a\in S}N(a)$，从而 $C(S)\subseteq\bigcap_{a\in S}N(a)$，所以

$$C(S)=\bigcap_{a\in S}N(a)$$

---

16. 证明：如果有限 p- 群 G 只有一个指数为 p 的子群，则 G 是一个循环群。

证明 不妨设 $|G|=p^n$，对 n 用归纳法证明。

$n=1$ 时，结论显然成立。

设 $k<n$ 时结论成立，下证 $k=n$ 时即 $|G|=p^n$ 时 G 为循环群。

由本章 §9 第 13 题的证明可知 G 的中心 C 的指数 $|C|>1$，故 $|G/C|<p^n$，令 H 为 G 的指数为 p 的子群，依题意，H 惟一。又由于

$$(G:H)=p\Leftrightarrow \text{等价于}(G/C:H/C)=p$$

故 G/C 也只有一个指数为 p 的子群，从而由 $|G/C|<p^n$ 及假设知 G/C 为循环群。故由本章 §2 第 6 题知 G 为交换群，即 G 为有限交换 p- 群，故由不变因子定理，G 可惟一分解为

$$G=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_s\rangle$$

其中 $|a_i|=p^{k_i}(i=1,2,\cdots,s)$。下证 $s=1$。

若 $s>1$，则 $\langle a_1\rangle$ 与 $\langle a_2\rangle$ 分别有惟一的指数为 p 的子群 $\langle a_1^p\rangle$ 与 $\langle a_2^p\rangle$，从而

$$\langle a_1^p\rangle\times\langle a_2\rangle\times\cdots\times\langle a_s\rangle \text{与} \langle a_1\rangle\times\langle a_2^p\rangle\times\cdots\times\langle a_s\rangle$$

为 G 的两个指数为 p 的子群，这与题设中的惟一性矛盾，因此 $s=1$，即 $G=\langle a_1\rangle$，为循环群。

---

17. 证明：n 阶群的自同构群是有限群，且其阶是 $(n-1)!$ 的一个因数。

证明 由 $|G|=n$，可设 $G=\{e,a_2,\cdots,a_n\}$，且记 $S=\{a_2,a_3,\cdots,a_n\}$，

$\mathrm{Aut}G$ 为 G 的自同构群。任意 $\sigma \in \mathrm{Aut}G$，由于 $\sigma(e)=e$，及 σ 为双射，故 $\sigma|_S$ 为 S 上的一个置换，因此 $\sigma|_S \in S_{n-1}$（S_{n-1} 为 S 上的 $n-1$ 次对称群），定义

$$\varphi:\sigma \longrightarrow \sigma|_S$$

则 φ 为 $\mathrm{Aut}G$ 到 S_{n-1} 上的一个单射。

又任 $\sigma \in \mathrm{Aut}G, x \in G$，有 $\sigma|_S(x)=\sigma(x)$，故 φ 为一个同态映射，即 φ 为 $\mathrm{Aut}G$ 到 S_{n-1} 的单同态映射，从而

$$\mathrm{Aut}G \cong \varphi(\mathrm{Aut}G) \leqslant S_{n-1}$$

故 $\mathrm{Aut}G$ 为有限群且由 Lagrange 定理知 $|\mathrm{Aut}G| \,\big|\, |S_{n-1}|$，即

$$|\mathrm{Aut}G| \,\big|\, (n-1)!$$

---

18. 设 G_1, G_2 是两个群。证明：若 $G_1 \cong G_2$，则

$$\mathrm{Aut}G_1 \cong \mathrm{Aut}G_2$$

再举例指出反之不成立。

证明　设 φ 为 G_1 到 G_2 的一个同构映射，任意 $\sigma_1 \in \mathrm{Aut}G_1, x_1 \in G_1$，定义

$$\sigma_2:\varphi(x_1) \longrightarrow \varphi(\sigma_1(x_1))$$

下证 $\sigma_2 \in \mathrm{Aut}G_2$。

任意 $x_2 \in G_2$，则存在 $x_1 \in G_1$，使 $\varphi(x_1)=x_2$，故 $\varphi(\sigma_1(x_1))$ 是由 x_2 完全确定的 G_2 中的一个元素。若任取 $y_2 \in G_2$，令 $\varphi(y_1)=y_2, \sigma_1(x_1)=y_1$，其中 $y_1, x_1 \in G_1$，则 $\varphi(x_1) \in G_2$ 且

$$\sigma_2(\varphi(x_1))=\varphi(\sigma_1(x_1))=\varphi(y_1)=y_2$$

从而 σ_2 是 G_2 到 G_2 的一个满射。

同理可证 σ_2 是 G_2 到 G_2 的单射。

又任 $x_1, y_1 \in G_1$，

$$\begin{aligned}\sigma_2(\varphi(x_1)\varphi(y_1)) &= \sigma_2(\varphi(x_1y_1))=\varphi(\sigma_1(x_1y_1)) \\ &= \varphi(\sigma_1(x_1)\sigma_1(y_1))=\varphi(\sigma_1(x_1))\cdot\varphi(\sigma_1(y_1)) \\ &= \sigma_2(\varphi(x_1))\cdot\sigma_2(\varphi(y_1))\end{aligned}$$

故综上可知 σ_2 为 G_2 的一个自同构，即 $\sigma_2 \in \mathrm{Aut}G_2$。

定义对应

$$\Psi:\sigma_1 \longrightarrow \sigma_2$$

则 Ψ 为 $\mathrm{Aut}G_1$ 到 $\mathrm{Aut}G_2$ 的映射，且任 $\tau_2 \in \mathrm{Aut}G_2$，定义

$$\tau_1:x_1 \longrightarrow \varphi^{-1}(\tau_2(\varphi(x_1)))$$

则 $\tau_1 \in \mathrm{Aut}G_1$。又任 $x_2 \in G_2$，则存在 $x_1 \in G_1$ 使 $\varphi(x_1) = x_2$，且

$$\varphi(\tau_1(x_1)) = \varphi\varphi^{-1}(\tau_2(x_2)) = \tau_2(x_2) = \tau_2(\varphi(x_1))$$

故 τ_1 是 τ_2 在 Ψ 下的原象，从而 Ψ 为满射。又由 τ_1 的定义及 φ 为同构映射可知 Ψ 也是 $\mathrm{Aut}G_1$ 到 $\mathrm{Aut}G_2$ 的单射，故 Ψ 为双射。

任 $\sigma_1, \sigma_1' \in \mathrm{Aut}G_1$，令

$$\sigma_2 : \varphi(x_1) \longrightarrow \varphi(\sigma_1(x_1)), \sigma_2' = \varphi(\sigma_1'(x_1))$$

则有

$$\sigma_2\, \sigma_2'(\varphi(x_1)) = \sigma_2(\varphi(\sigma_1'(x_1))) = \varphi(\sigma_1(\sigma_1'(x_1))) = \varphi((\sigma_1\, \sigma_1')(x_1))$$

故综上可知 Ψ 为 $\mathrm{Aut}G_1$ 到 $\mathrm{Aut}G_2$ 的同构映射，从而

$$\mathrm{Aut}G_1 \cong \mathrm{Aut}G_2$$

若设 G_1 为无限循环群，G_2 是三阶循环群，则由本章 §5 推论 2 知 $\mathrm{Aut}G_1 \cong \mathrm{Aut}G_2$，但显见 G_1 与 G_2 不同构，因此 $\mathrm{Aut}G_1 \cong \mathrm{Aut}G_2$ 未必有 G_1 与 G_2 同构。

---

19. 设 P 是有限群 G 的一个 Sylow p- 子群，$N \trianglelefteq G$。证明：

(1)$P \cap N$ 是 N 的一个 Sylow p- 子群；

(2)PN/N 是 G/N 的一个 Sylow p- 子群。

证明 (1) 显然 $P \cap N$ 为 p- 子群。记 $P_1 = P \cap N$，则若 $p \nmid (N : P_1)$，则 P_1 为 N 的Sylow p- 子群。

注意到

$$(N : P_1) = (N : N \cap P) = (PN : N)$$

$$(G : P) = (G : PN)(PN : P)$$

又 P 为 G 的一个 Sylow p- 子群，故 $p \nmid (G : P)$，即$(G : P)$ 中不含因子 p，从而

$$p \nmid (G : PN)(PN : P), p \nmid (PN : P)$$

进而 $p \nmid (N : P_1)$，即$(N : P_1)$ 中不含因子 p，故 $P \cap N$ 是 N 的一个 Sylow p- 子群。

(2) 依题意，设

$$|G| = p^n st, \ |N| = p^m st$$

其中$(p, st) = 1, m \leqslant n$，则 $|P| = p^n$，$|P \cap N| = p^r$，其中 $r \leqslant m$。

由群同构定理知

$$PN/N \cong P/(P \cap N)$$

故 $|PN/N| = |P/(P \cap N)| = p^{n-r}$，其中 $n-r \geqslant n-m$，而 $|G/N| = p^{n-m}$，$|PN/N| \mid |G/N|$，故

$$|PN/N| \leqslant p^{n-m}$$

即 $n-r \leqslant n-m$，从而 $|PN/N| = p^{n-m}$，于是 PN/N 是 G/N 的一个 Sylow p- 子群。

---

20. 设 S_3 是 $M = \{1,2,3\}$ 上的三次对称群，证明

$$\mathrm{Aut}S_3 \cong S_3$$

证明 $S_3 = \{(1),(12),(13),(23),(123),(132)\}$，其中 $(12),(13),(23)$ 为 S_3 的所有 2 阶元，故

$$H_1 = \{(1),(12)\}, H_2 = \{(1),(13)\}, H_3 = \{(1),(23)\}$$

为 S_3 的所有 2 阶子群。

记 $S = \{H_1, H_2, H_3\}$，任取 $\sigma \in \mathrm{Aut}S_3$，则 σ 引出 S 上的一个置换：

$$\varphi: \sigma \longrightarrow \begin{pmatrix} H_1 & H_2 & H_3 \\ \sigma(H_1) & \sigma(H_2) & \sigma(H_3) \end{pmatrix}$$

且这一对应 φ 是从 $\mathrm{Aut}S_3$ 到 S 上的三次对称群 S_3' 的一个同态映射，又

$$\sigma \in \mathrm{Ker}\varphi \Leftrightarrow \sigma \text{ 在 } S \text{ 上引出恒等置换}$$

即 $\sigma(H_i) = H_i (i = 1,2,3)$，亦即 σ 把 $(12),(13),(23)$ 分别变为自身。而

$$S_3 = \langle (12),(13),(23) \rangle$$

故 σ 是 S_3 的恒等置换，从而 φ 是单同态。

又 $|C(S_3)| = 1$，$\mathrm{Inn}S_3 \cong S_3/C(S_3) \cong S_3$，故

$$|\mathrm{Aut}S_3| \geqslant |\mathrm{Inn}S_3| = |S_3/C(S_3)| = |S_3| = 6$$

因此 φ 也是满同态，于是 φ 是同构映射，即

$$\mathrm{Aut}S_3 \cong S_3' \cong S_3$$

---

21. 设 G 是一个有限群，且 $|G| = p^2 q$，其中 p, q 是两个互异的素数。证明：G 不是单群。

证明 由第三 Sylow 定理知 G 的 p^2 阶和 q 阶子群的个数分别为

$$k_p = 1 \text{ 或 } q, k_q = 1 \text{ 或 } p \text{ 或 } p^2$$

若 $p>q$，则 $k_p=1$。

若 $p<q$，且 $k_q\neq 1$，则由 $1+q>p$ 知 $k_q\neq p$，所以必有 $k_q=p^2$。

由于互异 q 阶循环群的交必为 $\{e\}$，故 G 中的 q 阶元素的个数为 $p^2(q-1)=p^2q-p^2$，而剩下的 p^2 个元素恰组成一个 p^2 阶群，故 $k_p=1$。

综上可知或 $k_p=1$ 或 $k_q=1$，从而 G 不是单群。

---

22. 设 G 是一个有限群，且 $|G|=pqr$，其中 p,q,r 是互异素数。证明 G 不是单群。

证明 不妨设 $p>q>r$，由 Sylow 定理可设 G 的 Sylow p- 子群、Sylow q- 子群、Sylow r- 子群的个数分别为 k_p,k_q,k_r 个。

若 $k_p>1,k_q>1,k_r>1$，则由互异 Sylow p- 子群的交是 $\{e\}$ 知 k_p 个 Sylow p- 子群共含有 $k_p(p-1)$ 个 p 阶元，k_q 个 Sylow q- 子群共含有 $k_q(q-1)$ 个 q 阶元，k_r 个 Sylow r- 子群共含有 $k_r(r-1)$ 个 r 阶元，故

$$|G|=pqr\geqslant 1+k_p(p-1)+k_q(q-1)+k_r(r-1)$$

又由 Sylow 定理知 $k_p\mid qr$，而 p,q,r 是互异素数且 $k_p>1$，因此只有

$$k_p=q,r\text{ 或 }qr$$

若 $k_p=q$，则由 $p\mid k_p-1$ 可得 $p\mid q-1$，这与 $p>q$ 矛盾，故 $k_p\neq q$。同理 $k_p\neq r$。所以 $k_p=qr$。

又 $k_q\mid pr$，$pq\mid k_p-1$，$k_q>1$，$q>r$，故 $k_q\geqslant p$。同理 $k_r\geqslant q$，从而

$$\begin{aligned}pqr&\geqslant 1+k_p(p-1)+k_q(q-1)+k_r(r-1)\\&\geqslant 1+qr(p-1)+p(q-1)+q(r-1)\end{aligned}$$

即 $0\geqslant(p-1)(q-1)$，矛盾。所以 k_p,k_q,k_r 中至少有一个等于1，于是 G 至少含有一个非平凡正规子群，故 G 不是单群。

---

23. 证明：不存在 56 阶单群。

证明 设群 G 的阶为 56，由于 $56=2^3\cdot 7$，故由第三 Sylow 定理知，若记 G 的 Sylow 7- 子群个数为 k_7，则 $k_7\mid 56$ 且

$$k_7\equiv 1\pmod 7$$

又由 Lagrange 定理可得 $k_7=1$ 或 8。

若 $k_7=1$，即 Sylow 7- 子群惟一，且是 G 的非平凡正规子群，故 G 不是单群。

若 $k_7=8$，由于 G 的 Sylow 7- 子群是 7 阶群，故它们是循环群且任两个互异的 Sylow 7- 子群的交为 $\{e\}$，从而这些 Sylow 7- 子群共占去 G 的 49 个元素。又 Sylow 7- 子群与 Sylow 2- 子群的交为 $\{e\}$，于是 G 只有一个 Sylow 2- 子群，它即为 G 的正规子群，故 G 不是单群。

综上可知，不存在 56 阶单群。

---

24. 证明：凡 455 阶群必为循环群。

证明　设群 G 的阶为 455，而 $455=5\cdot 7\cdot 13$。

由第三 Sylow 定理知，G 的 Sylow 7- 子群个数 $k_7\mid 455$ 且

$$k_7\equiv 1(\mathrm{mod}\ 7)$$

从而 $k_7=1$，即 Sylow 7- 子群只有一个，记为 P_7，则 $P_7\trianglelefteq G$。

同理若记 P_{13} 为 G 的 Sylow 13- 子群，则 P_{13} 惟一且 $P_{13}\trianglelefteq G$。

而 G 的 Sylow 5- 子群的个数 $k_5\mid 455$ 且

$$k_5\equiv 1(\mathrm{mod}\ 5)$$

则 $k_5=1$ 或 $k_5=91$。若 $k_5=91$，则 G 共有 $91\times 4=364$ 个 5 阶元素，而 P_7P_{13} 中含有 91 个阶与 5 互素的元，两类元素共有 455 个，即 G 的全部元素。

任取一个 Sylow 5- 子群 P_5，记 $P=P_5P_7$，则 $P\leqslant G$ 且 $|P|=35$，又

$$P_5\trianglelefteq P, P_7\trianglelefteq P, P_5\cap P_7=\{e\}$$

故由本章 §8 定理 5 得 $P=P_5\times P_7$，P 是一个 35 阶循环群，于是 G 包含一个 35 阶的元素，但 G 的所有元中没有 35 阶元，矛盾，故 $k_5=1$，即 P_5 惟一，$P_5\trianglelefteq G$。由本章 §8 定理 5，$G=P_5\times P_7\times P_{13}$，故 G 为循环群。

---

25. 设 G 是一个有限非可换单群，p 是一个素数，且 $p\mid |G|$，证明：G 的 Sylow p- 子群的个数 $k>1$。

证明　不妨设 P 是群 G 的一个 Sylow$p$- 子群。

若 $|G|=p^m$，则由本章 §9 第 13 题可知 G 的中心 C 的阶大于 1。又由题设 G 不可换知 $G\neq C$，故 C 为 G 的非平凡正规子群，从而 G 不是单群，矛盾。于是 $|G|$ 至少有两个互异的素数因子，故

$$\{e\}\subset P\subset G$$

因此 P 若是 G 惟一的 Sylow p- 子群，则 P 即为 G 的一个非平凡的正规子群，与题设中 G 为单群矛盾。所以这样的 P 不惟一，即 G 的 Sylow p- 子群的个数 $k > 1$。

---

26. 设 G 是一个有限群，$H \trianglelefteq G, K \trianglelefteq G$，又 P 是 G 的一个 Sylow p- 子群。证明：

(1) $|P \cap HK| = \dfrac{|P \cap H| \cdot |P \cap K|}{|P \cap H \cap K|}$；

(2) $P(H \cap K) = PH \cap PK$。

证明 (1) 不妨设 $|G| = p^s q$，其中 $p \nmid q$，p 为素数，又 P 为 G 的 Sylow p-子群，故 $|P| = p^s$。

又 $H \trianglelefteq G, K \trianglelefteq G$，故可设

$$|H| = p^m a,\ |K| = p^n b,\ |H \cap K| = p^t c \qquad ①$$

且

$$H \cap K \trianglelefteq G, HK \trianglelefteq G$$

其中 $p \nmid a, p \nmid b, p \nmid c, m \leqslant s, n \leqslant s, t \leqslant m, t \leqslant n$ 又由本章 §9 第 19 题知 $P \cap H, P \cap K, P \cap H \cap K$ 分别为 $H, K, H \cap K$ 的 Sylow p- 子群，故由式 ①

$$|P \cap H| = p^m,\ |P \cap K| = p^n,\ |P \cap H \cap K| = p^t$$

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = p^{m+n-t} \cdot d \qquad ②$$

其中 $d = \dfrac{ab}{c}$ 为正整数，$p \nmid d$。

又 $P \cap HK$ 也是 HK 的 Sylow$p$- 子群，由式 ②

$$|P \cap HK| = p^{m+n-t} = \frac{|P \cap H| \cdot |P \cap K|}{|P \cap H \cap K|} \qquad ③$$

(2) 由式 ③ 及

$$|PHK| = \frac{|P| \cdot |HK|}{|P \cap HK|},\ |P(H \cap K)| = \frac{|P| \cdot |H \cap K|}{|P \cap H \cap K|}$$

可得（多次应用第二章 §7 定理 5）

$$|PH \cap PK| = \frac{|PH| \cdot |PK|}{|PHK|} = \frac{|P| \cdot |H \cap K|}{|P \cap H \cap K|} = |P(H \cap K)|$$

又 $|G|=p^tq$ 有限，且 $P(H\cap K)\subseteq PH\cap PK$，故有

$$P(H\cap K)=PH\cap PK$$

27. 证明：当 $n\geqslant 3$ 时，全体 3- 循环是交代群 A_n 的一个生成系。

证明 $n=3$ 时，结论显然成立。

$n>3$ 时，由于 A_n 为偶置换群，而每一偶置换可分解成偶数个对换的乘积，故 A_n 中的每一元素必有形如如下的乘积形式，即

$$(ab)(cd)\text{ 或 }(ab)(ac)$$

其中 a,b,c,d 为 $\{1,2,\cdots,n\}$ 中互异的元素，又因为

$$(ab)(cd)=(abc)(bcd),(ab)(ac)=(acb)$$

所以 A_n 中的每一元素又是一些 3- 循环之积，从而 A_n 由全体 3- 循环生成。

28. 证明：$n\geqslant 5$ 时，n 次交代群 A_n 是单群。

证明 设 $N\lhd A_n$ 且 $N\neq\{(1)\}$，下证 $N=A_n$。

由上题结果，A_n 由全体 3- 循环生成，为证 $N=A_n$，只需证明 N 包含全体的 3- 循环。

设 $(i_1i_2i_3)$ 与 $(j_1j_2j_3)$ 是任意两个 3- 循环，作置换 σ，使

$$\sigma(i_k)=j_k\quad(k=1,2,3)$$

在其余数字上，σ 作适当定义。因为 $n\geqslant 5$，故在 i_1,i_2,i_3 之外至少还有两个数字 l,m。如果 σ 是偶置换，令 $\varphi=\sigma$，若 σ 是奇置换，令 $\varphi=\sigma(lm)$，则有

$$\varphi(i_1i_2i_3)\varphi^{-1}=(j_1j_2j_3)$$

由于所设 $N\lhd A_n$，故由上可知只要证明 N 包含一个 3- 循环，则 N 就包含了全部的 3- 循环。

在正规子群 N 中，对所有非单位的置换，取使 $\tau(i)=i$ 成立个数最多的置换 τ，并记 $\tau(i)=i$ 成立的个数为 s。因为对换为奇置换，所以 s 不可能为 $n-2$，必小于或等于 $n-3$。若 $s=n-3$，则 τ 就是一个 3- 循环，从而由上证明可知 $N=A_n$，得证。下证 $s<n-3$ 不可能成立。

若 $s<n-3$，把 τ 分解成不相交循环的乘积，按分解式中是否含有长度 $\geqslant 3$ 的循环进行分类，有以下两种可能：

$$\tau:123\cdots \quad ①$$

$$\tau:(12)(34)\cdots \quad ②$$

在情况①中，因为$(123j)$为奇置换，所以$s<n-4$，不妨设4，5在τ下满足$\tau(i)=i$。在情形①或②中，取$\varphi=(345)$，作$\varphi\tau\varphi^{-1}$，则

$$\varphi\tau\varphi^{-1}=(124\cdots)\text{ 或 }\varphi\tau\varphi^{-1}=(12)(45)\cdots$$

令$\tau_1=\tau^{-1}\varphi\tau\varphi^{-1}$，在①中，$\tau_1(1)=1$；在②中$\tau_1(1)=1,\tau_1(2)=2$。而在两种情形下，满足$\tau(i)=i$的点均满足$\tau_1(i)=i$。因此不论在哪种情形下，满足$\tau_1(i)=i$的点都比满足$\tau(i)=i$的点多，且$\tau_1\neq\{(1)\}$，这与$\tau$的取法矛盾，从而$\tau$一定是3-循环。

---

29. 证明：当$n\geqslant 5$时，n次对称群S_n不是可解群。

证明 由本章§9第28题知$n\geqslant 5$时A_n是单群，故只有

$$\{e\}\lhd A_n\lhd S_n$$

而$A_n/\{e\}\cong A_n$是非交换群，由本章§2第8题可解群定义可知S_n不是可解群。

---

30. 若一个n次置换是a_1个1-循环，a_2个2-循环，…，a_n个n-循环（不相连循环且每个数码都出现）之积，则称此置换有循环结构

$$[1^{a_1},2^{a_2},\cdots,n^{a_n}]$$

证明：两n次置换σ,τ共轭$\Leftrightarrow\sigma$与τ有相同的循环结构。

证明 "$\Rightarrow$" 若σ与τ共轭，则存在n次置换π使

$$\sigma=\pi\tau\pi^{-1}$$

设$\tau=(i_1i_2\cdots i_s)(j_1j_2\cdots j_t)\cdots(k_1k_2\cdots k_m)$为不相连的循环结构，由第二章§6定理5可得

$$\begin{aligned}\sigma&=\pi\tau\pi^{-1}\\&=(\pi(i_1)\pi(i_2)\cdots\pi(i_s))(\pi(j_1)\pi(j_2)\cdots\pi(j_t))\cdots(\pi(k_1)\pi(k_2)\cdots\pi(k_m))\end{aligned}$$

从而σ仍为不相连的循环之积，故σ与τ有相同的循环结构。

"$\Leftarrow$" 若σ与τ有相同的循环结构，其中

$$\sigma=(i_1)(i_2)\cdots(i_s)\cdots(j_1j_2\cdots j_t)\cdots$$

$$\tau=(i_1')(i_2')\cdots(i_s')\cdots(j_1'\,j_2'\cdots j_t')\cdots$$

故设

$$\pi = \begin{pmatrix} i_1 & i_2 & \cdots & i_s & \cdots & j_1 & j_2 & \cdots & j_t & \cdots \\ i_1' & i_2' & \cdots & i_s' & \cdots & j_1' & j_2' & \cdots & j_t' & \cdots \end{pmatrix}$$

即

$$\pi(i_1) = i_1', \cdots, \pi(i_s) = i_s', \cdots, \pi(j_1) = j_1', \cdots, \pi(j_t) = j_t', \cdots$$

从而

$$\begin{aligned} \pi\tau\pi^{-1} &= (\pi(i_1))\cdots(\pi(i_s))\cdots(\pi(j_1)\cdots\pi(j_t))\cdots \\ &= (i_1')\cdots(i_s')\cdots(j_1'\, j_2'\cdots j_t')\cdots \\ &= \sigma \end{aligned}$$

即 σ 与 τ 共轭。

---

31. 设 a 是群 G 中阶为 $m_1m_2\cdots m_n$ 的一个元素。证明：若正整数 $m_1, m_2, \cdots, m_n$ 两两互素，则 a 可惟一表示为

$$a = a_1a_2\cdots a_n$$

其中 a_i 都是 a 的方幂，且

$$|a_i| = m_i \quad (i = 1, 2, \cdots, n)$$

证明　对 n 用数学归纳法证明。

先证存在性。

$n = 1$ 时显然成立。设 $k < n-1$ 时命题成立，当 $k = n$ 时，记

$$m = m_1m_2\cdots m_{n-1}$$

依题意有 m 与 m_n 互素，即 $(m, m_n) = 1$，故存在整数 s 及 t，使

$$ms + m_nt = 1$$

若令 $a' = a^{m_nt}, a_n = a^{ms}$，则

$$a = a^{ms+m_nt} = a^{m_nt}\cdot a^{ms} = a'\cdot a_n$$

因为 $|a| = m_1m_2\cdots m_n = mm_n$，所以

$$|a'| = m_1m_2\cdots m_{n-1}, \quad |a_n| = m_n$$

从而由假设可得

$$a' = a_1a_2\cdots a_{n-1}$$

其中 a_i 都是 a' 的方幂，进而是 a 的方幂，且 $|a_i| = m_i (i = 1, 2, \cdots, n-1)$，因此

$$a = a'\cdot a_n = a_1a_2\cdots a_{n-1}a_n$$

其中 $|a_i|=m_i$，且每个 a_i 都是 a 的方幂（$i=1,2,\cdots,n$）。

下证惟一性。

$n=1$ 时显然成立，设 $k=n-1$ 时成立，$k=n$ 时，若

$$a=a_1a_2\cdots a_n=b_1b_2\cdots b_n$$

且 $|a_i|=|b_i|=m_i$，a_i 与 b_i 都是 a 的方幂（$i=1,2,\cdots,n$），设

$$a'=a_1a_2\cdots a_{n-1},b'=b_1b_2\cdots b_{n-1}$$

则由题意可知

$$|a'|=|b'|=m_1m_2\cdots m_{n-1}=m$$

令

$$a'^{-1}b'=a_nb_n{}^{-1}=c$$

故有

$$c^m=(a'^{-1}b')^m=e,c^{m_n}=(a_nb_n^{-1})^{m_n}=e$$

又由存在性证明中可知 $(m,m_n)=1$，于是 $c=e$ 为群 G 的单位元，从而

$$a'=b',a_n=b_n$$

又由假设可知 $a_i=b_i(i=1,2,\cdots,n-1)$，所以

$$a_i=b_i\quad(i=1,2,\cdots,n)$$

第四章　环与域

导读

一、基本要求

1. 理解环与域的定义，理解单位元、逆元、零因子的概念及性质，掌握消去律与零因子的关系。

2. 掌握环与域的性质，掌握整环、除环、域的结构，理解环——交换环、有单位元环和无零因子环——整环、除环——域的关系。

3. 熟练掌握子环、理想的定义及求法；理解理想子环及零理想、单位理想和主理想的构成，能够判断一个环是否是理想子环及主理想子环。

4. 理解并掌握剩余类环的结构，掌握环同态基本定理。

5. 掌握极大理想的性质及作用。

6. 了解商域的结构。

7. 了解多项式环的概念及性质。

8. 了解如何构造分式域。

9. 了解环直和的概念、性质及判定。

10. 了解非交换环的存在性及构造。

二、重点与难点

1. 环、整环、除环、域的基本概念；

2. 剩余类环的概念及结构；

3. 环同态基本定理；

4. 理想与极大理想的概念与性质；

5. 商域的结构。

知识点考点精要

一、环的概念

1. 定义

(1) 加群

一个交换群的代数运算叫做加法并用加号表示时，称为一个加群。

(2) 环

设非空集合 R 有两个代数运算，一个叫加法并用 $+$ 表示，另一个叫乘法并用 $\cdot$ 表示。

若满足

①R 对加法作成一个加群；

②R 对乘法满足结合律：

$$(ab)c = a(bc)$$

③ 乘法对加法满足左右分配律：

$$a(b+c) = ab + ac, \qquad (b+c)a = ba + ca$$

其中 a、b、c 为 R 中任意元素。则称 R 对这两个代数运算作成一个环。

注 数域 F 上的全体多项式的集合 $F[x]$、全体 n 阶方阵的集合以及一个向量空间的全体线性变换的集合，对各自通常的加法和乘法都作成环，分别称为数域 F 上的多项式环，n 阶全阵环和线性变换环。

(3) 交换环、有限环与环的阶

① 交换环

若环 R 的乘法满足交换律，即对 R 中任意元素 a，b 都有

$$ab = ba$$

则称 R 为交换(可换) 环，否则称为非交换(非可换) 环。

② 有限环

若环 R 只含有限个元素，则称 R 为有限环。否则称为无限环。

③ 阶

有限环 R 的元素的个数称为 R 的阶，记为 $|R|$。若 R 为无限环，则称

其阶为无限。

(4) 单位元

若环 R 中有元素 e，它对 R 中每个元素 a 都有

$$ea = a$$

则称 e 为环 R 的一个左单位元；

若环 R 中有元素 e'，它对 R 中每个元素 a 都有

$$ae' = a$$

则称 e' 为环 R 的一个右单位元。

若 $e \in R$ 且既是 R 的左单位元又是 R 的右单位元，则称 e 为 R 的单位元。

(5) 子环

设 S 是环 R 的一个非空子集，如果 S 对 R 的加法与乘法也作成一个环，则称 S 是 R 的一个子环，记为 $S \leqslant R$ 或 $R \geqslant S$。

(6) 全阵环

设 R 为任意环，称

$$\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \quad (a_{ij} \in R)$$

为环 R 上的一个 $m \times n$ 矩阵。当 $m = n$ 时，称 $\boldsymbol{A}$ 为环 R 上的一个 n 阶方阵。

环 R 上的全体 n 阶方阵关于方阵的加法与乘法作成一个环，记作 $R_{n\times n}$，并称为环 R 上的 n 阶全阵环。

(7) 循环环

环 R 关于其加法作成一个群，记作 $(R,+)$，并称为环 R 的加群。若加群 $(R,+)$ 是一个循环群，则称 R 是一个循环环。

注 ① 若 $(R,+) = \langle a \rangle$，则循环环 R 可表示为 $R = \{\cdots,-2a,-a,0,a,2a,\cdots\}$，$a^2 = ka$，$k$ 为整数。

② 若 a 在 $(R,+)$ 中的阶为 n，则 R 可表示为 $R = \{0,a,2a,\cdots,(n-1)a\}$，$a^2 = ka$，$0 \leqslant k \leqslant n-1$。

2. 环中元素的一些运算规则

(1) $0a = a0 = 0$，其中 0 是环 R 的零元；

(2)$(-a)b = a(-b) = -ab$;

(3)$(-a)(-b) = ab$;

(4)$c(a-b) = ca - cb$,$(a-b)c = ac - bc$;

(5)$(\sum_{i=1}^{m} a_i)(\sum_{j=1}^{n} b_j) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j$;

(6)$(ma)(nb) = (na)(mb) = (mn)(ab)$,其中 m,n 为任意整数。

注 环的乘法未必可换。

3. 子环的判定

环 R 的非空子集 S 作成子环的充要条件是:

$$a,b \in S \Rightarrow a-b \in S$$

$$a,b \in S \Rightarrow ab \in S$$

4. 全阵环 $R_{n\times n}$ 中元素可逆的判定

设 R 是一个有单位元的交换环,则 R 上 n 阶全阵环 $R_{n\times n}$ 的方阵 A 在 $R_{n\times n}$ 中可逆的充要条件是:A 的行列式 $|A|$ 在 R 中可逆。

5. 循环环的性质

(1)pq 阶环必为循环环,其中 p、q 为两个互异的素数。

(2) 循环环必为交换环。

(3) 循环环的子环也是循环环。

(4) 循环环的子加群必为子环。

二、环的零因子和特征

1. 零因子、特征及相关定义

(1) 左(右) 零因子

设 $a \neq 0, a \in R$,R 为环。若存在 $b \neq 0, b \in R$,使 $ab = 0$($ba = 0$),则称 a 为 R 的一个左(右) 零因子,左、右零因子统称为零因子。

(2) 正则元

若 $a \in R$,且 a 既不是左零因子又不是右零因子,则称 a 为 R 的正则元。

(3) 整环

无零因子的交换环称为整环。

(4) 特征

若(任意) 环 R 的元素(对加法) 有最大阶 n,则称 n 为环 R 的特征(或

特征数)，记为 char$R$；若环 R 的元素(对加法)无最大阶，则称 R 的特征是无限(或零)。

2. 无零因子环的重要性质

(1)(消去律) 在环 R 中，

① 当 a 不是左零因子时，则

$$ab = ac, a \neq 0 \Rightarrow b = c$$

② 当 a 不是右零因子时，则

$$ba = ca, a \neq 0 \Rightarrow b = c$$

(2) 环 R 中

① 若无左(右)零因子，则消去律成立。

② 若 R 中有一个消去律成立，则 R 中无左及右零因子，且另一个消去律也成立。

3. 环 R 特征的判定及环具有特殊特征的性质

(1) 设 R 是一个环，令

$$M = \{n \mid n \text{ 是正整数且对 } R \text{ 中任意 } a, na = 0\}$$

则

① 当 M 是空集时 R 的特征无限；

② 当 M 非空时，M 中最小的正整数就是环 R 的特征。

(2) 若 R 是一个无零因子环，且 $|R| > 1$，则

① R 中所有非零元素(对加法)的阶均相同；

② 若 R 的特征有限，则必为素数。

(3) 若环 R 有单位元，则单位元在加群$(R,+)$中的阶就是 R 的特征。

(4) 若环 R 是交换环，特征是素数 p，则任意 $a_i \in R(i = 1,2,\cdots,m)$，有

$$(a_1 + a_2 + \cdots + a_m)^p = a_1^p + a_2^p + \cdots + a_m^p$$

4. p- 环及其性质

(1) 定义

设 R 是一个阶大于 1 且特征为素数 p 的环。若任 $a \in R$ 均有

$$a^p = a$$

则称 R 是一个 p- 环。

(2) 性质(必要条件)

p- 环必为交换环。

5. 零化子

(1) 左(右) 零化子

设 R 为环,$S \subset R, S \neq \varnothing$。若存在 $a \in R$,使

$$aS = \{ax \mid x \in S\} = \{0\} \quad (Sa = \{xa \mid x \in S\} = \{0\})$$

则称 a 为 S 的一个左(右) 零化子,并简记为 $aS = 0(Sa = 0)$。

左、右零化子统称为零化子。

(2) 真零化子

非零的零化子称为真零化子。

6. 全阵环 $R_{n\times n}$ 中 n 阶方阵是零因子的条件

(1) 矩阵的秩

设 R 是一个有单位元的交换环,$|R|>1$。$\boldsymbol{A}$ 是环 R 上的一个 $m\times n$ 矩阵,$t=\min\{m,n\}$,又令 S_i 为由 A 中所有 $i(i=1,2,\cdots,t)$ 阶子式作成的 R 的子集。

① 若 S_1 有真零化子,则称矩阵 $\boldsymbol{A}$ 的秩为 0;

② 若 $S_1,S_2,\cdots,S_r$ 均无真零化子,但 S_{r+1} 有真零化子,则称矩阵 $\boldsymbol{A}$ 的秩为 r。

矩阵 $\boldsymbol{A}$ 的秩记为 $r(\boldsymbol{A})$,显见有 $0 \leqslant r(\boldsymbol{A}) \leqslant t$。

(2) 齐次线性方程组有非零解的条件

设 R 是一个有单位元的交换环,$|R|>1$,$\boldsymbol{A}$ 是 R 上的 $m\times n$ 矩阵,$\boldsymbol{x}=(x_1,x_2,\cdots,x_n)^{\mathrm{T}}, x_i(i=1,2,\cdots,n)\in R$,则 R 上齐次线性方程组 $\boldsymbol{Ax}=\boldsymbol{0}$ 在 R 中有非零解的充要条件是

$$r(\boldsymbol{A}) < n$$

(3)$R_{n\times n}$ 中方阵为零因子的条件

设 R 为有单位元的交换环,$|R|>1$,$\boldsymbol{A}\in R_{n\times n}$,则 $\boldsymbol{A}$ 是全阵环 $R_{n\times n}$ 的零因子的充要条件是 $|\boldsymbol{A}|$ 是 R 的零因子。

三、除环和域

1. 除环和域的定义

(1) 除环

设 R 是一个环，$|R|>1$，若 R 有单位元且每个非零元素都有逆元，则称 R 是一个除环(或体)。

(2) 域

可换除环称为域。

2. 除环和域的性质

(1) 除环和域没有零因子；

注　除环和域的特征只能是素数或无限。

(2) 有限除环必为域；

(3) 有限环若有非零元素不是零因子，则必有单位元，且每个非零又非零因子的元素都是可逆元；

(4) 阶大于 1 的有限环 R 若无零因子，则必为除环，进而为域；

(5) 设 R 是环且 $|R|>1$，则 R 是除环的充要条件是：对 R 中任意元素 $a\neq 0,b$，方程

$$ax=b(\text{或 } ya=b)$$

在 R 中有解。

注　(5) 可作为除环的等价定义。

3. 域中的公式运算规则

(1) $\dfrac{b}{a}=\dfrac{d}{c}\Leftrightarrow ad=bc$ ；

(2) $\dfrac{b}{a}+\dfrac{d}{c}=\dfrac{bc+ad}{ac}$ ；

(3) $\dfrac{b}{a}\cdot\dfrac{d}{c}=\dfrac{bd}{ac}$ ；

(4) $\dfrac{\frac{b}{a}}{\frac{d}{c}}=\dfrac{bc}{ad}$ 。

4. 子域与子除环

(1) 定义

设 F_1 是域(除环)F 的一个子集，且 $|F_1|>1$，若 F_1 对 F 的两个运算也作成一个域(除环)，则称 F_1 是 F 的一个子域(子除环)。

(2) 判定条件

设 F_1 是域 F 的一个子集，且 $|F_1|>1$。则 F_1 作成 F 的一个子域的充要条件是

$$a,b\in F_1\Rightarrow a-b\in F_1$$

$$a\neq 0,b\in F_1\Rightarrow \frac{b}{a}\in F_1$$

即 F_1 对"减法与除法"封闭。

5. 乘群的定义

设 R 是一个有单位元的环，则 R 的可逆元也称为 R 的单位；R 的全体可逆元(单位)作成的群，称为 R 的乘群或单位群，记作 R^* 或 $U(R)$。

四、环的同态与同构

1. 定义

(1) 同态映射

设 R 与 $\overline{R}$ 是两个环，若有一个 R 到 $\overline{R}$ 的映射 φ 满足对任 a、$b\in R$，有

$$\varphi(a+b)=\varphi(a)+\varphi(b)$$

$$\varphi(ab)=\varphi(a)\varphi(b)$$

则称 φ 为环 R 到 $\overline{R}$ 的一个同态映射。

(2) 同构映射

若 φ 是环 R 到 $\overline{R}$ 的一个同态映射，且 φ 为双射，则称 φ 为环 R 到 $\overline{R}$ 的一个同构映射。

(3) 环的同态

若存在一个从 R 到 $\overline{R}$ 的同态满射，则称 R 与 $\overline{R}$ 同态，记为 $R\sim\overline{R}$。

(4) 环的同构

若从 R 到 $\overline{R}$ 存在一个同构映射，则称 R 与 $\overline{R}$ 同构，记为 $R\cong\overline{R}$。

(5) 环的自同构

若从 R 到 R 存在一个同构映射 φ，则称 φ 为环 R 的一个自同构。

2. 环同态的性质

(1) 设 R 与 $\overline{R}$ 是各有两个代数运算的集合，且 $R\sim\overline{R}$。则当 R 是环时，$\overline{R}$ 也是一个环。

(2) 设 R 与 $\overline{R}$ 均为环，且 $R\sim\overline{R}$，则

① R 的零元的象是 $\overline{R}$ 的零元；

② R 的元素 a 的负元的象是 a 的象的负元；

③ R 为交换环时，$\overline{R}$ 也是交换环；

④ R 有单位元时，$\overline{R}$ 也有单位元，且单位元的象是单位元。

3. 同构的性质

设 R 与 $\overline{R}$ 是两个环，且 $R \cong \overline{R}$，则 R 是整环(除环、域)当且仅当 $\overline{R}$ 是整环(除环、域)。

4. 挖补定理

设 S 是环 R 的一个子环，且 S 与环 $\overline{S}$ 同构，即

$$R \geqslant S \cong \overline{S}$$

又若 $\overline{S} \cap (R-S) = \varnothing$，即 $\overline{S}$ 同 S 在 R 中的余集 $R-S$ 无公共元素，则存在环 $\overline{R}$，使

$$R \cong \overline{R} \quad , \quad \overline{S} \leqslant \overline{R}$$

五、模 n 剩余类环

1. 定义

(1) 模 n 剩余类环

任取正整数 n，令

$$Z_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$$

即 Z_n 为 n 个同余类的集合，任 $\overline{i}, \overline{j} \in Z_n$，规定

$$\overline{i} + \overline{j} = \overline{i+j}, \overline{i}\,\overline{j} = \overline{ij}$$

则 Z_n 关于这两个运算作成一个环，且是一个具有单位元的交换环，称之为以 n 为模的剩余类环，或简称模 n 剩余类环。

(2) 互素

$\overline{i} \in Z_n$，若类 $\overline{i}$ 中有一个整数与 n 互素，则这个类中所有整数均同 n 互素，因此称类 $\overline{i}$ 与 n 互素。

注　在类 $\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}$ 中，有且只有 $\varphi(n)$ 个类同 n 互素。

2. 性质

(1) 在 Z_n 中

① 非零元 $\overline{m}$ 如果与 n 互素，则为可逆元；

② 若非零元 $\overline{m}$ 不与 n 互素，则为零因子。

注 Z_n 的单位群是一个 $\varphi(n)$ 阶交换群。

(2) ① 若 p 是一个素数,则环 Z_p 是一个域;

② 若 p 是一个合数,则环 Z_p 有零因子,从而不是域。

(3) 若 m,n 是两个正整数,则

$$Z_m \sim Z_n \Leftrightarrow n \mid m$$

3. 循环环的重要结论

(1) 除去零乘环外,在同构意义下,循环环有且只有整数环及其子环以及剩余类环及其子环。

(2)① 循环环的任何子加群都是一个子环;

②n 阶循环环有且只有 $T(n)$ 个子环;

③ Z_n 有且只有 $T(n)$ 个子环。

六、理想

1. 理想及单环的定义

(1) 左理想

设 N 是环 R 的一个子加群,即对 N 中任意元素 $a,b,a-b\in N$。若有

$$r\in R,a\in N\Rightarrow ra\in N$$

则称 N 是环 R 的一个左理想。

(2) 右理想

设 N 是环 R 的一个子加群,若

$$r\in R,a\in N\Rightarrow ar\in N$$

则称 N 是环 R 的一个右理想。

(3) 理想

若 N 既是环 R 的左理想又是右理想,则称 N 是环 R 的一个双边理想,或称理想,记为 $N\lhd R$,否则记为 $N\ntriangleleft R$。

注 ① 交换环的每个左或右理想都是双边理想。

② 任意阶大于 1 的环,有两个平凡理想,即$\{0\}$ 与 R,其中 R 又称为环 R 的单位理想。其余理想(若存在) 称为非平凡理想或真理想。

(4) 单环

只有平凡理想的非零环称为单环。

2. 循环环的理想

N 是循环环 $R=\{\cdots,-2a,a,0,a,2a,\cdots\}$ 的一个理想，当且仅当 N 是 R 的一个子加群(子环)。

注 整数环及模 n 剩余类环 Z_n 的子加群、子环、理想都是一回事，特别 Z_n 有 $T(n)$ 个理想。

3. 除环和域的理想及相关结论

(1) 除环和域只有平凡理想，即它们都是单环。

(2) 设 R 是一个阶大于 1 的环，且除平凡理想外无其他左、右理想，则

① R 有单位元时，R 为除环；

② R 无单位元时，R 为素阶零乘环。

(3) 设 R 是一个阶大于 1 的整环，若 R 只有有限个理想，则 R 必为域。

4. 单环的性质

(1) 阶大于 1 的可换单环必为域或素阶零乘环。

(2) 设 R 是一个有单位元的环，$K \lhd R_{n\times n}$，则存在惟一的 $D \lhd R$，使 $K=D_{n\times n}$，即在有单位元的环 R 上全阵环 $R_{n\times n}$ 的理想都是 R 中某个理想上的全阵环。

(3) 设 R 是有单位元的环，且 $|R|>1$，则

$$R_{n\times n} \text{ 是单环} \Leftrightarrow R \text{ 是单环}$$

特别，除环和域上的全阵环都是单环。

5. 环 R 理想的构造

(1) 主理想的定义

设 R 是一个环，任取 $a\in R$，则 R 中包含 a 的所有理想的交也是 R 的一个理想，且是 R 的包含 a 的最小理想。这个理想记作 $\langle a\rangle$，并称作 R 的由 a 生成的主理想。

(2) 主理想的结构

$$\langle a\rangle=\{xa+ay+na+\sum_{i=1}^{m}x_iay_i \mid x,y,x_i,y_i\in R,n\in Z,m\in Z_+\}$$

(3) 某些特殊环中主理想的结构

① 若 R 为交换环，则

$$\langle a\rangle=\{ra+na \mid r\in R,n\in Z\}$$

② 若 R 有单位元，则

$$\langle a\rangle=\{\sum_{i=1}^{m}x_iay_i \mid x_i,y_i\in R,m\in Z_+\}$$

③ 若 R 为有单位元的交换环，则

$$\langle a\rangle=\{ra \mid r\in R\}$$

注 循环环的每个理想都是主理想。整数环及模 n 剩余类环 Z_n 的每个理想都是主理想。

6. 理想的和与积

(1) 设 $N_i(i=1,2,\cdots,m)$ 是环 R 的 m 个理想(子环)，则

$$N_1+N_2+\cdots+N_m=\{\sum_{i=1}^{m}x_i \mid x_i\in N_i,i=1,2,\cdots,m\}$$

也是环 R 的一个理想(子环)。

(2) 设 R 是环，$A\lhd R,B\lhd R$，则

$$AB=\{\text{有限和}\sum a_ib_i \mid a_i\in A,b_i\in B\}$$

也是环 R 的一个理想(子环)。

注 这里的 AB 为理想 A 与 B 的乘积，若类似于群的乘积规定

$$AB=\{ab \mid a\in A,b\in B\}$$

则 AB 一般不再是环 R 的理想。

7. 主理想概念的一个推广

设 R 为环，$a_i\in R(i=1,2,\cdots,m)$，则

$$\langle a_1\rangle+\langle a_2\rangle+\cdots+\langle a_m\rangle\lhd R$$

记为 $\langle a_1+a_2+\cdots+a_m\rangle$，并称为由元素 $a_1,a_2,\cdots,a_m$ 生成的理想(它是 R 中包含元素 $a_1,a_2,\cdots,a_m$ 的最小理想)。

七、商环与环同态基本定理

1. 商环的定义

设 R 是环，$N\lhd R$。则 R/N 对陪集的加法与乘法作成一个环，称为 R 关于 N 的商环，且

$$R\sim R/N$$

注 ① 加法 $(a+N)+(b+N)=(a+b)+N$；

② 乘法 $(a+N)(b+N)=ab+N$；

③R 到 R/N 的同态映射 $\varphi: a \longrightarrow a+N$ 称为 R 到商环的自然同态。

2. 同态的性质

在环 R 到 $\overline{R}$ 的同态映射下，则

(1)R 的子环(理想) 的象是 $\overline{R}$ 的一个子环(理想)；

(2)$\overline{R}$ 的子环(理想) 的逆象是 R 的一个子环(理想)。

3. 环第一同构定理(环同态基本定理)

设 R 与 $\overline{R}$ 是两个环，且 $R \sim \overline{R}$。则

(1) 同态核 N(即零元的全体逆象) 是 R 的一个理想；

(2)$R/N \cong \overline{R}$。

注 在同构意义下，任何环能且只能与其商环同构。

4. 环第二同构定理

设 R 是环且

$$H \leqslant R,\ N \lhd R$$

则

(1) $N \lhd (H+N), H \cap N \lhd H$；

(2)$N/(H \cap N) \cong (H+N)/N$。

5. 环第三同构定理

设 R 是环，且

$$A \lhd R, B \lhd R, A \leqslant B$$

则

$$B/A \lhd R/A$$

且

$$R/A/B/A \cong R/B$$

八、素理想与极大理想

1. 素理想与极大理想的定义

(1) 素理想

设 R 是一个交换环，$P \lhd R$，若

$$ab \in P \Rightarrow a \in P \text{ 或 } b \in P$$

其中，$a,b \in R$，则称 P 是 R 的一个素理想。

(2) 极大理想

设 R 为环，$N \trianglelefteq R$ 且 $N \neq R$。若除 R 和 N 外，R 中没有包含 N 的其他理想，则称 N 为环 R 的一个极大理想。

2. 素理想与极大理想的条件

(1) 交换环 R 中，P 是 R 的素理想 $\Leftrightarrow$ 商环 R/P 无零因子，即为整环。

(2) 整数环 Z 中，N 是 Z 的极大理想 $\Leftrightarrow N$ 是由素数生成的理想。

(3) 一般的环 R 中，N 是 R 的极大理想 $\Leftrightarrow$ 商环 R/N 是单环。

3. 关于有单位元交换环的讨论

(1) 有单位元的可换单环必为域；

(2) 设 R 是有单位元的交换环，$N \trianglelefteq R$，则

$$R/N \text{ 是域} \Leftrightarrow N \text{ 是环 } R \text{ 的极大理想}$$

注 必要性不要求有单位元。

(3) 有单位元的交换环的极大理想必为素理想。

九、环与域上的多项式环

1. 多项式环的定义

(1) 多项式

设 R 为有单位元的环，x 为一个记号(称为 R 上的未定元)，称形如

$$f(x) = a_0x^0 + a_1x + \cdots + a_nx^n \qquad (a_i \in R)$$

的表达式为环 R 上未定元 x 的多项式，其中 $a_i(i = 1,2,\cdots,n)$ 称为多项式的系数，系数全为 0 的多项式称为零多项式，记为 0。

(2) 多项式环

R 上未定元 x 的全体多项式关于多项式的加法与乘法作成一个环称为 R 上未定元 x 的多项式环，记为 $R[x]$。

2. 有单位元环 R 上多项式环 $R[x]$ 的性质

(1)R 与 $R[x]$ 的关系

①R 是 $R[x]$ 的一个子环；

②$R[x]$ 的单位元就是 R 的单位元；

③ $R[x]$ 是交换环 $\Leftrightarrow R$ 是交换环。

(2)R 是一个有单位元的环，则

$$R[x]\text{ 是整环}\Leftrightarrow R\text{ 是整环}$$

(3)$R[x]$ 中多项式的除法

设 R 是有单位元的环，则 $R[x]$ 中任意多项式 $f(x)$，$g(x)\neq 0$($g(x)$ 的最高项系数是 R 的一个可逆元)，在 $R[x]$ 中存在惟一多项式 $q_1(x)$，$r_1(x)$ 及 $q_2(x)$，$r_2(x)$，使

$$f(x)=g(x)q_1(x)+r_1(x)$$

$$f(x)=q_2(x)g(x)+r_2(x)$$

其中 $r_1(x)=0$ 或 $r_1(x)$ 次数 $<g(x)$ 次数；$r_2(x)=0$ 或 $r_2(x)$ 次数 $<g(x)$ 次数。并分别称 $q_1(x)$，$r_1(x)$ 与 $q_2(x)$，$r_2(x)$ 为 $f(x)$ 用 $g(x)$ 除所得的右商、右余式与左商、左余式。

3. 域 F 上多项式的根

(1) 设 F 是域 E 的一个子域，$a\in E$，则

$$a\text{ 是 }F\text{ 上多项式 }f(x)\text{ 的根}\Leftrightarrow(x-a)\mid f(x)$$

其中，x 是 E 上未定元。

(2) 设 F 是域 E 的一个子域，x 是 E 上未定元，则 F 上 n 次($n>0$)多项式 $f(x)$ 在 E 中根的个数(k 重根以 k 个计)不超过 $f(x)$ 的次数 n。

(3) 设 F 是域 E 的一个子域，F 上多项式 $f(x)$ 在 $E[x]$ 中可分成一次因子的乘积。则

$$f(x)\text{ 在 }E\text{ 中无重根}\Leftrightarrow(f(x),f'(x))=1$$

十、分式域(商域)

1. 定义

设 K 是包含整环 $R(|R|>1)$ 的一个域，则 K 中一切形如

$$\frac{b}{a}=a^{-1}b=ba^{-1}\quad(a,b\in R,a\neq 0)$$

的元素作成 K 的一个子域 F，它包含 R 为其子环。称 F 为 R 的分式域或商域。

2. 分式域的存在性

整环的分式域必存在。

3. 惟一性

同构的整环其分式域也同构。即在同构意义下整环的分式域存在且

惟一。

十一、环的直和

1. 定义

(1) 外直和

设 $R_i(i=1,2,\cdots,n)$ 是 n 个环，令

$$R=\{(a_1,a_2,\cdots,a_n)\mid a_i\in R_i\}$$

规定

$$(a_1,a_2,\cdots,a_n)=(b_1,b_2,\cdots,b_n)\Leftrightarrow a_i=b_i\quad(i=1,2,\cdots,n)$$

$$(a_1,a_2,\cdots,a_n)+(b_1,b_2,\cdots,b_n)=(a_1+b_1,a_2+b_2,\cdots,a_n+b_n)$$

$$(a_1,a_2,\cdots,a_n)\cdot(b_1,b_2,\cdots,b_n)=(a_1b_1,a_2b_2,\cdots,a_nb_n)$$

则 R 对上述二运算作成一个环，并称环 R 为环 $R_1,R_2,\cdots,R_n$ 的外直和。

(2) 内直和

设 $R_i(i=1,2,\cdots,n)$ 是环 R 的理想。若

①$R=R_1+R_2+\cdots+R_n$；

②R 中每个元素表为 $R_1,R_2,\cdots,R_n$ 中元素相加时，表示法惟一。

则称环 R 是子环 $R_1,R_2,\cdots,R_n$ 的内直和，简称直和，记作

$$R=R_1\oplus R_2\oplus\cdots\oplus R_n$$

(3) 直和项

设 R 为环，$N\trianglelefteq R$，若存在 N'，$N'\trianglelefteq R$ 使

$$R=N\oplus N'$$

则称 N 是环 R 的一个直和项。

2. 环是其子环的直和的充要条件

设 R 为环，$R_i\trianglelefteq R(i=1,2,\cdots,n)$，$R=R_1+R_2+\cdots+R_n$，则

$$R=R_1\oplus R_2\oplus\cdots\oplus R_n\Leftrightarrow \text{零元素表示法惟一}$$

$$\Leftrightarrow R_i\cap\sum_{j\neq i}^{n}R_j=\{0\}\quad(i=1,2,\cdots,n)$$

3. 直和的性质

(1) 若环 R 的理想 N 是 R 的一个直和项，则 N 的理想也是 R 的理想；

(2) 设环 $R=\sum\limits_{i=1}^{m}\oplus R_i$。

若$N_i \trianglelefteq R_i(i=1,2,\cdots,m)$，则

$$N_1 \oplus N_2 \oplus \cdots \oplus N_m \trianglelefteq R$$

反之，设 $N \trianglelefteq R$，则当 R 有单位元时存在$N_i \trianglelefteq R_i$，使

$$N = N_1 \oplus N_2 \oplus \cdots \oplus N_m$$

(3) 设 R 为环，$\mathrm{char}\ R = n$。若 $n = n_1 n_2$，且$(n_1, n_2) = 1$，则存在 R 的理想 R_1 和 R_2 使

$$R = R_1 \oplus R_2$$

且 $\mathrm{char}\ R_1 = n_1$，$\mathrm{char}\ R_2 = n_2$。

(4) 设环 $R = R_1 \oplus R_2$，又 $R_1 = N_1 \oplus N_2$，则

$$R = N_1 \oplus N_2 \oplus R_2$$

(5) 设环 R 的特征为 n，且

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$$

其中 p_i 是互异素数，$k_i \geqslant 1(i=1,2,\cdots,m)$，则存在环 R 的理想R_i，其特征为 $p_i^{k_i}$，且

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_m$$

十二、非交换环

1. 非交换的存在性

(1) 对任意整数 $n > 1$，总存在 n^2 阶非交换环。

其构造如下：

令 $R = (Z_n, +) \oplus (Z_n, +)$，加法为通常加法，乘法为

$$(x_1, y_1)(x_2, y_2) = (x_2 + y_2)(x_1, y_1)$$

则 R 是一个 n^2 阶非交换环。

(2) 对任意素数 p 和任意整数 $n > 1$，总存在 p^s 阶非交换环，其中 $s = \dfrac{n(n+1)}{2}$。

其构造为：域 Z_p 上一切 n 阶上三角矩阵作成的集合记为R，则 R 对方阵的普通加法与乘法作成一个 p^s 阶非交换环。

2. n 阶非交换环存在的充要条件

设 n 为大于 1 的整数，则存在 n 阶非交换环 $\Leftrightarrow n$ 有平方因子，即存在整

数 $d>1$ 使 $d^2\mid n$。

释疑解惑

一、对环的理解

1. 关于单位元

(1) 环 R 可能有单位元，也可能没有单位元，如整数环 Z 有单位元，而偶数环没有；也可能仅有左(右)单位元，没有右(左)单位元。如 $R=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix}\middle|a,b\in F\right\}$ 为域 F 上的环，有左单位元 $\begin{pmatrix}1&x\\0&0\end{pmatrix}(x\in F)$，但无右单位元，而 F 上形如 $\begin{pmatrix}a&0\\b&0\end{pmatrix}$ 的方阵环无左单位元，但有右单位元 $\begin{pmatrix}1&0\\x&0\end{pmatrix}(x\in F)$。

(2) 环 R 与其子环 S 的单位元的关系有

①R 有单位元，但 S 没有单位元；

如 R 为整数环，S 为偶数环。

②R 没有单位元而 S 有单位元；

如 $$R=\left\{\begin{pmatrix}a&0\\b&0\end{pmatrix}\middle|a,b\in Q\right\},S=\left\{\begin{pmatrix}a&0\\0&0\end{pmatrix}\middle|a\in Q\right\}$$

R 与 S 均为有理数域上的环且 S 为 R 的子环。但 R 没有单位元，而 S 有单位元 $\begin{pmatrix}1&0\\0&0\end{pmatrix}$。

③R 和 S 都有单位元，但两个单位元不同；

如取 R 为有理数域上的 2 阶全阵环，取 S 同 ② 中的 S，则 S 为 R 的子环且 R 的单位为 $\begin{pmatrix}1&0\\0&1\end{pmatrix}$，二者单位元不同。

④R 和 S 均有单位元且相同。

如 R 为实数域，S 为有理数域，则二者单位元均为 1。

2. 关于可逆元(单位)

环中的可逆元也称为单位,这一概念只有对有单位元1的环才有意义,应注意单位与单位元是两个不同的概念。

(1) 当环 R 与其子环 S 均有单位元且相同时,有下面的结论:

① 若 a 是子环 S 的单位,则 a 也是 R 的单位,且 a 在 S 中的逆元与 a 在 R 中的逆元一致。

② 若 a 是 R 的单位,即使 $a\in S$,a 也未必是 S 的单位。

如整数环 Z 是有理数域 Q 的子环,二者有相同的单位元。Q 中的任何非零元都是单位,但整数环 Z 中的单位仅有 ± 1。

(2) 当环 R 与其子环 S 均有单位元,但不同时,有下面的结论:

若 $a(\in S)$ 在 S 中是单位,则 a 必不是 R 的单位。即 R 的单位必不在 S 中。

证明 设 e 与 e' 分别为 R 及其子环 S 的单位元,且 $e\neq e'$,$a\in S$ 且 a 在 S 中可逆。下面证明 a 在 R 中不可逆。否则,若 a 是 R 的可逆元,则 a 不能是 R 的零因子。故由

$$a=e\cdot a=e'\cdot a$$

得

$$ea-e'a=0$$

即 $(e-e')a=0$,因 a 不是 R 的零因子,故

$$e-e'=0$$

即

$$e=e'$$

这与 $e\neq e'$ 矛盾,故 a 不能是 R 的可逆元(单位)。

(3) 当环 R 无单位元,子环 S 有单位元时,由于 R 无单位元,故不能说 S 中的单位 a 是否是 R 中的单位。当 R 有单位元,子环 S 无单位元时,也不能说 S 中的元素 a 是否是 R 中的单位。

3. 关于零因子

(1) 设环 R 的子环为 S,若 $a\in S$ 为 S 的零因子,则 a 也是 R 的零因子;若 a 不是 S 的零因子,则 a 未必不是 R 的零因子。

(2) 环 R 若有左零因子,则必有右零因子,反之亦然;

(3) 环 R 的一个元素如果是一个左(右)零因子,它不一定是一个右(左)零因子。

4. 关于环定义中的两个代数运算

环 R 中的两个代数运算,一个称为加法,另一个称为乘法。R 对加法作成群,对乘法满足结合律,乘法对加法满足左、右分配律。由此可知,这两个代数运算是有顺序的,它们的地位并不平等,若记加法为"+",乘法为"·",有时这个环也记为 $(R,+,\cdot)$(或称 R 对 $+$,$\cdot$ 作成一个环),而不能记作 $(R,\cdot,+)$。当然,加法与乘法也可采用其他符号来表示。

5. 环的分类

① 按环 R 中元素的个数是否有限可分为有限环与无限环;

② 按环 R 的乘法是否满足交换律可分为交换环和非交换环;

③ 按环 R 是否有单位元可分为有单位元环和无单位元环;

④ 按环 R 是否有零因子可分为含零因子环和无零因子环。其中无零因子的交换环称为整环;

⑤ 若环 R 的阶大于 1,R 有单位元且每个非零元均为单位,则称环 R 为除环,交换除环为域。

需注意的是,在不同的教材中零因子及整环等可能会有不同的定义方式,阅读时需注意对比。

二、除环的一个等价定义与群的一个等价定义的比较

1. 群的一个等价定义

半群 G 作成一个群 $\Leftrightarrow$ 方程 $ax=b$,$ya=b$ 在 G 中有解 $(a,b\in G)$。它要求两个方程均有解。

2. 除环的一个等价定义

阶大于 1 的环 R 是除环 $\Leftrightarrow$ 方程 $ax=b$(或 $ya=b$) 在 R 中有解 $(a,b\in R,a\neq 0)$。

它要求一个方程有解,在教材中利用方程 $ax=b$ 在环 R 中有解得到环 R 的全体非零元有右单位元且每个非零元都有右逆元,从而得 R 为除环。利用方程 $ya=b$ 在 R 中有解与此类似。

三、环的同态与同态基本定理

1. 在环的同态映射中，需注意环中两个代数运算的顺序。

2. 环 R 到环 $\overline{R}$ 的同态映射的保运算应是加法对加法，乘法对乘法，即

$$\varphi(a+b)=\varphi(a)\oplus\varphi(b)$$
$$\varphi(a\circ b)=\varphi(a)\,\bar{\circ}\,\varphi(b)$$

其中"$+$"与"$\circ$"，"$\oplus$"与"$\bar{\circ}$"分别表示 R 与 $\overline{R}$ 中的两个代数运算加法与乘法，通常的 R 与 $\overline{R}$ 中的代数运算都用同一符号表示。

3. 零因子在环同态映射下不具有传递性。由此，若 $R\overset{\varphi}{\sim}\overline{R}$，则 R 为整环未必有 $\overline{R}$ 是整环，R 不是整环但 $\overline{R}$ 可能是整环。

4. 环同态基本定理与群同态基本定理类似。它说明，环 R 的任一商环 R/N 都是 R 的同态象，而环 R 的任一同态象在同构的意义上只能是 R 的商环。从而由环 R 的任一理想 N 都可得到 R 的一个同态象。反之，由 R 的任一同态象都能得到 R 的一个理想（即满同态的核）。

另一方面，环 R 的同态象 R' 未必有与 R 完全相同的性质，但由环同态基本定理可知，在 R 中一定存在一个理想（满同态的核）N，使 R' 与 R/N 具有完全相同的性质。从而，若掌握了 R/N，就清楚了 R 的同态象 R'。

四、整数环 Z 与模 n 剩余类环 Z_n

1. Z 的任两个不同的子环，作为加群，它们都是无限循环群，因此，它们是同构的。但作为环，它们不同构。例如环 $\langle s\rangle$ 与 $\langle t\rangle$（其中 $s,t\in Z, s\neq\pm t, st\neq 0$）不同构。

2. Z_n 中的任两个不同的子环不同构

证明 ① 若 Z_n 的两个子环不同阶，结论显然成立。

② 设 R 为 Z_n 的任意 k 阶子环，则 $k\mid n$。而 $(Z_n,+)$ 为 n 阶循环群，故对 n 的每个正因数 k，$(Z_n,+)$ 有且仅有一个 k 阶子群，从而 Z_n 有且仅有一个 k 阶子环。于是可知，Z_n 的任两个不同子环不同构。

五、关于理想

1. 理想的传递性

设 A 是环 R 的理想，B 是环 A 的理想，若环 A 有单位元，则 B 必为 R

的理想。

证明 由子环具有传递性可知 B 为 R 的子环。任 $b \in B \subseteq A, r \in R$，则由

$$eb = be = b$$

及 $re, er \in A$（因 A 为 R 的理想）可知

$$rb = r(eb) = (re)b \in B, \quad br = (be)r = b(er) \in B$$

因此 B 为 R 的理想。

注 ①A 有单位元 e 仅是充分的，并非必要的。

如偶数环 A 是整数环 Z 的理想，而

$$B = \langle 4 \rangle = \{4n \mid n \in Z\}$$

既是偶数环的理想，又是 Z 的理想，但偶数环没有单位元。

② 一般而言，理想的理想未必是原环的理想。如 F 为任一域，令

$$B = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & a \\ 0 & 0 & 0 \end{pmatrix} \middle| a \in F \right\}, A = \left\{ \begin{pmatrix} 0 & 0 & x \\ 0 & 0 & y \\ 0 & 0 & 0 \end{pmatrix} \middle| x, y \in F \right\}$$

$$R = \left\{ \begin{pmatrix} a_1 & a_2 & a_3 \\ 0 & a_4 & a_5 \\ 0 & 0 & a_6 \end{pmatrix} \middle| a_i \in F, \quad i = 1, 2, \cdots, 6 \right\}$$

则 B 为 A 的理想，A 为 R 的理想，但 B 不是 R 的理想。

2. 主理想

由主理想的定义可知，主理想是环 R 的一类构造简单且易于掌握的理想，特别当 R 是有单位元的交换环时，$\langle a \rangle$ 的构造更为简单（它类似于整数环 Z 中的理想 $\langle a \rangle$ 由一切形如 na 的元构成，其中 $n \in Z$）。而主理想环是一个整环，且它的任一理想均为主理想。因此，主理想环较一般环更容易掌握其构造。

3. 极大理想与素理想

由任一有单位元的交换单环必是域可知，在任一有单位元的交换环中，任一极大理想必是素理想。

但一般的，(1) 素理想未必是极大理想。

如 $\{0\}$ 是整数环 Z 的素理想但不是极大理想，$\langle x \rangle$ 是 $Z[x]$ 中的素理想，但有 $\langle x \rangle \subseteq \langle 2, x \rangle \subsetneq Z[x]$。

(2) 在一般交换环中，极大理想未必是素理想。

如$\langle 4\rangle$是偶数环E中的极大理想，但$E/\langle 4\rangle=\{\overline{0},\overline{2}\}$中有零因子$\overline{2}$。

六、关于商域的构造

教材本章 §10 定理 2 通过具体构造分式域的方法指出了阶大于 1 的整环的分式域的存在性。方法如下。

令

$$M=\{(a,b)\mid a,b\in R,a\neq 0\}$$

用$\dfrac{b}{a}$表示M中元素(a,b)所在的等价类，设

$$F=\left\{\frac{b}{a}\,\middle|\,a,b\in R,a\neq 0\right\}$$

则F对普通分式的加法与乘法作成一个域，即为整环R的分式域。从而指出阶大于 1 的整环能够包含在一个域中，且分式域就是包含R的最小域。

七、关于环与域上的多项式

对于有单位元环上的多项式$f(x)$，不能采用通常的函数观点去处理。例如，R为有限环时，取$R=Z_2=\{\overline{0},\overline{1}\}$，此时，$R[x]$上的多项式$f(x)=x+\overline{1}$与$g(x)=x^2+\overline{1}$是两个不等的多项式，但$f(x)$与$g(x)$在$x=\overline{0}$时的值均为$\overline{1}$，在$x=\overline{1}$时的值均为$\overline{0}$，而$R=Z_2$只有$\overline{0}$与$\overline{1}$两个元素，因此，作为变数$x$的函数$f(x)$与$g(x)$又是相等的。所以，对于任意有单位元的环$R$，不能把多项式看作$x$的函数。

八、各种环之间的关系

各种环之间的关系如图 4-1 所示。

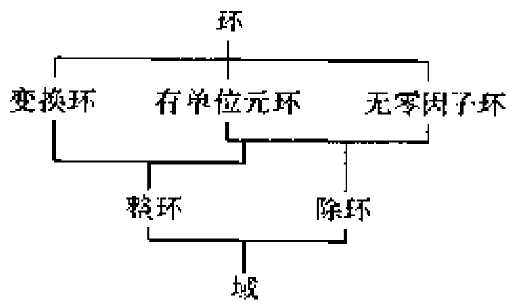

图 4-1

典型题精讲

1. 证明：二项式定理

$$(a+b)^n = a^n + C_n^1 a^{n-1}b + \cdots + C_n^i a^{n-i}b^i + \cdots + b^n$$

在交换环中成立。

证明　用数学归纳法证明。

$n=1$ 时显然成立。

设 $n=k$ 时结论成立。$n=k+1$ 时，由于乘法满足交换律，有

$$\begin{aligned}(a+b)^{k+1} &= (a+b)^k(a+b)\\ &= (a^k + C_k^1 a^{k-1}b + \cdots + C_k^i a^{k-i}b^i + \cdots + b^k)(a+b)\\ &= a^{k+1} + (C_k^1+1)a^k b + \cdots + (C_k^i + C_k^{i-1})a^{k-i+1}b^i + \cdots + b^{k+1}\end{aligned}$$

由于

$$C_k^i + C_k^{i-1} = C_{k+1}^i$$

故

$$(a+b)^{k+1} = a^{k+1} + C_{k+1}^1 a^k b + \cdots + C_{k+1}^i a^{k+1-i}b^i + \cdots + b^{k+1}$$

从而二项式定理在交换环中成立。

---

2. 设环 R 对加法作成一个循环群。证明：R 是交换环。

证明　设 R 作为加群是由元 a 生成的循环群，任取 $b,c\in R$，则

$$b = ma, c = na$$

其中 m,n 为整数，故

$$bc = (mn)a^2 = cb$$

因此 R 为交换环。

---

3. 设 R 是一个有单位元的环，类似于群可定义出其左(右)逆元：记单位元为 $1, a\in R$，若存在 $b\in R$，使 $ba=1$，则称 b 为 a 的左逆元。证明：若 a 在 R 中有且只有一个左逆元 b，则 a 是可逆元，且 $b=a^{-1}$。

证明　因为 $ba=1$，故

$$(ab-1+b)a = aba - a + ba = a - a + ba = 1$$

又 a 的左逆元惟一。于是

$$ab-1+b=b, ab=1$$

即 b 也是 a 的右逆元，从而 a 是可逆元且 $b=a^{-1}$。

---

4. 设 R 是有单位元 1 的环，a 是 R 的幂零元，证明：$1-a$ 是 R 的可逆元，并求其逆元。

证明　因为 a 是 R 的幂零元，故存在正整数 n，使 $a^n=0$，从而

$$(1-a)(1+a+a^2+\cdots+a^{n-1})=1-a^n=1$$

$$(1+a+a^2+\cdots+a^{n-1})(1-a)=1-a^n=1$$

故 $1-a$ 是可逆元且

$$(1-a)^{-1}=1+a+a^2+\cdots+a^{n-1}$$

---

5. 设 R 是有单位元 1 的有限交换环。证明：

(1)R 的元不是单位就是零因子；

(2) 含有限个元的整环是域。

证明　(1) 设 $|R|=n$，若 $a\in R$ 不是单位，则不存在 $x\in R$，使 $ax=1$，令

$$S=\{ar\mid r\in R\}$$

因为 $1\notin S$，故 S 为 R 的真子集，S 中元素个数小于 n。但形如 ar 的乘积可写出 n 个，故存在 $r_1,r_2\in R, r_1\neq r_2$ 使

$$ar_1=ar_2, a(r_1-r_2)=0$$

其中 $r_1-r_2\neq 0$，于是 a 为 R 的左零因子。

同理可证 a 为 R 的右零因子。

(2) 由(1) 知，有限整环 R 无零因子，故 R 的每个非零元都是可逆元，从而 R 为域。

---

6. 设 $F=\{a+b\sqrt{3}\mid a,b\in Q\}$。证明：$F$ 对普通加法和乘法作成一个域。

证明　易证 F 对普通加法和乘法作成一个整环。设 $a+b\sqrt{3}$ 为 F 的任一非零元。下面证明 $a+b\sqrt{3}$ 在 F 中有逆，从而 F 为一个域。

a,b 不能同时为零，故 $a^2-3b^2\neq 0$。否则 $a^2=3b^2$，若 $b=0$，可得 $a=$

0，与 $a+b\sqrt{3}$ 为非零元矛盾；若 $b\neq 0$，则 $\frac{a}{b}=\pm\sqrt{3}$，与 $\frac{a}{b}$ 为有理数矛盾。从而

$$(a+b\sqrt{3})\left(\frac{a}{a^2-3b^2}-\frac{b}{a^2-3b^2}\sqrt{3}\right)=1$$

$$\frac{a}{a^2-3b^2}-\frac{b}{a^2-3b^2}\sqrt{3}\in F$$

即 $a+b\sqrt{3}$ 在 F 中有逆，故 F 为一个域。

---

7. 证明：一个至少有两个元且无零因子的有限环 R 为除环。

证明 设

$$R^* = \{r \mid r\text{ 为 }R\text{ 的非零元}\}$$

由于 R 至少含两个元，故 $R^*\neq\varnothing$，且

①R^* 对乘法封闭(因 R 没有零因子)；

②R^* 的元对乘法适合结合律(因 R 的元对乘法适合结合律)；

③R^* 中消去律成立(因 R 中无零因子)。

又 R^* 中仅有有限个元，故 R^* 作成一个乘群。

设 1 为 R^* 的单位元，由于 $1\cdot 0=0\cdot 1=0$，故 1 也是 R 的单位元，因而 R^* 中元在 R^* 中的逆与在 R 中的逆是一致的，所以 R 为一个除环。

---

8. 证明：有理数域 Q 是域 $Q(\mathrm{i})=\{a+b\mathrm{i}\mid a,b\in Q\}$ 的惟一真子域。

证明 Q 显然是 $Q(\mathrm{i})$ 的一个真子域，下证惟一性。

不妨设 F 是 $Q(\mathrm{i})$ 的任一子域，则 F 中含有一个非零元 a，从而含有元素 $a^{-1}a=1$。从而 F 含有一切整数和一切有理数，因此有

$$Q\subseteq F\subseteq Q(\mathrm{i})$$

若 $F\neq Q$，则至少存在一个数

$$a+b\mathrm{i}\in F$$

其中 $a,b\in Q,b\neq 0$，故

$$a+b\mathrm{i}-a=b\mathrm{i}\in F,\quad b^{-1}b\mathrm{i}=\mathrm{i}\in F$$

因此 F 含有一切 $a+b\mathrm{i}$，所以 $F=Q(\mathrm{i})$，即 Q 是 $Q(\mathrm{i})$ 的惟一真子域。

9. 设 I 和 J 为环 R 的左(右、双边)理想,则 $I+J=\{u+v \mid u\in I, v\in J\}$ 是 R 的左(右、双边)理想。

证明 不妨设 I 和 J 是 R 的左理想,则任

$$a=u_1+v_1, b=u_2+v_2\in I+J, u_i\in I, v_i\in J \quad (i=1,2)$$

及任 $r\in R$,有

$$a-b=(u_1+v_1)-(u_2+v_2)=(u_1-u_2)+(v_1-v_2)\in I+J$$

$$ra=r(u_1+v_1)=ru_1+rv_1\in I+J$$

所以 $I+J$ 是 R 的左理想。

同理可证当 I 和 J 是 R 的右(双边)理想时,$I+J$ 是 R 的右(双边)理想。

---

10. 设 Z 是整数环,则 $\langle 4,9\rangle=\langle 1\rangle$。

证明 显见 $\langle 1\rangle=Z$,又

$$1=(-2)\times 4+9\in\langle 4,9\rangle$$

从而 $\langle 4,9\rangle=Z$,所以

$$\langle 1\rangle=\langle 4,9\rangle$$

---

11. 设 R 为无零因子环(既无左零因子,又无右零因子)。若 $e(\neq 0)\in R$ 满足条件 $e^2=e$,证明:e 为环 R 的单位元。

证明 任 $x\in R$

$$e(ex-x)=e^2x-ex=ex-ex=0$$

即

$$e(ex-x)=0$$

由于 R 无左零因子且 $e\neq 0$,故有

$$ex-x=0, ex=x$$

同理有

$$(x-xe)e=xe-xe^2=xe-xe=0$$

即 $(x-xe)e=0$,由 R 无右零因子且 $e\neq 0$ 得

$$x-xe=0, xe=x$$

从而由上可知,e 为环 R 的单位元。

---

12. 找出 $Z_6=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$ 的所有理想。

解 首先,任一理想必包含零元 $\bar{0}$;

另一方面,若 Z_6 的理想 N 包含单位元 $\bar{1}$,则有 $N=Z_6$;若 N 包含 $\bar{5}$,由于 $\bar{0}-\bar{5}=\bar{1}$,故 $N=Z_6$。

又由于

$$\bar{2}+\bar{3}=\bar{5},\ \bar{3}+\bar{4}=\bar{1}$$

所以当 Z_6 的理想 N 同时包含 $\bar{2}$ 和 $\bar{3}$,或同时包含 $\bar{3}$ 和 $\bar{4}$ 时,也必有 $N=Z_6$。

从而由上可知 Z_6 除平凡理想 Z_6 和 $\{\bar{0}\}$ 外,只有 $\{\bar{0},\bar{3}\}$ 及 $\{\bar{0},\bar{2},\bar{4}\}$。

习题全解

§1 环的定义(P155)

1. 设 R 为实数集,问:R 对数的普通加法以及新规定的乘法

$$a\circ b=|a|b$$

是否作成环?

解 只需验证乘法 $\circ$ 满足结合律及左、右分配律。

$$(a\circ b)\circ c=(|a|b)\circ c=|a||b|c$$
$$a\circ(b\circ c)=a\circ(|b|c)=|a||b|c$$

即结合律满足。

$$a\circ(b+c)=|a|(b+c)=|a|b+|a|c=a\circ b+a\circ c$$

即左分配律满足。

$$(b+c)\circ a=|b+c|a,\ b\circ a+c\circ a=|b|a+|c|a$$

由于 $|b+c|\leqslant|b|+|c|$,故可知当 b 与 c 异号时乘法的右分配律不满足,从而不能作成环。

---

2. 数域 F 上一切形如

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

的方阵对普通加法和乘法是否作成环?是否可换和有单位元?哪些元素有逆元?

解 由方阵的加法及乘法的性质可知 F 上一切形如$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$的方阵作成环，且任 $x \in F$，

$$\begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

可知一切形如$\begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix}$的方阵为左单位元，但不是右单位元，从而单位元不存在，因此环中元素不可逆。

又显见

$$\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$$

二者不等，故此环不可换。

---

3. 设 R 为所有有理数对(x_1, x_2)作成的集合，加法与乘法分别为

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$
$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$$

问：R 是否作成环？是否可换和有单位元？哪些元素有逆元？

解 显见 R 对加法作成群，对乘法满足结合律。又

$$\begin{aligned}(a_1, a_2)((b_1, b_2) + (c_1, c_2)) &= (a_1, a_2)(b_1 + c_1, b_2 + c_2) \\ &= (a_1(b_1 + c_1), a_2(b_2 + c_2)) \\ (a_1, a_2)(b_1, b_2) + (a_1, a_2)(c_1, c_2) &= (a_1 b_1, a_2 b_2) + (a_1 c_1, a_2 c_2) \\ &= (a_1(b_1 + c_1), a_2(b_2 + c_2))\end{aligned}$$

故 R 的乘法对加法满足左分配律，同理可得也满足右分配律。又因为

$$(a_1, a_2)(b_1, b_2) = (b_1, b_2)(a_1, a_2) = (a_1 b_1, a_2 b_2)$$

因此 R 作成一个交换环。

显然

$$(1,1)(a_1, a_2) = (a_1, a_2)(1,1) = (a_1, a_2)$$

故$(1,1)$为此环的单位元，从而若

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2) = (1,1)$$

则必 $b_i = a_i^{-1}$ 且 $a_i \neq 0 (i = 1,2)$，即当 $a_1 a_2 \neq 0$ 时，(a_1, a_2)有逆元(a_1^{-1}, a_2^{-1})，当 $a_1 a_2 = 0$ 时(a_1, a_2)无逆元。

4. 如果环 R 中的元素 a 满足 $a^2 = a$，则称 a 为 R 的幂等元。如果环 R 中每个元素都是幂等元，则称 R 为布尔(G. Boole, 1815 ~ 1864) 环。证明：布尔环是交换环，而且其中任何元素 a 都有

$$a + a = 0$$

证明 任 $a,b \in R$，则由 R 中每个元为幂等元知

$$(a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2 = a + b + ab + ba$$

$$(a+b)^2 = a + b$$

从而 $ab + ba = 0$。若令 $b = a$，则有

$$a^2 + a^2 = 0，即\ a + a = 0$$

故得 $a = -a$，又由 $ab + ba = 0$ 知

$$ba = -ab$$

于是有

$$ba = -(-a)b = ab$$

所以布尔环 R 又是交换环。

---

5. 证明：加群 G 的全体自同态映射对以下运算

$$(\sigma + \tau)a = \sigma a + \tau a$$

$$(\sigma\tau)a = \sigma(\tau a) \quad (\forall a \in G)$$

(σ、τ 为 G 的自同态映射) 作成一个有单位元的环。

称这个环为加群 G 的自同态环。

证明 设 G 的全体自同态映射作成的集合为 R，显然零同态 $\theta \in R$，$R \neq \varnothing$。

先证明 R 对题设中的加法作成群。

任 $\sigma, \tau, \pi \in R$，$a \in G$，则

$$(\theta + \sigma)a = \theta a + \sigma a = \sigma a$$

$$(-\sigma + \sigma)a = -\sigma a + \sigma a = 0$$

$$\begin{aligned}((\sigma + \tau) + \pi)a &= (\sigma + \tau)a + \pi a = (\sigma a + \tau a) + \pi a \\ &= \sigma a + (\tau a + \pi a) = \sigma a + (\tau + \pi)a \\ &= (\sigma + (\tau + \pi))a\end{aligned}$$

从而由 a 的任意性

$$(\sigma + \tau) + \pi = \sigma + (\tau + \pi)$$

$$\theta+\sigma=\sigma$$
$$-\sigma+\sigma=\theta$$

即 R 对题设中定义的加法满足结合律，存在零元及负元，故 R 作成加群。

下证 R 对乘法满足结合律，乘法对加法满足左、右分配律。

$$\begin{aligned}((\sigma\tau)\pi)a &= (\sigma\tau)(\pi a)=\sigma(\tau(\pi a))\\ &= \sigma((\tau\pi)a)=(\sigma(\tau\pi))a\end{aligned}$$
$$\begin{aligned}(\sigma(\tau+\pi))a &= \sigma((\tau+\pi)a)=\sigma(\tau a+\pi a)\\ &= \sigma(\tau a)+\sigma(\pi a)=(\sigma\tau)a+(\sigma\pi)a\end{aligned}$$
$$\begin{aligned}((\tau+\pi)\sigma)a &= (\tau+\pi)(\sigma a)=\tau(\sigma a)+\pi(\sigma a)\\ &= (\tau\sigma)a+(\pi\sigma)a\end{aligned}$$

从而由 a 的任意性有

$$(\sigma\tau)\pi=\sigma(\tau\pi)$$
$$\sigma(\tau+\pi)=\sigma\tau+\sigma\pi$$
$$(\tau+\pi)\sigma=\tau\sigma+\pi\sigma$$

从而综上可知 R 作成一个环。

若设恒等自同构为 τ，则对任 $\sigma\in R$，显见有

$$\sigma\tau=\tau\sigma=\sigma$$

故恒等自同构为环 R 的单位元。

---

6. 证明：对有单位元的环来说，其加法满足交换律可以由环定义中其它条件推出。

证明 设 e 为环 R 的单位元，任 $a,b\in R$，若 $a+b=b+a$，则环 R 对加法满足交换律。又

$$\begin{aligned}(a+b)-(b+a) &= e(a+b)-e(b+a)\\ &= e(a+b)+(-e)(b+a)\\ &= ea+eb+(-e)b+(-e)a \quad \text{（左分配律）}\\ &= ea+(e+(-e))b+(-e)a\\ &\qquad\qquad \text{（右分配律，加法的结合律）}\\ &= ea+0+(-e)a \quad \text{（对加法作成群）}\\ &= (e+(-e))a \quad \text{（右分配律）}\\ &= 0\end{aligned}$$

从而 $a+b=b+a$，即 R 中的加法满足交换律。

---

7. 设环 R 有单位元(用 1 表示)，又 $a,b\in R$。证明：如果 $a+b=ab$ 且 $1-a$ 在 R 中有逆元，则 $ab=ba$。

证明 由 $a+b=ab$ 可得

$$1=ab-(a+b)+1=(1-a)(1-b)$$

又 $1-a$ 可逆，故 $(1-a)^{-1}=1-b$，从而 $(1-b)(1-a)=1$，即

$$\begin{aligned}1=(1-b)(1-a)&=ba-(a+b)+1\\&=ba-ab+1\end{aligned}$$

于是有 $ba-ab=0$，即 $ab=ba$。

---

8. 证明：循环环必是交换环，并且其子环也是循环环。

证明 不妨设循环环

$$R=\{\cdots,-2a,-a,0,a,2a,\cdots\}$$

且 $a^2=ka$，k 为整数。任意的 $x,y\in R$，则存在整数 s,t，使

$$x=sa,y=ta$$

于是

$$xy=sta^2=stka=yx$$

即 R 为交换环，又因为循环群的子群仍为循环群，故循环环的子环仍为循环环。

§2 环的零因子和特征(P164)

1. 证明：

(1) 若环 R 有正则元，则其全体正则元对乘法作成一个半群。

(2) 环 R 的元素 $a\neq 0$ 是正则元，当且仅当由 $axa=0$ 可得 $x=0$。

证明 (1) 不妨设 S 为 R 中的全体正则元作成的集合，故只需证明 S 对于乘法封闭。

任 $a,b\in S$，有 $ab\neq 0$，若 $c\in R$，使

$$(ab)c=0,a(bc)=0$$

因为 a 为正则元，故 $bc=0$，又因 b 为正则元，故 $c=0$。即 ab 不是零因子，故 $ab\in S$，S 对乘法作成半群。

(2)"⇒"　设 $a \in R, a \neq 0$ 是正则元且 $axa = 0$，故 $a(xa) = 0$，由 a 为正则元可得

$$xa = 0$$

进而

$$x = 0$$

"⇐"　设 $a \in R, a \neq 0$，若 $ab = 0$，则 $aba = 0$，从而由条件知 $b = 0$；同理，若 $ba = 0$，则同样由 $aba = 0$ 可得 $b = 0$，即 a 不是零因子，为正则元。

---

2. 设环 R 有左单位元 e。证明：如果 R 没有右零因子，则 e 是环 R 的单位元。

证明　若 $e = 0$，则易得 $R = \{0\}$，e 显然是 R 的单位元。若 $e \neq 0$，则

$$0 = xe - xe = (xe - x)e$$

及 R 中无右零因子，故必 $xe - x = 0$，即 $xe = x$，即 e 也是右单位元，从而 e 为 R 的单位元。

---

3. 证明：数域 F 上 n 阶全阵环的元素 $\boldsymbol{A} \neq \boldsymbol{O}$ 若不是零因子，就是可逆元（即可逆方阵）。

证明　设数域 F 上的 n 阶全阵环为 $M_n(F)$。任 $\boldsymbol{A} \in M_n(F)$ 且 $\boldsymbol{A} \neq \boldsymbol{O}$，若 $|\boldsymbol{A}| \neq 0$，则存在可逆方阵 $\boldsymbol{A}^{-1}$，即 $\boldsymbol{A}$ 为 $M_n(F)$ 中的可逆元。

若 $|\boldsymbol{A}| = 0$，则齐次线性方程组 $\boldsymbol{Ax} = \boldsymbol{0}$ 有非零解，设 $b = (b_1, b_2, \cdots, b_n)^{\mathrm{T}}$ 为 $\boldsymbol{Ax} = \boldsymbol{0}$ 的一组非零解，以 b 为一列其余各列全为 0 构造一个 n 阶方阵 $\boldsymbol{B}$，则 $\boldsymbol{B} \neq \boldsymbol{O}$ 且 $\boldsymbol{AB} = \boldsymbol{O}$，从而 $\boldsymbol{A}$ 为 $M_n(F)$ 的零因子。

---

4. 证明：交换环的全体幂零元作成一个子环。

证明　设 S 是交换环 R 的所有幂零元的集合。由 $0 \in S$ 知 $S \neq \varnothing$。任 $a, b \in S \subseteq R$，则存在正整数 m, n，使

$$a^m = b^n = 0$$

从而由 R 可交换知

$$\begin{aligned}(a-b)^{m+n} &= a^{m+n} - C_{m+n}^1 a^{m+n-1} b + \cdots + (-1)^k C_{m+n}^k a^{m+n-k} b^k + \cdots + \\ &\quad (-1)^{m+1} b^{m+1} \\ &= 0\end{aligned}$$

$$(ab)^{mn} = a^{mn} b^{mn} = 0$$

即 $a - b$ 与 ab 都是 R 的幂零元，故 $a - b, ab \in S$，S 是 R 的子环。

5. 设 a 是环 R 的一个幂零元。证明：若有正整数 $n>1$ 使 $a^n=a$，则 $a=0$。

证明 因 a 为环 R 的一个幂零元，故存在一个最小的正整数 m，使 $a^m=0$。

若 $1<n<m$，令

$$m=ns+t$$

其中 $0\leqslant t<n$，从而由 $a^n=a$ 可知

$$0=a^m=a^{ns+t}=a^{ns}a^t=a^{s+t}$$

但由 $n>1$ 可知 $0<s+t<m$，故上式与 m 是使 $a^m=0$ 成立的最小的正整数矛盾。所以由上知 $n\geqslant m$，令

$$n=mq+r$$

其中 $0\leqslant r<m$，于是由 $a^m=0$ 知

$$a=a^n=a^{mq+r}=a^{mq}\cdot a^r=0$$

---

6. 设 $Z_{n\times n}$ 为整数环 Z 上的 $n(n>1)$ 阶全阵环。举例给出其子环 S_1，S_2 除共同满足 $S_1\subset S_2\subset Z_{n\times n}$，外，并分别满足：

(1) S_1 与 S_2 都有单位元，但不相等；

(2) S_1 与 S_2 有相同的单位元；

(3) S_1 有单位元，S_2 无单位元；

(4) S_1 无单位元，S_2 有单位元；

(5) S_1 与 S_2 都无单位元。

解 (1) S_1 为所有形如 $\begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$ 的方阵构成的集合，则 S_1 为 $Z_{n\times n}$ 的子环，其中有单位元 $\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$；

S_2 为所有形如 $\begin{pmatrix} x_1 & 0 & \cdots & 0 \\ 0 & x_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & x_n \end{pmatrix}$ 的方阵构成的集合，则 S_2 为 $Z_{n\times n}$ 的

子环，其中有单位元$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$。

(2)S_1 为所有形如$\begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & x & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & x \end{pmatrix}$的方阵构成的集合，则 S_1 为 $Z_{n\times n}$ 的子环，其中有单位元$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$；

S_2 为所有形如$\begin{pmatrix} x_1 & 0 & \cdots & 0 \\ 0 & x_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & x_n \end{pmatrix}$的方阵构成的集合，则 S_2 为 $Z_{n\times n}$ 的子环，其中有单位元$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$。

(3)S_1 为所有形如$\begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$的方阵构成的集合，则 S_1 为 $Z_{n\times n}$ 的子环，其中有单位元$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$；

S_2 为所有形如$\begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ x_n & 0 & \cdots & 0 \end{pmatrix}$的方阵构成的集合，则 S_2 中无单位元。

(4) S_1 为所有形如$\begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ x_n & 0 & \cdots & 0 \end{pmatrix}$的方阵构成的集合，则 S_1 中无单位元；

S_2 为所有形如$\begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & y_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ x_n & 0 & \cdots & y_n \end{pmatrix}$的方阵构成的集合，则 S_2 为 $Z_{n\times n}$ 的子环，其中有单位元$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$。

(5) S_1 为所有形如$\begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$的方阵构成的集合，$S_2$ 为所有形如$\begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ x_n & 0 & \cdots & 0 \end{pmatrix}$的方阵构成的集合，则 $S_1 \subset S_2$ 且均为子环，但它们没有单位元。

---

7. 设 R 是一个无零因子的环。证明：若 $|R|$ 为偶数，则 R 的特征必为 2。

证明 不妨记 R_+ 为 R 的加群，则由第二章 §2 第 4 题知 R_+ 中存在 2 阶元（且个数为奇数），从而由定理 3 知 R_+ 中除非零元外，其余元素均为 2 阶元，故 R 的特征为 2。

---

8. 证明：p-环无非零幂零元。

分析 由上面的第 5 题即可得到。

证明 （略）

§3 除环和域（P170）

1. 证明域中元素满足分式运算规则(1) ~ (4)。

即证明下列四式成立：

(1) $\frac{b}{a}=\frac{d}{c}\Leftrightarrow ad=bc$；

(2) $\frac{b}{a}+\frac{d}{c}=\frac{bc+ad}{ac}$；

(3) $\frac{b}{a}\cdot\frac{d}{c}=\frac{bd}{ac}$；

(4) $\dfrac{\frac{b}{a}}{\frac{d}{c}}=\frac{bc}{ad}$

证明 (1) 两边同乘以 ac，由可换性得

$$\frac{b}{a}=\frac{d}{c}\Rightarrow ac\frac{b}{a}=ac\frac{d}{c}\Rightarrow bc=ad$$

且由消去律在域内成立（域内无零因子），得

$$\frac{b}{a}\neq\frac{d}{c}\Rightarrow ac\frac{b}{a}\neq ac\frac{d}{c}\Rightarrow bc\neq ad$$

反之亦然。

(2) 左边乘以 ac 得

$$\left(\frac{b}{a}+\frac{d}{c}\right)ac=\frac{b}{a}ac+\frac{d}{c}ac=bc+ad$$

右边乘以 ac 得

$$\left(\frac{bc+ad}{ac}\right)ac=bc+ad$$

从而

$$\frac{b}{a}+\frac{d}{c}=\frac{bc+ad}{ac}$$

(3) 左边 $=\frac{b}{a}\cdot\frac{d}{c}=ba^{-1}\cdot dc^{-1}=bda^{-1}c^{-1}$

$$=bd(ca)^{-1}=bd(ac)^{-1}=\frac{bd}{ac}$$

(4) $\frac{bc}{ad}=bc(ad)^{-1}=bcd^{-1}a^{-1}$

$$=ba^{-1}cd^{-1}=ba^{-1}(dc^{-1})^{-1}=\frac{ba^{-1}}{dc^{-1}}=\frac{\frac{b}{a}}{\frac{d}{c}}$$

---

2. 证明本节定理 4。

证明 若 F_1 为 F 的子域，则任 $a,b\in F_1$，有 $a-b\in F_1$ 且 $a\neq 0$ 时，$a^{-1}\in F_1$，从而 $a^{-1}b=ba^{-1}=\frac{b}{a}\in F_1$。即任 $a,b\in F_1$，有 $a-b\in F_1$ 且 $a\neq 0$ 时 $\frac{b}{a}\in F_1$。

反之 $a\neq 0$ 时取 $b=a$，则 $1\in F_1$，知 F_1 中有单位元，进而任 $a\neq 0$，$a\in F_1$，$\frac{1}{a}=a^{-1}\in F_1$，即 F_1 中任非零元均可逆。任 $a,b\in F_1$，当然有 a，$b\in F$，故 $ab=ba$，即可换，从而由本章 §1 定理 1 知 F_1 为域 F 的子域。

---

3. 证明：域和其子域有相同的单位元。

证明 设 F_1 为域 F 的子域，$1'$ 为 F_1 的单位元，1 为 F 的单位元。任取 $a\neq 0$，$a\in F_1$，则由 F_1 为域可知 $a^{-1}\in F_1$ 且 $aa^{-1}=1'$。又 $a\in F$ 及 F 为域故也有 $a^{-1}\in F$，$aa^{-1}=1$，从而

$$1=aa^{-1}=1'$$

故域 F 及其子域 F_1 具有相同的单位元。

---

4. 设 α、β、γ 是三个四元数。证明：

$$(\alpha\beta-\beta\alpha)^2\gamma=\gamma(\alpha\beta-\beta\alpha)^2$$

证明 令 $t=(\alpha\beta-\beta\alpha)^2$，只需证 $t\gamma=\gamma t$，依题意设

$$\alpha=a_0+a_1i+a_2j+a_3k$$
$$\beta=b_0+b_1i+b_2j+b_3k$$

由四元数乘法可得

$$\alpha\beta-\beta\alpha=2(a_2b_3-a_3b_2)i+2(a_3b_1-a_1b_3)j+2(a_1b_2-a_2b_1)k$$

又因为若 $\Delta=ai+bj+dk$，则 $\Delta^2=-a^2-b^2-c^2$，从而

$$\begin{aligned}t&=(\alpha\beta-\beta\alpha)^2\\&=-4[(a_2b_3-a_3b_2)^2+(a_3b_1-a_1b_3)^2+(a_1b_2-a_2b_1)^2]\end{aligned}$$

为一实数，所以它同任一四元数可换，即 $t\gamma=\gamma t$。

---

5. 证明：(1) 集合 $R=\left\{\begin{pmatrix}a&2b\\b&a\end{pmatrix}\middle|a,b\in \text{数域 } F\right\}$

关于方阵的普通加法与乘法作成一个有单位元的交换环。又问：单位群 $R^*=?$

(2) 当 F 为有理数域时 R 还作成域，但当 F 为实数域时 R 不作成域。

证明 (1) 依矩阵的性质可知 R 对普通加法作成群，对普通乘法满足结合律，乘法对加法满足左、右分配律，故 R 对普通加法与乘法作成一个环，显见 R 中有单位元(二阶单位矩阵)。

由于任 $a,b,x,y\in F$，

$$\begin{pmatrix}a&2b\\b&a\end{pmatrix}\begin{pmatrix}x&2y\\y&x\end{pmatrix}=\begin{pmatrix}ax+2by&2(ay+bx)\\ay+bx&ax+2by\end{pmatrix}=\begin{pmatrix}x&2y\\y&x\end{pmatrix}\begin{pmatrix}a&2b\\b&a\end{pmatrix}$$

故 R 是可换的，从而 R 是一个有单位元的交换环。

又 $\begin{vmatrix}a&2b\\b&a\end{vmatrix}=a^2-2b^2$，故可知

$$R^*=\left\{\begin{pmatrix}a&2b\\b&a\end{pmatrix}\middle|a^2\neq 2b^2\right\}$$

(2) 记

$$\boldsymbol{A}=\begin{pmatrix}a&2b\\b&a\end{pmatrix}$$

当 F 为有理数域时，设

$$A \in R \text{且} A \neq O$$

故
$$|A| = a^2 - 2b^2$$

若 $|A| = 0$，即 $a^2 = 2b^2$，则 $b \neq 0$（否则 $a = b = 0, A = O$），故 $\left(\frac{a}{b}\right)^2 = 2$，这在有理数域内是不可能的。故 $|A| \neq 0$，因此 A 有可逆矩阵，且

$$A^{-1} = \frac{A^*}{|A|} = \frac{1}{a^2 - 2b^2}\begin{pmatrix} a & -2b \\ -b & a \end{pmatrix} \in R$$

即 A 在 R 中有逆元，又由(1)中结论，故 F 为有理数域时 R 作成域。

F 为实数域时，易知矩阵

$$A = \begin{pmatrix} \sqrt{2} & 2 \\ 1 & \sqrt{2} \end{pmatrix} \in R$$

且 $A \neq O$，但由于 $|A| = 0$，故 A 在 R 中无逆元。此时 R 不能作成域。

---

6. 设 F 是一个域，且 $|F| = 4$，证明：

(1) $\mathrm{char}\,F = 2$；

(2) F 中非 0 及 1 的两个元素都满足方程 $x^2 = x + 1$。

证明 (1) 设 $\mathrm{char}\,F = p$，则 p 为素数且为 F 中非零元（对加法来说）的阶，又 $|F| = 4$，故 $p \mid 4$，因此 $p = 2$，$\mathrm{char}\,F = 2$。

(2) 由(1)及第 3 章 §1 第 5 题知加群 F 与 Klein 四元群同构。另一方面，乘群 F^* 的阶为 3，因而是循环群，可设 $F^* = \{1, a, a^2\}$，故 $F = \{0, 1, a, a^2\}$，由于加群 F 与 Klein 四元群同构，有

$$a + 1 = a^2, a^2 + 1 = a = (a^2)^2$$

因此 F 的非 0 及 1 的两个元素都满足方程 $x^2 = x + 1$。

§4 环的同态与同构(P174)

1. 如果环 R 中元素 a 同 R 中每个元素可换，则称 a 为环 R 的一个中心元素。R 的所有中心元素作成的集合叫做环 R 的中心。证明：

(1) 环的中心是一个可换子环；

(2) 除环的中心是一个域。

证明 (1) 设 a, b 为环 R 的中心元素，则任 $x \in R$，

$$(a-b)x = ax - bx = xa - xb = x(a-b)$$
$$(ab)x = a(bx) = a(xb) = (ax)b = x(ab)$$

故 $a-b$ 与 ab 都是中心元素，故环 R 的中心为 R 的子环。又显见 $ab = ba$，故该中心为 R 的交换子环。

(2) 由(1) 知一个除环 R 的中心是一个交换子环 N，由于 N 中含有单位元 $1 \neq 0$，要证 N 为一个域只需证明若非零元 $x \in N$，则 x 在 N 中均有逆元。

任 $a \in R$，由 $0 \neq x \in N$ 得

$$ax = xa$$

故 $x^{-1}axx^{-1} = x^{-1}xax^{-1}$，$x^{-1}a = ax^{-1} \in R$，从而 $x^{-1} \in N$，因此，除环 R 的中心 N 为一个域。

---

2. 证明：有理数域 Q 的自同构只有恒等同构。

证明　设 σ 为有理数域 Q 的自同构。由于在同构映射下，单位元与单位元对应，负元与负元对应，逆元与逆元对应，故任整数 n 由 $\sigma(1) = 1$ 可知 $\sigma(n) = n$ 且

$$\sigma\left(\frac{m}{n}\right) = \sigma\left(m \cdot \frac{1}{n}\right) = \sigma(m)\sigma(n)^{-1} = \frac{m}{n} \quad (n \neq 0, m, n \text{ 为任一整数})$$

即 σ 为恒等同构，从而 Q 的自同构只有恒等同构。

---

3. 设 Q 是有理数域，证明：域

$$Q(\mathrm{i}) = \{a + b\mathrm{i} \mid a, b \in Q\}$$

有且只有两个自同构。

证明　设 σ 为 $Q(\mathrm{i})$ 的一个自同构，是必有

$$\sigma(0) = 0, \sigma(1) = 1, \sigma\left(\frac{m}{n}\right) = \frac{m}{n}$$

其中 $\frac{m}{n}$ 为有理数。又由于

$$-1 = \sigma(-1) = \sigma(\mathrm{i}^2) = \sigma(\mathrm{i})^2$$

故 $\sigma(\mathrm{i}) = \pm \mathrm{i}$，因此

当 $\sigma(\mathrm{i}) = \mathrm{i}$ 时

$$\sigma(a + b\mathrm{i}) = \sigma(a) + \sigma(b)\sigma(\mathrm{i}) = a + b\mathrm{i}$$

当 $\sigma(\mathrm{i})=-\mathrm{i}$ 时

$$\sigma(a+b\mathrm{i})=\sigma(a)+\sigma(b)\sigma(\mathrm{i})=a-b\mathrm{i}$$

从而 $Q(\mathrm{i})$ 的自同构只有两个。

---

4. 问：域 $Q(\mathrm{i})$ 与域

$$Q(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in Q\}$$

是否同构？同构时给出一个同构映射，不同构时证明之。

证明　设 σ 是 $Q(\sqrt{2})$ 到 $Q(\mathrm{i})$ 的一个同构映射，则

$$\sigma(1)=1,\sigma(4)=4$$

又

$$\begin{aligned}\sigma(4)=\sigma(\sqrt{2}\cdot 2\sqrt{2})&=\sigma(\sqrt{2})\sigma(2\sqrt{2})\\&=\sigma(\sqrt{2})\cdot\sigma(2)\cdot\sigma(\sqrt{2})\\&=2\sigma(\sqrt{2})^2\end{aligned}$$

故 $\sigma(\sqrt{2})^2=2$，故 $\sigma(\sqrt{2})=\pm\sqrt{2}$，但在 $Q(\mathrm{i})$ 中 $\pm\sqrt{2}$ 是不存在的，矛盾，所以 $Q(\sqrt{2})$ 到 $Q(\mathrm{i})$ 的同构映射是不存在的。

---

5. 证明：每个无单位元的环 R 都可嵌入（即在同构意义下包含在）一个有单位元的环中。

证明　令 $K=\{(a,n)\mid a\in R,n\in \mathbf{Z}\}$ 且任 $(a,m)\in K,(b,n)\in K$，约定：

$$(a,m)=(b,n)\Leftrightarrow a=b,m=n$$

$$(a,m)+(b,n)=(a+b,m+n)$$

$$(a,m)+(b,n)=(ab+na+mb,mn)$$

则可验证 K 对上述约定的加法与乘法作成环。又任 $(a,m)\in K$，

$$(a,m)(0,1)=(0,1)(a,m)=(a,m)$$

故环 K 具有单位元 $(0,1)$。任 $a\in R$，定义

$$\varphi: a\longrightarrow(a,0)$$

并记 $R_0=\{(a,0)\mid a\in R\}$，则 φ 是 R 到 R_0 的一个环同构，故 $R\cong R_0$。

从而若规定 $(a,0)=a$，则 $R\leqslant K$，且 R 中无单位元，即无单位元环 R 被包含在有单位元的环 K 中。

6. 设 R 是一个环，$u \in R$。证明：R 对以下二运算作成一个环且与 R 同构：

$$a \oplus b = a + b - u, a \circ b = ab - au - ub + u^2 + u$$

证明 任 $a,b \in R$，则 $a \oplus b \in R$，$a \circ b \in R$，即 R 对两种运算 $\oplus$ 及 $\circ$ 是封闭的，记 R 对 $\oplus$ 及 $\circ$ 作成的集合为 $R(\oplus, \circ)$。任 $x \in R$，定义

$$\varphi: x \longrightarrow x + u$$

则 φ 是 R 到 $R(\oplus, \circ)$ 的双射，又

$$\begin{aligned}\varphi(a+b) &= (a+b)+u = (a+u)+(b+u)-u \\ &= \varphi(a)+\varphi(b)-u = \varphi(a) \oplus \varphi(b)\end{aligned}$$

$$\begin{aligned}\varphi(a) \circ \varphi(b) &= (a+u) \circ (b+u) \\ &= (a+u)(b+u)-(a+u)u-u(b+u)+u^2+u \\ &= ab+au+ub+u^2-au-u^2-ub-u^2+u^2+u \\ &= ab+u = \varphi(ab)\end{aligned}$$

从而 φ 是 R 到 $R(\oplus, \circ)$ 的同构映射，又 R 为环，由定理 1，$R(\oplus, \circ)$ 也是环，且与 R 同构。

---

7. 证明：实数域的自同构只有恒等自同构。

证明 设 σ 是实数域 R 的任一自同构，则由第 2 题知任整数 m,n，任有理数 r，

$$\sigma(r) = r, \sigma\left(\frac{n}{m}\right) = \frac{n}{m}$$

当 $a \in R$ 且 $a > 0$ 时，存在 $b \in R$，使 $a = b^2$，从而

$$\sigma(a) = \sigma(b^2) = \sigma(b)^2 > 0$$

于是任 $c \in R$，当 $a > c$，即 $a - c > 0$ 时

$$\sigma(a-c) > 0$$

又
$$\sigma(a-c) = \sigma(a) - \sigma(c)$$

故
$$\sigma(a) > \sigma(c)$$

另一方面，任 $a \in R$，则存在有理数 s,t，使 $s < a < t$，故由上述所证可知

$$\sigma(s) < \sigma(a) < \sigma(t) \text{ 即 } s < \sigma(a) < t$$

即对满足 $s < a < t$ 的任何有理数 s,t 均有

$$s < \sigma(a) < t$$

所以必有 $\sigma(a)=a$，即 σ 是 R 的恒等自同构。

§ 5 模 n 剩余类环(P180)

1. 证明：同余类的乘法是 Z_n 的一个代数运算。

证明 设 $\bar{i}=\bar{s},\bar{j}=\bar{t}$，则

$$n \mid (i-s), n \mid (j-t)$$

其中 $i,,j,s,t$ 为整数，进而

$$n \mid [i(j-t)+t(i-s)], \text{即 } n \mid (ij-st)$$

故 $\overline{ij}=\overline{st}$，于是同余类的乘法是 Z_n 的一个代数运算。

---

2. 试指出环 Z_8 中的可逆元和零因子；再给出它的所有子环。

解 由定理 1 可知 Z_8 中的可逆元有：$\bar{1},\bar{3},\bar{5},\bar{7}$；

Z_8 中的零因子有：$\bar{2},\bar{4},\bar{6}$。

因为 Z_8 是循环环，其子加群就是子环，从而由 $8=2^3$ 知其全部子环有 $T(8)=3+1=4$ 个，即 $\{\bar{0}\},\{\bar{0},\bar{4}\},\{\bar{0},\bar{2},\bar{4},\bar{6}\},Z_8$。

---

3. 试给出 Z_{10} 的所有子环，并指出它们各自的特征。

解 $10=2\times5,T(10)=(1+1)(1+1)=4$，故模 10 的剩余类环 Z_{10} 有 $T(10)=4$ 个子环，即

$$\{\bar{0}\},\{\bar{0},\bar{5}\},\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8}\},Z_{10}$$

它们的特征依次分别是 1,2,5,10。

---

4. 证明 Euler 定理：设 n 是正整数，又 $(a,n)=1$，则

$$a^{\varphi(n)}\equiv 1 \pmod{n}$$

其中 $\varphi(n)$ 是欧拉函数。

证明 由定理 1 可知，Z_n 中的元素 $\bar{k}$ 是可逆元当且仅当 n 与 k 互素，又小于 n 且与 n 互素的正整数有 $\varphi(n)$ 个，故 Z_n 中的全体可逆元对乘法作成一个 $\varphi(n)$ 阶交换群。记该群为 G，又 $(a,n)=1$，故 $\bar{a}\in G$，由 Lagrange 定理，$\bar{a}$ 在 G 中的阶整除 $\varphi(n)$，于是 $\bar{a}^{\varphi(n)}=\bar{1}$ 即

$$a^{\varphi(n)}\equiv 1 \pmod{n}$$

5. 设 $g(x)$ 是系数属于域 Z_p（p 为素数）的一个多项式，证明：

$$[g(x)]^p = g(x^p)$$

证明 设

$$g(x) = a_0 + a_1 x + \cdots + a_n x^n$$

其中 $a_i \in Z_p (i = 0,1,2,\cdots,n)$。因为 Z_p 与多项式环 $Z_p[x]$ 的特征均为 p，且任 $a \in Z_p, a^p = a$，所以

$$\begin{aligned}[g(x)]^p &= a_0^p + a_1^p x^p + \cdots + a_n^p (x^p)^n \\ &= a_0 + a_1 x^p + \cdots + a_n (x^p)^n \\ &= g(x^p)\end{aligned}$$

---

6. 设 $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ 是 $n > 1$ 的标准分解式。证明：剩余类环 Z_n 有

$$p_1^{k_1-1} p_2^{k_2-1} \cdots p_m^{k_m-1}$$

个幂零元。

证明 若 $\overline{a}$ 为 Z_n 的幂零元，则存在正整数 s，使 $\overline{a}^s = \overline{0}$，故

$$n \mid a^s，即\ p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m} \mid a^s$$

于是 $p_i \mid a (i = 1,2,\cdots,m)$，又 $p_1, p_2, \cdots, p_m$ 是互异的素数，从而有

$$p_1 p_2 \cdots p_m \mid a, \overline{a} \in \langle \overline{p_1 p_2 \cdots p_m} \rangle$$

另一方面，若 $\overline{a} \in \langle \overline{p_1 p_2 \cdots p_m} \rangle$，即 $p_i \mid a$，令

$$s = \max\{k_1, k_2, \cdots, k_m\}$$

则 $(p_1 p_2 \cdots p_m)^s \mid a^s$，进而 $n \mid a^s$，故

$$\overline{a}^s = \overline{a^s} = \overline{0}$$

综上可知 $\langle \overline{p_1 p_2 \cdots p_m} \rangle$ 是由 Z_n 的所有幂零元作成的集合，而 $\langle \overline{p_1 p_2 \cdots p_m} \rangle$ 由元素 $\overline{p_1 p_2 \cdots p_m}, 2\,\overline{p_1 p_2 \cdots p_m}, \cdots, (p_1^{k_1-1} p_2^{k_2-1} \cdots p_m^{k_m-1})\,\overline{p_1 p_2 \cdots p_m}$ 组成，所以 Z_p 有 $p_1^{k_1-1} p_2^{k_2-1} \cdots p_m^{k_m-1}$ 个幂零元。

---

7. 证明：整数环的不同子环不同构。

证明 不妨设 $\langle m \rangle$，$\langle n \rangle$ 是整数环 Z 的任意两个不同子环，则 $m \neq \pm n$。

若 $\langle m \rangle$ 与 $\langle n \rangle$ 间存在同构映射 φ，且 $\varphi(m) = sn, \varphi(tm) = n$，故

$$\varphi(stm) = sn = \varphi(m)$$

从而 $stm = m, st = 1$，又 $s, t \in Z$，故 $s = \pm 1$。

当 $s=1$ 时，$\varphi(m)=n$，故

$$\varphi(m^2)=\varphi(m\cdot m)=\varphi(m)^2=n^2$$
$$=m\varphi(m)=mn$$

于是 $m=n$ 矛盾。

当 $s=-1$ 时，$\varphi(m)=-n$，故

$$\varphi(m^2)=\varphi(m\cdot m)=\varphi(m)^2=(-n)^2=n^2$$
$$=m\varphi(m)=-mn$$

于是 $m=-n$ 矛盾。

综上可知整数环的不同子环不同构。

---

8. 两个 n 阶循环环 R 与 $\overline{R}$ 同构的充分与必要条件是，存在整数 $k(0\leqslant k<n)$，并在 R 与 $\overline{R}$ 中分别有生成元 a 与 $\overline{a}$ 满足

$$a^2=ka,\overline{a}^2=k\overline{a}$$

证明 "⇒" 设 φ 为 R 到 $\overline{R}$ 的同构映射，则 $R=\langle a\rangle$ 且存在 $0\leqslant k<n$，使 $a^2=ka$。由于在同构映射下，生成元与生成元相对应，故

$$\overline{a}=\varphi(a)$$

为 $\overline{R}$ 的一个生成元且

$$\overline{a}^2=k\overline{a}\quad(0\leqslant k<n)$$

"⇐" 设 R 与 $\overline{R}$ 分别有生成元 a 与 $\overline{a}$ 且存在整数 $k(0\leqslant k<n)$，使

$$a^2=ka,\overline{a}=k\overline{a}$$

定义映射

$$\varphi: ma\longrightarrow m\overline{a}$$

其中 m 为非负整数，则易验证 φ 为环 R 到 $\overline{R}$ 的一个同构映射，即 $R\cong\overline{R}$。

§ 6 理想(P189)

1. 证明：

(1) 环中任意个理想的交仍是一个理想；

(2) 环中包含子集 S 的所有理想的交是 R 中包含 S 的最小子理想。

证明 (1) 只需证明任两个理想的交仍是一个理想。

不妨设 N_1,N_2 均为环 R 的理想，则任 $r\in R,a,b\in N_1\cap N_2$，有

$$(a-b) \in N_1 \cap N_2, ar, ra \in N_1 \cap N_2$$

因此 $N_1 \cap N_2$ 也是环 R 的理想。

(2) 设 K 为环 R 包含 S 的理想，即 $S \subseteq K \trianglelefteq R$，$N$ 为环 R 的所有包含 S 的理想的交，则

$$S \subseteq N = \bigcap_{S \subseteq K \trianglelefteq R} K$$

则由(1)知 $N \trianglelefteq R$，显见，若有 $K' \trianglelefteq R$ 且 $S \subset K'$，必有 $N \subseteq K'$，即 N 是 R 中包含 S 的最小理想。

---

2. 设 R 是环，$a, b \in R$，证明：

(1) $aR = \{ar \mid r \in R\}$，$Rb = \{rb \mid r \in R\}$ 分别是环 R 的右、左理想；

(2) $aRb \mid = \{arb \mid r \in R\} \leqslant R$。

证明 (1) 任 $ar_1, ar_2 \in aR$，则 $ar_1 - ar_2 = a(r_1 - r_2) \in aR$

任 $r_0 \in R$，$ar \in aR$，则

$$ar \cdot r_0 = a(rr_0) \in aR$$

故 aR 为环 R 的右理想。Rb 为环 R 的左理想类似可证。

(2) 显然任 $r_1, r_2 \in R$，有

$$ar_1b - ar_2b = a(r_1 - r_2)b, \quad ar_1b \cdot ar_2b = a(r_1bar_2)b$$

故

$$aRb \leqslant R$$

---

3. 设 S 是环 R 的一个非零子集，证明：S 的全体左(右)零化子作成 R 的一个左(右)理想。称其为 S 的左(右)零化理想。

证明 ① 设 A 为 S 的全体左零化子作成的集合，由 $0 \in A$ 可知 $A \neq \varnothing$，任 $a, b \in A$，有 $aS = bS = \{0\}$，从而

任 $x \in S$，$r \in R$，有

$$(a-b)x = ax - bx = 0, (ra)x = r(ax) = 0$$

故 $a-b, ra \in A$，所以 A 为 R 的左理想，即 S 的全体左零化子作成 R 的左理想。

② 类似可证 S 的全体右零化子作成 R 的一个右理想。

4. 设 R 为偶数环。证明：

$$N=\{4r \mid r\in R\}\lhd R$$

问 $N=\langle 4\rangle$ 是否成立？N 是由哪个偶数生成的主理想？

证明 设 $4r_1,4r_2$ 为 N 的任意两个元，由于两偶数相减仍为偶数，故

$$4r_1-4r_2=4(r_1-r_2)\in N$$

任 $r\in R$，由于两偶数相乘还是偶数，故

$$r(4r_1)=(4r_1)r=4(r_1r)\in N$$

从而

$$N\lhd R$$

因为 $4\in\langle 4\rangle$，但 $4\notin N$，因此 $N\neq\langle 4\rangle$，易知

$$N=\{\cdots,-16,-8,0,8,16,\cdots\}=\langle 8\rangle$$

即 N 是偶数环中由元素 8 生成的主理想。

---

5. 证明：

(1) 若 $N\lhd Z$，且 a 是 N 中最小的正整数，则 $N=\langle a\rangle$；

(2) 若 $a_1,a_2,\cdots,a_m$ 是整数环 Z 中的 m 个整数，且其最大公因数是 d，则

$$\langle a_1,a_2,\cdots,a_m\rangle=\langle d\rangle$$

证明 (1) 任 $b\in N$，令

$$b=as+t$$

其中 s,t 均为整数且 $0\leqslant t<a$，则 $t=b-as\in N$，又 a 是 N 中最小的整数，故 $t=0$，因此

$$b=as\in\langle a\rangle$$

从而

$$N\subseteq\langle a\rangle$$

又已知 R 是有单位元的交换环，且 $a\in N$，故 $\langle a\rangle\subseteq N$。

于是综上可得 $N=\langle a\rangle$。

(2) 任 $a\in\langle a_1,a_2,\cdots,a_m\rangle$，令

$$a=k_1a_1+k_2a_2+\cdots+k_ma_m$$

其中 $k_i\in Z$，由题意知 $d\mid a$，故 $a\in\langle d\rangle$，即有 $\langle a_1,a_2,\cdots,a_m\rangle\subseteq\langle d\rangle$。

又 d 为 $a_i(i=1,2,\cdots,m)$ 的最大公因数，故存在整数 $t_i(i=1,2,\cdots,$

m)，使

$$d = t_1a_1 + t_2a_2 + \cdots + t_ma_m$$

从而 $$d \in \langle a_1, a_2, \cdots, a_m\rangle, \langle d\rangle \subseteq \langle a_1, a_2, \cdots, a_m\rangle$$

因此综上有 $$\langle a_1, a_2, \cdots, a_m\rangle = \langle d\rangle$$

---

6. 证明：域 F 上多项式环 $F[x]$ 的每个理想都是主理想。

证明 不妨设 N 是多项式环 $F[x]$ 的任一理想。

若 $N = \{0\}$，则 $N = \langle 0\rangle$；

若 $N \neq \{0\}$，任取 $f(x) \in N$，令

$$f(x) = a(x)s(x) + t(x)$$

其中 $s(x)$ 为 N 中次数最低的多项式，$t(x) = 0$ 或次数小于 $s(x)$ 的次数。

由 $s(x) \in N \trianglelefteq F[x]$ 知 $a(x)s(x) \in N$，故

$$t(x) = f(x) - a(x)s(x) \in N$$

又 $s(x)$ 是 N 中次数最低的多项式，故 $t(x) = 0$，从而

$$f(x) = a(x)s(x), f(x) \subseteq \langle s(x)\rangle$$

又 $\langle s(x)\rangle \subseteq N$，因此 $N = \langle s(x)\rangle$，即多项式环 $F[x]$ 的每个理想都是主理想。

---

7. 举例指出，环 R 的中心不一定是 R 的理想。

解 不妨设 R 是数域 F 上的 2 阶全阵环，若记 $\boldsymbol{E}$ 为 2 阶单位矩阵，则 R 的中心

$$N = \{a\boldsymbol{E} \mid a \in F\}$$

且由第 4 章 §4 第 1 题知 N 作成 R 的子环。显见

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \notin N$$

故 N 不是 R 的理想。

---

8. 证明：§4 中例 3 中的环 F_N，当 $\boldsymbol{N}$ 为降秩方阵时，不是单环。

证明 不妨设 $\boldsymbol{N}$ 的秩为 r，依题意知 $0 \leqslant r < n$。因此齐次线性方程组

$$\boldsymbol{NX} = \boldsymbol{O}$$

有非零解。类似的方程组 $\boldsymbol{YN} = \boldsymbol{O}$ 也有非零解，设它们的非零解依次分别

为

$$\boldsymbol{a}=(a_1,a_2,\cdots,a_n)^{\mathrm{T}},\boldsymbol{b}=(b_1,b_2,\cdots,b_n)^{\mathrm{T}}$$

令 $\boldsymbol{A}$ 是第一列为 $\boldsymbol{a}$，其余各列为 $\boldsymbol{0}$ 的 n 阶方阵，$\boldsymbol{B}$ 是第一行为 $\boldsymbol{b}^{\mathrm{T}}$，其余各行为 $\boldsymbol{0}^{\mathrm{T}}$ 的 n 阶方阵，其中 $\boldsymbol{0}=(\underbrace{0,0,\cdots,0}_{n个})^{\mathrm{T}}$，则

$$\boldsymbol{AB}\neq\boldsymbol{O}\text{ 且 }\boldsymbol{NA}=\boldsymbol{BN}=\boldsymbol{O}$$

从而任 $\boldsymbol{C}\in F_N$，任 $\boldsymbol{X}\in F_N$ 有

$$\boldsymbol{C}\circ(\boldsymbol{AXB})=(\boldsymbol{AXB})\circ\boldsymbol{C}=\boldsymbol{O}$$

因此

$$D=\{\boldsymbol{AXB}\mid\boldsymbol{X}\in F_N\}\trianglelefteq F_N$$

又显见任何满秩方阵均不属于 D，故 $D\triangleleft F_N$。

又由 $\boldsymbol{AB}\neq\boldsymbol{O}$ 及 $\boldsymbol{AB}=\boldsymbol{AEB}\in D$ 知 $D\neq\{0\}$，于是 D 为环 F_N 的一个非平凡理想，进而 F_N 不是单环。

§7 商环与环同态基本定理(P194)

1. 设 N 是环 R 到环 $\overline{R}$ 的同态满射 φ 的核。证明：

$$\varphi\text{ 是同构映射}\Leftrightarrow N=\{0\}$$

证明 “$\Rightarrow$” 由 §4 定理 2 知若 φ 是同构映射，则 $N=\{0\}$。

“$\Leftarrow$” 设 $N=\{0\}$，φ 为环 R 到 $\overline{R}$ 的同态满射。且任 $a,b\in R$，$\varphi(a)=\varphi(b)$，则

$$\varphi(a)-\varphi(b)=\varphi(a-b)=\overline{0}$$

故 $a-b\in N=\{0\}$，从而 $a-b=0$，$a=b$，即 φ 又为单射。因为 φ 为环 R 到环 $\overline{R}$ 的双射，所以 φ 是同构映射。

---

2. 设 R 是有单位元的整环。证明：

(1) 若 $\mathrm{char}R=\infty$，则 R 有子环与 Z 同构；

(2) 若 $\mathrm{char}R=p$，则 R 有子环与 Z_p 同构。

证明 (1) 由 $\mathrm{char}R=\infty$ 可知，若 e 为 R 的单位元，则任 $n\in Z$，定义

$$\sigma:n\longrightarrow ne$$

则 σ 是整数环 Z 到环 R 的单同态。故

$$Z\cong\sigma(Z)\leqslant R$$

(2) 同理由 $\operatorname{char} R = p$ 知

$$\sigma: ne \longrightarrow \overline{n}$$

是 R 的子环 $R_1 = \{0, e, 2e, \cdots, (p-1)e\}$ 到 $Z_p = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{p-1}\}$ 的同构映射，因此

$$R_1 \cong Z_p$$

---

3. 设 φ 是环 R 到环 $\overline{R}$ 的一个同态满射，K 为同态核，$N \trianglelefteq R$。证明：若 $K \subseteq N$，则 N 在 $\overline{R}$ 中的象的逆象就是 N。

证明　设 $\varphi(N) = \overline{N}$，需证明 $N = \varphi^{-1}(\overline{N})$，显然 $N \subseteq \varphi^{-1}(\overline{N})$，下证 $\varphi^{-1}(\overline{N}) \subseteq N$。

任意的 $a \in \varphi^{-1}(\overline{N})$，即 $\varphi(a) \in \overline{N}$，记 $\overline{n} = \varphi(a)$，则 $\overline{n} \in \overline{N}$，从而存在 $n \in N$，使

$$\varphi(n) = \overline{n}$$

于是

$$\varphi(n) = \overline{n} = \varphi(a)$$

又由 φ 是同态映射知

$$\overline{0} = \varphi(a) - \varphi(n) = \varphi(a - n)$$

即 $a - n \in K \subseteq N$，记 $a - n = n_1 \in N$，则 $a = n + n_1 \in N$，因而由 a 的任意性知

$$\varphi^{-1}(\overline{N}) \subseteq N$$

综上可知

$$N = \varphi^{-1}(\overline{N})$$

---

4. 令 $R = \{a + b\mathrm{i} \mid a, b \in Q\}$，$\overline{R}$ 为由一切形如

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad (a, b \in Q)$$

的方阵作成的集合。证明：对普通加法与乘法来说，R 与 $\overline{R}$ 同构且 $\overline{R}$ 是一个域。

证明　定义

$$\varphi: a + b\mathrm{i} \longrightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

则 φ 是 R 到 $\overline{R}$ 的一个双射。

又因为

$$\begin{aligned}\varphi((a+bi)+(c+di)) &= \varphi((a+c)+(b+d)i)\\ &= \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix}\\ &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix}+\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\\ &= \varphi(a+bi)+\varphi(c+di)\end{aligned}$$

$$\begin{aligned}\varphi((a+bi)(c+di)) &= \varphi((ac-bd)+(ad+bc)i)\\ &= \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}\\ &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\\ &= \varphi(a+bi)\varphi(c+di)\end{aligned}$$

故 φ 又是同态映射，从而 φ 是 R 到 $\overline{R}$ 的同构映射，即 $R\cong\overline{R}$。又由于 R 为域，故由本章 §4 定理 3 知 $\overline{R}$ 也是一个域。

附：证明 $R=\{a+bi \mid a,b\in Q\}$ 是一个域。

易证 R 对普通加法和乘法作成一个整环。

设 $a+bi$ 为 Q 的一个非零元，则 a 和 b 不能同时为零，从而 $a^2+b^2\neq 0$，又因为

$$(a+bi)\left(\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i\right)=1$$

且

$$\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i\in R$$

故 F 的任意非零元在 R 中有逆元，因此 R 是一个域。

---

5. 设 R 为环，$N\lhd R$，证明：

(1) R/N 中的理想都具有形状 K/N，其中 K 是 R 的含 N 的理想；

(2) 在自然同态 $R\sim R/N$ 之下，R 的理想 H 的象为 $(H+N)/N$。

证明 (1) 设任 $\overline{K}\lhd R/N$，且 $K=\{k \mid k+N\in\overline{K}, k\in R\}$。对任 $k_1,k_2\in K, a\in R$，有

$$k_1+N, k_2+N \in \overline{K}$$

且

$$(a+N)(k_1+N)=ak_1+N \in \overline{K}$$

$$(k_1+N)(a+N)=k_1a+N \in \overline{K}$$

故 $k_1-k_2, ak_1, k_1a \in K$，因此 $K \trianglelefteq R$ 且 $\overline{K}=K/N$。

(2) 已知 $H \trianglelefteq R$ 且在自然同态下 H 的象为 K/N，故任意的 $k+N \in K/N$，存在 $h \in H$，使

$$h+N=k+N，即\ k-h \in N$$

令 $k-h=n$，则

$$k=h+n \in H+N, K \subseteq H+N$$

另一方面，任意的 $h+n \in H+N$（其中 $h \in H, n \in N$），则 $h+n$ 在自然同态下的象为

$$h+n+N=h+N \in K/N$$

因而

$$h+n \in K, H+N \subseteq K$$

综上可知 $K=H+N$，即 H 的象为 $(H+N)/N$。

§8　素理想和极大理想(P200)

1. 问 $\langle x\rangle$ 是不是多项式环 $Z[x]$ 的极大理想？又 $\langle x\rangle$ 是不是 $Q[x]$ 的极大理想？

解　① 因为

$$\langle x\rangle=\{常数项为零的整系数多项式全体\}$$

$$\langle 2,x\rangle=\{常数项为偶数的整系数多项式全体\}$$

显见有 $\langle x\rangle \subseteq \langle 2,x\rangle$，$2 \notin \langle x\rangle$，$\langle x\rangle \neq \langle 2,x\rangle$，又 $\langle 2,x\rangle \neq Z[x]$，故 $\langle x\rangle$ 不是 $Z[x]$ 的一个极大理想。

② 设 N 是 $Q[x]$ 的一个理想，且

$$\langle x\rangle \subseteq N, \langle x\rangle \neq N$$

则存在

$$f(x)=a_0+a_1x+\cdots+a_nx^n \in N \quad (a_0 \neq 0)$$

由此得

$$a_0 = f(x) - x(a_1 + a_2x + \cdots + a_nx^{n-1}) \in N$$

于是 $1 = \frac{1}{a_0} \cdot a_0 \in N$，因而 $N = (1) = Q[x]$，所以 $\langle x \rangle$ 是 $Q[x]$ 的极大理想。

---

2. 证明：$\langle 4 \rangle$ 是偶数环 R 的极大理想，但 $R/\langle 4 \rangle$ 不是域。

证明 $\langle 4 \rangle$ 刚好含有一切 $4n$，其中 n 是整数，设 N 是 R 的一个理想，且 $\langle 4 \rangle \subseteq N$，$\langle 4 \rangle \neq N$，则

$$4n \neq 2m = a \in N$$

由此知 $a = 4q + 2$，$2 = 4q + 2 - 4q \in N$，因而 $N = \langle 2 \rangle = R$，所以 $\langle 4 \rangle$ 是 R 的一个极大理想。

在 $R/\langle 4 \rangle$ 中，$[2] \neq [0]$ 而 $[2][2] = [4] = [0]$，即 $R/\langle 4 \rangle$ 有零因子，不是一个域。

---

3. 问：偶数环 R 的极大理想是否均为 $\langle 2p \rangle$？其中 p 是素数。又其素理想是否只有 $\{0\}$，R 和 $\langle 4 \rangle$？

解 ① 先证 $\langle 2p \rangle$ 是 R 的极大理想（p 为素数）。

当 $p = 2$ 时，由上面第 2 题知 $\langle 2p \rangle = \langle 4 \rangle$ 是偶数环 R 的极大理想。

当 $p \neq 2$ 时，设 N 为 R 的理想，且 $\langle 2p \rangle \subset N$。则由整数环是主理想环可知偶数环也是主理想环，故有 $N = \langle q \rangle$，$q \in R$。

由 $\langle 2p \rangle \subset N$ 可知 $2p = qt$，其中 $t \in Z$，即 $q \mid 2p$。

又因为 p 是素数，所以有 $(p,q) = 1$ 或 $p \mid q$。

当 $p \mid q$ 时，由 $q \in R$ 可知 $2 \mid q$，且 $(p,2) = 1$，故 $2p \mid q$，从而 $q \in \langle 2p \rangle$，$\langle q \rangle \subseteq \langle 2p \rangle$，这与 $\langle 2p \rangle \subset N$ 相矛盾。

因此由上可知，若 $N = \langle q \rangle \supset \langle 2p \rangle$，则必有 $(p,q) = 1$，又已证 $q \mid 2p$，所以 $q \mid 2$，而 q 为偶数，故 $q = \pm 2$，由此可知 $\langle q \rangle = R$，所以 $\langle 2p \rangle$ 当 $p \neq 2$ 时也是偶数环 R 的极大理想。

另一证法 设 N 为 R 的理想，且 $\langle 2p \rangle \subset N$，则存在 $2k \in N$，但 $2k \notin \langle 2p \rangle$，故 $p \nmid k$，$(p,k) = 1$，即存在 $s,t \in Z$，使

$$ps + kt = 1$$

任 $2m \in R$，有

$$2m = 2(ps + kt)m = 2psm + 2ktm \quad (m \in N)$$

因此

$$N = R$$

另一方面，若 $\langle 2m \rangle$ 为 R 的一个极大理想，如果 m 为合数，则存在 $1 < m_1 < m, 1 < m_2 < m$，使

$$m = m_1 m_2$$

故 $\langle 2m \rangle \subset \langle 2m_1 \rangle \subset R$，这与 $\langle 2m \rangle$ 是极大理想矛盾，从而 m 必为素数。综上可知，$\langle 2p \rangle$（p 为素数）是偶数环 R 的全部极大理想。

② 由本节例 2 知 R 的素理想有 $\{0\}$，R，及 $\langle 2p \rangle$。

故 $\langle 4 \rangle$ 不是 R 的素理想。

---

4. 试给出模 6 与模 10 剩余类环 Z_6 与 Z_{10} 中的所有素理想和极大理想，并说明理由。

证明　① 由剩余类环是循环环及循环环的子加群、子环和理想是等价的，从而可知 Z_6 的全部理想为

$$R_1 = \{\bar{0}\}, R_2 = \{\bar{0}, \bar{3}\}, R_3 = \{\bar{0}, \bar{2}, \bar{4}\}, Z_6$$

由于 Z_6 有零因子，故 R_1 不是素理想，进而不是极大理想。又易知 R_2 与 R_3 都是 Z_6 的极大理想，所以由推论 2 知 R_2 与 R_3 都是 Z_6 的素理想，从而 Z_6 的素理想有 R_2、R_3、Z_6，极大理想有 R_2、R_3。

② 类似于 ① 的讨论，Z_{10} 的素理想为

$$\{\bar{0}, \bar{5}\}, \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}, Z_{10}$$

Z_{10} 的极大理想有 $\{\bar{0}, \bar{5}\}$，$\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$。

---

5. 设 R 是交换环，$N \trianglelefteq R$。证明：R/N 是域的充分与必要条件是，N 是 R 的极大理想且由 $a^2 \in N$ 可得 $a \in N$。

证明　"$\Rightarrow$"　设 R/N 是域，由本章 §6 定理 2，R/N 也是单环，从而由本节定理 3 知 N 是环 R 的极大理想。

又任 $a \in R$，且 $a^2 \in N$，在域 R/N 中有

$$\bar{a}^2 = \overline{a^2} = \bar{0}$$

故 $\bar{a} = \bar{0}$，因此 $a \in N$。

“$\Leftarrow$” 若 N 是环 R 的极大理想，且由 $a^2 \in N$ 可得 $a \in N$。令

$$N' = \{b + ax \mid b \in N, x \in R, a \notin N\}$$

则有 $N \subseteq N' \lhd R$，又由于 $a^2 \in N'$ 但 $a^2 \notin N$，于是有 $N \subset N'$。而由条件，N 是环 R 的极大理想，从而必有 $N' = R$。这样，对任意 $c \in R$，存在 $b \in N$ 及 $x \in R$，使

$$c = b + ax$$

即对于 R/N 有 $\bar{c} = \bar{a}\,\bar{x}$，方程 $\bar{a}x = \bar{c}(\bar{a} \neq \bar{0})$ 在 R/N 中有解。

由题设 R 是交换环，故 R/N 可换，从而 R/N 是域。

§9 环与域上的多项式环(P204)

1. 设 R 是环 K 的一个子环，二者有相同的单位元，又 x 是 K 上未定元，$a \in K$，并令

$$R[a] = \{f(a) \mid f(x) \in R[x]\}$$

证明

$$R[x] \sim R[a]$$

证明 任 $f(x) \in R[x]$，定义

$$\varphi: f(x) \to f(a)$$

则 φ 是从 $R[x]$ 到 $R[a]$ 的一个满射。又任 $f(x), g(x) \in R[x]$，

$$\varphi(f(x) + g(x)) = f(a) + g(a) = \varphi(f(x)) + \varphi(g(x))$$

$$\varphi(f(x)g(x)) = f(a)g(a) = \varphi(f(x))\varphi(g(x))$$

从而 φ 是从 $R[x]$ 到 $R[a]$ 的一个同态满射，故 $R[x] \sim R[a]$。

---

2. 试举例指出：环 $R[x]$ 中的 m 次与 n 次多项式的乘积可能不是一个 $m+n$ 次多项式。

解 例如环 $Z_6[x]$ 中的多项式

$$f(x) = \bar{3}x^3 - \bar{3}x^2 \text{ 与 } g(x) = \bar{2}x^2 + \bar{1}$$

分别是 3 次与 2 次多项式，而

$$f(x)g(x) = \bar{3}x^3 - \bar{3}x^2$$

不是 $3+2$ 次多项式。

---

3. 试求出多项式

$$f(x)=\overline{3}+x-\overline{2}x^2+\overline{4}x^3$$

在域 Z_5 中的所有根。

解 由 $Z_5=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}$，故经验算可知 $f(x)$ 在 Z_5 内无根。

---

4. 求出域 Z_3 上的所有 2 次不可约多项式。

解 $Z_3=\{\overline{0},\overline{1},\overline{2}\}$，故 Z_3 上的 2 次不可约多项式有

$$x^2+\overline{1},x^2+x-\overline{1},x^2-x-\overline{1}$$

共三个。

---

5. 设 F^* 是域 F 的非零元素作成的乘群。证明：F^* 的任何有限子群都是循环群。

证法 1 设 $G\leqslant F^*$ 且 $|G|=n$，令

$$K=\{k\mid k\text{ 为正整数},a^k=1,a\in G\}$$

记 $m=\min K$，则由于 $|G|=n\in K$ 可知 $m\leqslant n$。

反之，由 $m\in K$ 知 G 中 n 个元都是方程 $x^m-1=0$ 的解，则 $n\leqslant m$，故 $n=\min K$，即 G 中存在 n 阶元，由第二章 §2 推论 1 知 G 为循环群。

证法 2 设 $G\leqslant F^*$ 且 $|G|=n$。设 $a\in G$，且 a 在 G 中的阶最大，记 $|a|=m$，则 $m\mid n$。

又因为 G 是交换群，故任 $x\in G$，均满足方程

$$x^m-1=0$$

又域 F 上 m 次方程在 F 中最多有 m 个根，因此 $n\leqslant m$，从而又由 $m\mid n$ 知 $m=n$，且 $G=\langle a\rangle$。

---

6. 设 R 是有理数域上的 2 阶方阵环，x 是 R 上未定元，又

$$f(x)=\begin{pmatrix}2&1\\0&0\end{pmatrix}x^2+\begin{pmatrix}0&0\\1&0\end{pmatrix}x+\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

$$g(x)=\begin{pmatrix}0&1\\-1&0\end{pmatrix}x+\begin{pmatrix}1&1\\1&1\end{pmatrix}$$

求 $f(x)$ 用 $g(x)$ 除所得的右商和右余式，并指出其右商 $\neq$ 左商，右余式 $\neq$ 左余式。

解 依定理 2 可知所求左商与左余式分别为

$$q_1(x)=\begin{pmatrix}1 & -2\\0 & 0\end{pmatrix}x+\begin{pmatrix}1 & -1\\0 & -1\end{pmatrix},r_1=\begin{pmatrix}1 & 0\\1 & 2\end{pmatrix}$$

右商与右余式分别为

$$q_2(x)=\begin{pmatrix}0 & 0\\2 & 1\end{pmatrix}x+\begin{pmatrix}1 & 1\\-2 & -1\end{pmatrix},r_2=\begin{pmatrix}2 & 0\\1 & 1\end{pmatrix}$$

显见左商与右商不等,左余式与右余式不等。

*§10 分式域(P208)

1. 证明:域 F 的分式域就是自身。

证明 因为 F 为域,故对 F 中任意元素 b 及非零元素 a,均有

$$\frac{b}{a}=ba^{-1}=a^{-1}b\in F$$

因此域 F 的分式域就是自身。

---

2. 证明定理 2 中集合 M 的元素间的关系

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

是一个等价关系。

证明 显见 $(a,b)\sim(a,b)$,$(c,d)\sim(a,b)$,即反身性及对称性成立。

设 $(a,b)\sim(c,d)$,$(c,d)\sim(s,t)$,可证明 $(a,b)\sim(s,t)$,其中 $acs\neq 0$,显见有

$$ad=bc,ct=ds$$

故 $adct=bcds$,又 R 是整环,消去律成立以及 $c\neq 0$,从而有

$$adt=bds$$

若 $d=0$,则由 $ct=ds$ 知 $t=0$,由 $ad=bc$ 知 $b=0$,因此 $at=bs$。

若 $d\neq 0$,则可从 $adt=bds$ 消去 d,即得 $at=bs$。总之有 $at=bs$,所以 $(a,b)\sim(s,t)$,传递性成立。

综上可知定理 2 中集合 M 的元素间的关系是一个等价关系。

---

3. 证明定理 2 中的 φ 是 R 到 S 的一个同构映射。

证明 显见 φ 是满射,又任 $\frac{ab}{b},\frac{cb}{b}\in S$,其中 $b\neq 0$,若

$$\frac{ab}{b}=\frac{cb}{b}\text{ 即 }ab^2=cb^2$$

则由 R 是整环，消去律成立，以及 $b\neq 0$ 知 $b^2\neq 0$，故消去 b^2 得 $a=c$，因此 φ 又是单射。

又因为

$$\varphi(a+c)=\frac{(a+c)b}{b}=\frac{ab}{b}+\frac{cb}{b}=\varphi(a)+\varphi(c)$$

$$\varphi(ac)=\frac{ac\cdot b}{b}=\frac{ab}{b}\cdot\frac{cb}{b}=\varphi(a)\varphi(c)$$

从而综上可知 φ 是 R 到 S 的同构映射。

---

4. 问：Gauss 整环 $Z[\mathrm{i}]$ 的分式域为何？

解　$Z[\mathrm{i}]=\{a+b\mathrm{i}\mid a,b\in Z\}$，显见 $Z[\mathrm{i}]$ 包含整数环及元素 i，故由定理 1，$Z[\mathrm{i}]$ 的分式域为 $Q[\mathrm{i}]=\{a+b\mathrm{i}\mid a,b\in Q\}$。

---

5. 设 p 是一个素数。证明：

$$R=\left\{\frac{m}{n}\,\middle|\,m,n\in Z,(n,p)=1\right\}$$

是一个整环，并求其分式域。

证明　显见 R 为交换环且无零因子，故 R 是一个整环。

又任 $a,b\in R(a\neq 0)$，不妨设

$$a=\frac{m_1}{n},b=\frac{m_2}{n}$$

则 $m_1,m_2\in Z$ 且 $m_1\neq 0$，

$$\frac{b}{a}=a^{-1}b=ba^{-1}=\frac{m_2}{m_1}$$

从而可知 R 的分式域为有理数域 Q。

§ 11　环的直和(P216)

1. 设环 $R=\sum\limits_{i=1}^{n}\oplus R_i$。证明：环 R 有单位元当且仅当每个理想 R_i 有单位元。并且

$$1 = 1_1 + 1_2 + \cdots + 1_n$$

其中 1 是 R 的单位元，1_i 是 R_i 的单位元。

证明 “$\Rightarrow$” 设 1 为 R 的单位元，由题设已知

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_n$$

从而可令

$$1 = 1_1 + 1_2 + \cdots + 1_n$$

其中 $1_i \in R_i$，任意 $x_i \in R_i$，则

$$x_i = 1x_i = (1_1 + 1_2 + \cdots + 1_n)x_i = 1_i x_i$$

$$x_i = x_i 1 = x_i(1_1 + 1_2 + \cdots + 1_n) = x_i 1_i$$

所以 1_i 是 R_i 的单位元。

“$\Leftarrow$” 设 1_i 是 R_i 的单位元，令

$$e = 1_1 + 1_2 + \cdots + 1_n$$

由题设，对任 $r \in R$，也可令

$$r = r_1 + \cdots + r_i + \cdots + r_n$$

其中 $r_i \in R_i(i = 1,2,\cdots,n)$。故

$$\begin{aligned} re &= (r_1 + \cdots + r_i + \cdots + r_n)(1_1 + \cdots + 1_i + \cdots + 1_n) \\ &= r_1 1_1 + \cdots + r_i 1_i + \cdots + r_n 1_n \\ &= r_1 + \cdots + r_i + \cdots + r_n = r \\ er &= (1_1 + \cdots + 1_i + \cdots + 1_n)(r_1 + \cdots + r_i + \cdots + r_n) \\ &= 1_1 r_1 + \cdots + 1_i r_i + \cdots + 1_n r_n \\ &= r_1 + \cdots + r_i + \cdots + r_n = r \end{aligned}$$

从而 $er = re = r$，即 $e = 1$ 是 R 的单位元。

---

2. 设 $Z_2 = \{0,1\}$，且

$$R = \{(a_1,a_2,\cdots,a_n) \mid a_i \in Z_2\}$$

即 R 是 n 个环 Z_2 的外直和。证明：R 是一个布尔环。又 R 的特征为何？

证明 由 $a_i \in Z_2$ 知 $a_i^2 = a_i$，故

$$(a_1,a_2,\cdots,a_n)^2 = (a_1,a_2,\cdots,a_n)$$

即 R 是布尔环且 $\mathrm{char}R = 2$。

3. 设环 $R=\sum_{i=1}^{n}\oplus R_i$，证明：

$$\varphi_i: a=a_1+\cdots+a_i+\cdots+a_n\to a_i\quad(i=1,2,\cdots,n)$$

（其中 $a_i\in R_i$）是环 R 到 R_i 的同态满射（称为正则投射），且

(1) $\varphi_i\varphi_j=\begin{cases}\varphi_i, & i=j\\ 0, & i\neq j\end{cases}$

(2) $\varphi_1+\varphi_2+\cdots+\varphi_n=\varepsilon$

其中 0 是零同态（即把环 R 的每个元素都变为零元素），ε 为环 R 的恒等变换。

证明 (1) 显见 φ_i 是环 R 到 R_i 的满射，任 $a,b\in R$，则

$$a=a_1+\cdots+a_i+\cdots+a_n,b=b_1+\cdots+b_i+\cdots+b_n$$

且有

$$a+b=(a_1+b_1)+\cdots+(a_i+b_i)+\cdots+(a_n+b_n)$$
$$ab=a_1b_1+\cdots+a_ib_i+\cdots+a_nb_n$$

从而

$$\varphi_i(a+b)=\varphi_i(a)+\varphi_i(b)$$

且

$$\varphi_i(ab)=\varphi_i(a)\varphi_i(b)$$

所以 φ_i 是环 R 到 R_i 的同态满射。

又由上述证明可知

$$\varphi_i\varphi_i(a)=\varphi_i(a_i)=a_i$$
$$\varphi_i\varphi_j(a)=\varphi_i(a_j)=0\quad(i\neq j)$$

故有

$$\varphi_i\varphi_j=\begin{cases}\varphi_i, & i=j\\ 0, & i\neq j\end{cases}$$

(2) 又由于

$$(\varphi_1+\varphi_2+\cdots+\varphi_n)(a)=\varphi_1(a)+\varphi_2(a)+\cdots+\varphi_n(a)$$
$$=a_1+a_2+\cdots+a_n=a$$

故

$$\varphi_1+\varphi_2+\cdots+\varphi_n=\varepsilon$$

4. 设 N 是环 R 的一个理想。证明：如果 N 有单位元，则 N 是环 R 的一个直和项。

证明 只需证明存在 R 的理想 N'，使 $R = N \oplus N'$。

设 e 为 N 的单位元，令

$$N' = \{x \mid x \in R, xe = ex = 0\}$$

则由 $0 \in N'$ 可知 $N' \neq \varnothing$。设 $x, y \in N'$，则 $xe = ex = ye = ey = 0$，从而

$$(x-y)e = e(x-y) = 0$$

即

$$x - y \in N'$$

任意 $r \in R$，由于 $N \trianglelefteq R$ 且 e 为 N 的单位元知

$$re \in N$$

且

$$re = e(re)$$

又任 $x \in N'$，$xe = ex = 0$，故

$$(xr)e = x(re) = x(ere) = xe(re) = 0$$

$$e(xr) = (ex)r = 0$$

从而 $(xr)e = e(xr) = 0$，即 $xr \in N'$，而类似可得 $rx \in N'$，于是有 $N' \trianglelefteq R$，即 N' 是 R 的一个理想。

任 $x \in N \cap N'$，即 $x \in N$ 且 $x \in N'$，故 $xe = x$ 且 $xe = 0$，于是 $x = 0$，$N \cap N' = \{0\}$。

任意的 $r \in R$，由题设可知 $re, er \in N$，记 $a = re$，则

$$ae = (re)e = re, (r-a)e = 0$$

$$er = ere = ea, e(r-a) = 0$$

从而 $r - a = b \in N'$，$r = a + b \in N + N'$。于是综上知 $R = N \oplus N'$。

---

5. 设 $n_1, n_2, \cdots, n_s$ 是 s 个两两互素的正整数。证明：剩余类环 $Z_{n_1 n_2 \cdots n_s}$ 与 $Z_{n_1}, Z_{n_2}, \cdots, Z_{n_s}$ 的外直和

$$Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_s}$$

同构。

证明 任 $\overline{x} \in Z_{n_1 n_2 \cdots n_s}$，定义

$$\varphi: \overline{x} \to \underbrace{(\overline{x}, \overline{x}, \cdots, \overline{x})}_{s\text{个}\overline{x}}$$

其中$(\overline{x}, \overline{x}, \cdots, \overline{x})$中第 i 个 $\overline{x} \in Z_{n_i}$ $(i = 1, 2, \cdots, s)$。

若$(\overline{x}, \overline{x}, \cdots, \overline{x}) = (\overline{y}, \overline{y}, \cdots, \overline{y})$，则

$$n_i \mid (x - y) \quad (i = 1, 2, \cdots, s)$$

又题设中 $n_1, n_2, \cdots, n_s$ 为 s 个两两互素的正整数，故

$$n_1 n_2 \cdots n_s \mid (x - y)$$

于是在环 $Z_{n_1 n_2 \cdots n_s}$ 中，$\overline{x} = \overline{y}$，即 φ 为单射。

又 $Z_{n_1 n_2 \cdots n_s}$ 的阶与直和 $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_s}$ 的阶均为 $n_1 n_2 \cdots n_s$，从而 φ 为双射，而

$$\begin{aligned} \varphi(\overline{x+y}) &= (\overline{x+y}, \overline{x+y}, \cdots, \overline{x+y}) \\ &= (\overline{x}, \overline{x}, \cdots, \overline{x}) + (\overline{y}, \overline{y}, \cdots, \overline{y}) \\ &= \varphi(\overline{x}) + \varphi(\overline{y}) \end{aligned}$$

$$\begin{aligned} \varphi(\overline{xy}) &= (\overline{xy}, \overline{xy}, \cdots, \overline{xy}) \\ &= (\overline{x}, \overline{x}, \cdots, \overline{x})(\overline{y}, \overline{y}, \cdots, \overline{y}) \\ &= \varphi(\overline{x})\varphi(\overline{y}) \end{aligned}$$

即 φ 保持加法与乘法运算，因此 φ 是 $Z_{n_1 n_2 \cdots n_s}$ 到 $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_s}$ 的同构。

---

6. 设 R 为环，e 是 R 的一个幂等元。又令

$$R(1-e) = \{r - re \mid r \in R\}, (1-e)R = \{r - er \mid r \in R\}$$

$$(1-e)R(1-e) = \{r - re - er + ere \mid r \in R\}$$

(R 不一定有单位元) 证明：

(1)$R(1-e)$、$(1-e)R$ 分别为环 R 的左、右理想；

(2)eRe，$eR(1-e)$ 与$(1-e)Re$ 都是 R 的子环，且后二者还是零乘环；

(3) 作为加群，R 有直和分解：

$$R = Re \oplus R(1-e); R = eR \oplus (1-e)R;$$

$$R = eRe \oplus eR(1-e) \oplus (1-e)Re \oplus (1-e)R(1-e)$$

并分别称这三个直和分解为加群$(R, +)$ 关于幂等元 e 的左、右和双边

Peirce 分解。

提示：用 e 乘某式一边或两边，并证 0 表示法惟一。

证明 (1) 任 $r_1, r_2, r \in R$，由

$$(r_1 - r_1 e) - (r_2 - r_2 e) = (r_1 - r_2) - (r_1 - r_2)e$$

$$r_1(r - re) = r_1 r - r_1 re$$

知 $R(1-e)$ 为环 R 的左理想。由

$$(r_1 - er_1) - (r_2 - er_2) = (r_1 - r_2) - e(r_1 - r_2)$$

$$(r - er)r_1 = rr_1 - err_1$$

知$(1-e)R$ 为环 R 的右理想。

(2) 由于 $er_1e \cdot er_2e = e(r_1er_2)e$ 以及

$$er_1e - er_2e = e(r_1 - r_2)e$$

故 $eRe \leqslant R$。类似可证 $eR(1-e) \leqslant R$，$(1-e)Re \leqslant R$。

由 e 为 R 的幂等元知

$$(er_1 - er_1e)(er_2 - er_2e)$$

$$= er_1er_2 - er_1er_2 - er_1er_2e + er_1er_2e = 0$$

故 $eR(1-e)$ 为 R 的零乘子环。

类似可证$(1-e)Re$ 也是 R 的零乘子环。

(3)① 任 $r \in R$，则由 $r = re + (r - re) \in Re + R(1-e)$ 可知

$$R = Re + R(1-e)$$

任 $x \in Re \cap R(1-e)$，则存在 $r_1 \in R, r_2 \in R$，使

$$x = r_1 e = r_2(1-e)$$

又 $e^2 = e$，从而

$$x = r_1 e = r_1 e^2 = (r_1 e)e = (r_2 - r_2 e)e = 0$$

即

$$Re \cap R(1-e) = \{0\}$$

因此

$$R = Re \oplus R(1-e)$$

② 任 $r \in R$，则由 $r = er + (r - er) \in eR + (1-e)R$ 可知

$$R = eR + (1-e)R$$

任 $x \in eR \cap (1-e)R$，则存在 $r_1, r_2 \in R$，使

$$x = er_1 = (1-e)r_2$$

从而由 $e^2=e$ 知

$$x=er_1=e^2r_1=e(er_1)=e(r_2-er_2)=er_2-e^2r_2=0$$

于是

$$eR\cap(1-e)R=\{0\}$$

从而 $$R=eR\oplus(1-e)R$$

③ 任 $r\in R$，由

$$r=ere+(er-ere)+(re-ere)+(r-er-re+ere)$$

可知

$$R=eRe+eR(1-e)+(1-e)Re+(1-e)R(1-e)$$

如果

$$0=er_1e+(er_2-er_2e)+(r_3e-er_3e)+(r_4-er_4-r_4e+er_4e)\quad(*)$$

利用 $e^2=e$，式 $(*)$ 两边同乘 e 得

$$er_1e=0$$

式 $(*)$ 左乘 e 得

$$er_2-er_2e=0$$

式 $(*)$ 右乘 e 得

$$r_3e-er_3e=0$$

代入式 $(*)$ 又得

$$r_4-er_4-r_4e+er_4e=0$$

综上可知 0 的表示法唯一，从而

$$R=eRe\oplus eR(1-e)\oplus(1-e)Re\oplus(1-e)R(1-e)$$

*§12　非交换环(P221)

1. 验算 §12 定理 1 证明中给出的环 R 的结合律(对乘法)成立。

证明　因为

$$(x_1,y_1)(x_2,y_2)=(x_2+y_2)(x_1,y_1)$$

所以

$$\begin{aligned}[(x_1,y_1)(x_2,y_2)](x_3,y_3)&=(x_2+y_2)(x_1,y_1)(x_3,y_3)\\&=(x_2+y_2)(x_3+y_3)(x_1,y_1)\end{aligned}$$

$$\begin{aligned}(x_1,y_1)[(x_2,y_2)(x_3,y_3)]&=(x_1,y_1)[(x_3+y_3)(x_2,y_2)]\\&=(x_3+y_3)(x_1,y_1)(x_2,y_2)\end{aligned}$$

$$= (x_3 + y_3)(x_2 + y_2)(x_1, y_1)$$

即 $$[(x_1, y_1)(x_2, y_2)](x_3, y_3) = (x_1, y_1)[(x_2, y_2)(x_3, y_3)]$$

---

2. 问：§12 定理 1 证明中给出的环 R 是否有单位元?为什么?

解 若环 R 的单位元存在，不妨设为 (a,b)，则有

$$(a,b)(1,0) = (1,0)$$

又据规定的乘法有

$$(a,b)(1,0) = (1+0)(a,b) = (a,b)$$

故

$$(a,b) = (1,0)$$

同理有

$$(a,b)(0,1) = (a,b) = (0,1)$$

因此 $n \mid (a-1)$ 且 $n \mid a$，这与 $n > 1$ 矛盾，所以单位元不存在。

---

3. 给出 §12 例 1 中 4 阶非交换环 R_1 的乘法表，并证明环 R_1 与环 R_2 不同构。

证明 依次用 $0,a,b,c$ 表示 R_1 中的 4 个元素，用 $0,x,y,z$ 依次表示下列四个二阶方阵

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

即 R_2 中的四个元素，则非交换环 R_1 与 R_2 的乘法表如下

·	0	a	b	c
0	0	0	0	0
a	0	a	a	0
b	0	b	b	0
c	0	c	c	0

·	0	x	y	z
0	0	0	0	0
x	0	x	y	z
y	0	x	y	z
z	0	0	0	0

下证 R_1 与 R_2 不同构。

如果 R_1 与 R_2 同构，φ 为其同构映射，按乘法表，除 $\varphi(0) = 0$ 外，若①$\varphi(a) = x, \varphi(b) = y$，则由 φ 同构及乘法表可知

$$\varphi(ab) = \varphi(a)\varphi(b) = xy = y$$

又由乘法

$$\varphi(ab)=\varphi(a)=x$$

因此 $x=y$，矛盾。

若 $\varphi(a)=x,\varphi(b)=z$，则 $\varphi(ab)=\varphi(a)\varphi(b)=xz=z$

$$\varphi(ab)=\varphi(a)=x$$

故 $x=z$，也矛盾。

② 若 $\varphi(a)=y,\varphi(b)=x$，则

$$\varphi(ab)=\varphi(a)\varphi(b)=yx=x$$

$$\varphi(ab)=\varphi(a)=y$$

故 $x=y$，矛盾。

若 $\varphi(a)=y,\varphi(b)=z$，则

$$\varphi(ab)=\varphi(a)\varphi(b)=yz=z$$

$$\varphi(ab)=\varphi(a)=y$$

故 $z=y$，矛盾。

③ 若 $\varphi(a)=z,\varphi(b)=x$，则

$$\varphi(ab)=\varphi(a)\varphi(b)=zx=0$$

$$\varphi(ab)=\varphi(a)=z$$

故 $z=0$，矛盾。

若 $\varphi(a)=z,\varphi(b)=y$，则

$$\varphi(ab)=\varphi(a)\varphi(b)=zy=0$$

$$\varphi(ab)=\varphi(a)=z$$

故 $z=0$，矛盾。

综上可知，R_1 与 R_2 不能同构。

---

4. 令 R_1' 为由 Z_2 上 4 个二阶方阵

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

关于方阵的普通加法与乘法作成的环。证明：§ 12 例 1 中的环 R_1 与这个环 R'_1 同构。

证明　用 $0,x,y,z$ 依次表示上面的四个二阶方阵。则可得乘法表如下

$\cdot$	0	x	y	z
0	0	0	0	0
x	0	x	x	0
y	0	y	y	0
z	0	z	z	0

易知 R_1 与 R_1' 对加法均作成 Klein 四元群。定义

$$\varphi: 0 \longrightarrow 0, \quad a \longrightarrow x$$

$$b \longrightarrow y, \quad c \longrightarrow z$$

则 φ 是从环 R_1 到 R_1' 的同构映射。因此 $R_1 \cong R_1'$。

5. 给出两个不同构的 12 阶非交换环。

解 仍用 R_2 表示上面第 3 题中的非交换环 R_2，则由 R_2 不可换知 12 阶环

$$R' = R_2 \oplus Z_3$$

不可换，其中 Z_3 为以 3 为模的剩余类环。

取 R 为 §12 例 2 中的

$$R = R_1 \oplus Z_3$$

其中 R_1 为例 1 中的 4 阶非交换环，进而 R 是 12 阶非交换环。下证 R 与 R' 不同构。

否则，若 $R \cong R'$，则 $R_1 \cong R/Z_3 \cong R'/Z_3 \cong R_2$，故 $R_1 \cong R_2$，与第 3 题结论矛盾。因此 R 与 R' 不同构。

6. 给出两个不同构的无限非交换环。

解 设 R 是整数环 Z 上的 2 阶全阵环，则 R 是无限非交换环。又记 Z_2 为以 2 为模的剩余类环，则 $R \oplus Z_2$ 也是无限非交换环。但由于 $R \oplus Z_2$ 有 2 阶子环，R 中没有 2 阶子环，所以二者不同构。

7. 证明：若 e 是环 R 的惟一的左单位元，则 e 必是 R 的单位元。

证明 任意的 $a,b \in R$，由于 e 为环 R 的左单位元，则

$$(ae - a + e)b = a(eb) - ab + eb = ab - ab + b = b$$

即 R 中元素 $ae - a + e$ 也是 R 的左单位元，又 e 为 R 惟一的左单位元，故

$$ae - a + e = e \quad 即\ ae = a$$

由 a 的任意性知 e 也是环 R 的右单位元，因此，e 必为 R 的单位元。

8. 设 R 是一个有单位元(用 1 表示)的环,$a,b\in R$,证明:如果 $1+ab$ 在 R 中有逆元,则 $1+ba$ 在 R 中也有逆元。

证明 不妨设 $c=(1+ab)^{-1}$,即

$$c(1+ab)=(1+ab)c=1$$

故有

$$c-1+cab=c-1+abc=0$$

从而

$$\begin{aligned}(1-bca)(1+ba)&=1-bca+ba-bcaba\\&=1-b(c-1+cab)a=1\\(1+ba)(1-bca)&=1+ba-bca-babca\\&=1-b(c-1+abc)a=1\end{aligned}$$

因此 $1+ba$ 在 R 中有逆元 $1-bca$。

---

9. 设 R 是一个有单位元的环。如果 R 中元素 a,b 有 $ab=1$,则称 b 是 a 的一个右逆元,而称 a 是 b 的一个左逆元。证明卡普兰斯基(I. Kaplansky)定理:若 R 中元素 a 有多于一个的右逆元,则 a 必有无限多个右逆元。

证法 1 先证明 a 为可逆元 $\Leftrightarrow a$ 不是左零因子 $\Leftrightarrow a$ 的右逆元唯一。

可逆元显然不是零因子。设 a 不是左零因子,则对 a 的任意两个右逆元 u 和 v,由

$$a(u-v)=0$$

可得 $u=v$,即右逆元惟一。

设 u 是 a 的惟一右逆元,则由

$$au=1,a(ua-1+u)=1$$

可知 $ua-1+u=u,ua=1$,即得 a 为可逆元。

下证若 a 有多于一个右逆元时,则 a 必有无限多个右逆元。

若 a 的右逆元有且仅有 n 个,记为 $b_1,b_2,\cdots,b_n(n\geqslant 2)$,令

$$c_i=b_1+1-b_ia\quad(i=1,2,\cdots,n)$$

则 $ac_i=1$,进而每个 c_i 都是 a 的右逆元,且 $c_1,c_2,\cdots,c_n$ 必两两互异。若存在某个 $c_i=b_1$,则 $b_ia=1$,a 为可逆元,与前面所证的若 a 为可逆元,则其右逆元惟一的结论矛盾。从而 $b_1,c_1,c_2,\cdots,c_n$ 是 a 的 $n+1$ 个互异右逆元,这与 n 的最小性矛盾。

证法 2 设 a 的右逆元有且仅有 n 个，记为 $b_1,b_2,\cdots,b_n(n \geqslant 2)$，则由

$$ab_i = 1 \quad (i = 1,2,\cdots,n)$$

可知

$$a(1 - b_ia + b_1) = 1 \quad (i = 1,2,\cdots,n)$$

当 $i \neq j$ 时，如果 $1 - b_ia + b_1 = 1 - b_ja + b_1$，则有 $b_ia = b_ja$，两边同时右乘 b_1，则有 $b_i = b_j$，矛盾，故 $i \neq j$ 时

$$1 - b_ia + b_1 \neq 1 - b_ja + b_1$$

于是 $c_i = 1 - b_ia + b_1(i = 1,2,\cdots,n)$ 为 a 的所有右逆元，所以存在 $i(i = 1,2,\cdots,n)$，使

$$b_1 = 1 - b_ia + b_1$$

故 $b_ia = 1$，取 $j \neq i(j = 1,2,\cdots,n)$ 在 $b_ia = 1$ 两边同时右乘 b_j，由 b_j 为右逆元可知

$$b_iab_j = b_j, b_i = b_j$$

这与 $b_1,b_2,\cdots,b_n$ 为 a 的互不相同的 n 个右逆元矛盾。

综上可知 a 有无限多个右逆元。

---

10. 设 R 是一个有单位元的环，a 与 b 是 R 的单位(即可逆元)。证明：若有二互素整数 m,n 使

$$a^m = b^m, a^n = b^n$$

则必 $a = b$。

证明 若 m 与 n 互素，即 $(m,n) = 1$，则存在整数 s,t，使 $ms + nt = 1$，因此

$$a = a^{ms+nt} = a^{ms}a^{nt} = (a^m)^s(a^n)^t$$
$$b = b^{ms+nt} = b^{ms}b^{nt} = (b^m)^s(b^n)^t$$

而 $a^m = b^m, a^n = b^n$，所以由上式可知 $a = b$。

---

11. 设 R 为布尔环，即环 R 中每个元素 x 都有 $x^2 = x$，证明：若 $|R| \geqslant 3$，则 R 不是整环。

证明 假设 R 是整环，则 R 中无零因子。

由 $|R| \geqslant 3$ 可知存在非零元素 $a,b \in R$ 且 $a \neq b$，由 $a^2 = a$ 即 $a^2 - a = 0$ 得

$$(a^2-a)b = a(ab-b) = 0$$

由假设，R 中无零因子以及 $a \neq 0$ 得 $ab-b=0$，又 $b^2=b$，故

$$ab-b = ab-b^2 = (a-b)b = 0$$

又由假设 R 中无零因子以及 $b \neq 0$ 可得 $a-b=0$，即 $a=b$，矛盾。所以假设不成立，R 不是整环。

---

12. 设 R 是一个 Jacobson 环，即对 R 中每个元素 a 都有与 a 有关的整数 $n>1$ 使 $a^n=a$。证明：R 的幂等元都是中心元。

证明 设 a 为 R 的幂等元，即 $a^2=a$。故任 $x \in R$，

$$(axa-ax)^2 = (axa-ax)(axa-ax) = 0$$
$$(axa-xa)^2 = (axa-xa)(axa-xa) = 0$$

从而 $axa-ax$ 与 $axa-xa$ 为环 R 的幂零元，于是由本章 §2 第 5 题知

$$axa-ax=0, axa-xa=0$$

故

$$axa = ax = xa$$

即 a 是 R 的中心元。

---

13. 设 R 是一个有单位元（用 1 表示）的有限环。证明：如果 $ab=1$，则 $ba=1$。

证明 任 $x \in R$，若 $bx=0$，则两边同时左乘 a，利用题设条件 $ab=1$ 得

$$x = (ab)x = a \cdot 0 = 0$$

即 $x=0$，从而可知 b 不是 R 的左零因子。故任 $x,y \in R$，若 $x \neq y$，则

$$bx \neq by$$

因为 R 有限，故可设 $R=\{a_1,a_2,\cdots,a_n\}$，由上述证明，有

$$R = bR = \{ba_1, ba_2, \cdots, ba_n\}$$

又 $1 \in R$，故存在某 i，使 $ba_i=1$，若两边同时左乘 a，则有

$$a(ba_i) = (ab)a_i = a_i = a$$

所以

$$ba = 1$$

---

14. 若对环 R 中每个元素 a 都有 $a' \in R$（a' 与 a 相关）使 $a=aa'a$，则称 R 为正则环。证明：

(1) p- 环是正则环，但反之不成立；

(2) 再指出正则环的子环不一定是正则环；

(3) 对正则环 R 中任二元素 a,b，都有 R 中幂等元 e_1,e_2，使

$$Ra = Re_1,\ Ra + Rb = Re_2$$

证明 (1) 设 R 是一个 p- 环。

$p = 2$ 时，任 $a \in R$，均有 $a^2 = a$，故有 $a^3 = a$，即存在 $a' = a$，使 $aa'a = a$，因此 R 是正则环。

$p > 2$ 时，任 $a \in R$，均有 $a^p = a$，故存在 $a' = a^{p-2}$，使 $aa'a = a$，因此 R 是正则环。

由本章 §2 定理 6 知 p- 环是交换环，故非交换的正则环必不是 p- 环，如四元数除环是正则环，但不是 p- 环。

(2) 除环与域都是正则环，其中有理数域是正则环，但其子环整数环不是正则环。

(3) 由 R 是正则环可知任意 $a \in R$，存在 $a' \in R$，使 $aa'a = a$。

若令 $e_1 = a'a$，则 $ae_1 = a$ 且 $e_1^2 = a'(aa'a) = a'a = e_1$，故

$$Ra = Rae_1 \subseteq Re_1$$

又

$$Re_1 \subseteq Ra$$

故

$$Ra = Re_1$$

又任 $b \in R$，易知

$$Rb \subseteq Rbe_1 + R(b - be_1)$$

故由 $e_1 = a'a$ 及已证 $Ra = Re_1$ 得

$$Ra + Rb = Re_1 + R(b - be_1)$$

记 $R(b - be_1) = Re$，其中 $e = e^2 \in Re$，因此

$$e \in R(b - be_1)$$

设 $e = r(b - be_1)$，则 $ee_1 = 0$，令 $e_3 = e - e_1e$，故

$$ee_3 = e, e_3^2 = e_3, e_1e_3 = e_3e_1 = 0$$

又 $e_3 \in Re, e \in Re_3$，故 $Re = Re_3$，于是

$$Ra + Rb = Re_1 + Re_3$$

从而若令 $e_2 = e_1 + e_3$，则有 $e_2^2 = e_2$ 且

$$r_1e_1 + r_2e_3 = (r_1e_1 + r_2e_3)(e_1 + e_3) \in Re_2$$

$$Re_1 + Re_3 = Re_2$$

于是有

$$Ra + Rb = Re_2$$

15. 设 R 是一个正则环。证明：若 R 中元素 a 对 R 中任意元素 x 都有 $b \in R$，使

$$ax + b + axb = 0$$

则必 $a = 0$。

证明　依题意，任 $a \in R$，存在 $a' \in R$，使 $aa'a = a$，从而对 a，$-a'$ 存在 $b \in R$，使

$$a(-a') + b + a(-a')b = 0$$

上式两边同时左乘 aa'，则

$$-aa'aa' + aa'b - aa'aa'b = 0$$

由于 $aa'a = a$，进而有

$$-aa' + aa'b - aa'b = 0, \text{即 } aa' = 0$$

在 $aa' = 0$ 两边同时右乘 a，结合 $aa'a = a$ 得

$$a = aa'a = 0a = 0$$

16. 设 $G = \langle a \rangle$ 为 n 阶循环群，$U(Z_n)$ 为模 n 剩余类环 Z_n 的单位群。证明：

$$\text{Aut}G \cong U(Z_n)$$

再由此利用数论结论证明：

$$\text{Aut}G \text{ 是循环群} \Leftrightarrow n \text{ 为 } 2,4,p^k,2p^k(p \text{ 为奇素数})$$

证明　因为 G 的自同构把生成元 a 仍变成生成元 a^m，又 $|U(Z_n)| = \varphi(n)$，其中 $\varphi(n)$ 为欧拉函数，所以 $(m,n) = 1$ 且 $|\text{Aut}G| = \varphi(n)$，定义

$$\varphi: \sigma \longrightarrow m$$

其中 σ 为自同构且 $\sigma(a) = a^m$，则 φ 是 $\text{Aut}G$ 到 $U(Z_n)$ 的一个同构映射，故

$$\text{Aut}G \cong U(Z_n)$$

因而若 $U(Z_n)$ 是循环群，则其充要条件为 $\text{Aut}G$ 是循环群。由数论知 $U(Z_n)$ 为循环群的充要条件是 $n = 2,4,p^k$ 或 $2p^k$，其中 p 为奇素数，即有命题

$$\text{Aut}G \text{ 是循环群} \Leftrightarrow n \text{ 为 } 2,4,p^k,2p^k(p \text{ 为奇素数})$$

17. 如果一个环的特征是素数。问：这个环是否一定无零因子？

解 模 p(p 为素数) 的剩余类环 Z_p 上的 $n>1$ 阶全阵环，其中特征为素数，但该环有零因子，从而结论不一定成立。

---

18. 证明：若加群 G 为可分解群，则其自同态环不是域。

证明 不妨设 $G=H\oplus R$，其中 $H,R<G$，任 $h\in H$，$r\in R$，定义

$$\sigma: h+r\longrightarrow h,\ \tau: h+r\longrightarrow r$$

则 σ 与 τ 为 G 的两个自同态，显见有

$$\sigma\tau(h+r)=0$$

出 h 与 r 的任意性可知 $\sigma\tau=0$，故 G 的自同态环有零因子存在，从而不是域。

---

19. 证明：有理数域 Q 的加群 $(Q,+)$ 的自同态环与 Q 同构。

证明 加群 $(Q,+)$ 的自同态环记为 $\mathrm{End}(Q,+)$。任 $\sigma\in\mathrm{End}(Q,+)$，若令 $\sigma(1)=a$，由 σ 为同态。故任有理数 $\frac{n}{m}$ 均有 $\sigma\left(\frac{n}{m}\right)=\frac{n}{m}a$，即 $\sigma(1)$ 完全确定了 $(Q,+)$ 的自同态 σ。任意 $\sigma\in\mathrm{End}(Q,+)$，定义

$$\varphi: \sigma\to\sigma(1)$$

则 φ 是 $\mathrm{End}(Q,+)$ 到 Q 的一个双射。又任意的 $\sigma,\tau\in\mathrm{End}(Q,+)$，

$$\begin{aligned}\varphi(\sigma+\tau)&=(\sigma+\tau)(1)=\sigma(1)+\tau(1)\\&=\varphi(\sigma)+\varphi(\tau)\\ \varphi(\sigma\tau)&=\sigma\tau(1)=\sigma(\tau(1))\\&=\sigma(a)=a\sigma(1)\\&=\tau(1)\sigma(1)=\sigma(1)\tau(1)\\&=\varphi(\sigma)\varphi(\tau)\end{aligned}$$

因此综上可知 φ 是 $\mathrm{End}(Q,+)$ 到 Q 的一个同构映射，即有

$$\mathrm{End}(Q,+)\cong Q$$

---

20. 在所有 n 阶循环环中，有且只有 $T(n)$ 个是互不同构的。其中 $T(n)$ 表示 n 的正因数的个数。

证明 ① 由于模 n 剩余类环为一个 n 阶循环环，故 n 阶循环环是存在的，

现设 $R = \langle a \rangle$，且

$$a^2 = ka \quad (0 \leqslant k < n)$$

则 R 共有 $\varphi(n)$ 个生成元，设为

$$r_1 a, r_2 a, \cdots, r_{\varphi(n)} a$$

其中 $r_1 = 1, 1 \leqslant r_i < n, (r_i, n) = 1 (i = 1, 2, \cdots, \varphi(n); \varphi(n)$ 为欧拉函数)。

又设$(k,n) = d$，则存在上面的某 r_i 及整数 s，满足

$$kr_i + ns = d$$

于是由 $a^2 = ka$ 得

$$\begin{aligned}(r_i a)^2 &= (kr_i)(r_i a) \\ &= (d - ns)(r_i a) = d(r_i a)\end{aligned}$$

即对 n 阶循环环来说，总存在 R 的生成元 $r_i a$ 及 n 的正因数 d，使上式成立，故由本章习 §5 第 8 题知，互不同构的 n 阶循环环不超过 $T(n)$ 个。

② 设 $R = \langle a \rangle, \overline{R} = \langle b \rangle$ 是两个 n 阶循环环，且

$$a^2 = ka, b^2 = hb$$

$$k \mid n, h \mid n, 0 \leqslant k, h \leqslant n - 1, k \neq h$$

下证 R 与 $\overline{R}$ 不同构。由本章 §5 第 8 题知即要证明整数组

$$kr_1, kr_2, \cdots, kr_{\varphi(n)} \text{ 与 } hr_1, hr_2, \cdots, hr_{\varphi(n)}$$

中对模 n 没有同余的。否则，设 kr_i 与 hr_j 对模 n 同余，即

$$kr_i = nq_1 + r, hr_j = nq_2 + r \quad (0 \leqslant r < n)$$

则由 $k \mid n, h \mid n$ 得 $k \mid r, h \mid r$，从而 $k \mid h r_j$，但由于 $(r_j, n) = 1, k \mid n$，故 $(r_j, k) = 1$，因此 $k \mid h$，同理可得 $h \mid k$。从而 $h = k$，矛盾。

所以综合 ①、② 可知，在所有 n 阶循环环中，有且只有 $T(n)$ 个是互不同构的。

---

21. 设 $Z[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in Z\}$ 为 Gauss 整环。问：环 $Z[\mathrm{i}]/\langle 1 + \mathrm{i} \rangle$ 有多少个元素？是否为域？

解 $Z[\mathrm{i}]$ 是有单位元的可换环，故

$$\begin{aligned}\langle 1 + \mathrm{i} \rangle &= \{(x + y\mathrm{i})(1 + \mathrm{i}) \mid x + y\mathrm{i} \in Z[\mathrm{i}]\} \\ &= \{(x - y) + (x + y)\mathrm{i} \mid x, y \in Z\}\end{aligned}$$

又由于整数 k, l 具有相同的奇偶性当且仅当存在整数 x, y 满足

$$k = x - y, l = x + y$$

因此对于 $k+li \in Z[\mathrm{i}]$，$k+li \in \langle 1+\mathrm{i} \rangle$ 当且仅当 k 与 l 具有相同的奇偶性。

从而由上述证明可知 $1 \in Z[\mathrm{i}]$，但 $1 \notin \langle 1+\mathrm{i} \rangle$，任取 $m+n\mathrm{i} \in Z[\mathrm{i}]$，若 $m+n\mathrm{i} \notin \langle 1+\mathrm{i} \rangle$，则 m 与 n 有相反的奇偶性，故 $m-1$ 与 n 就有相同的奇偶性，因此

$$m+n\mathrm{i}-1=(m-1)+n\mathrm{i} \in \langle 1+\mathrm{i} \rangle$$

即 $m+n\mathrm{i}+(1+\mathrm{i})=1+\langle 1+\mathrm{i} \rangle$，从而 $Z[\mathrm{i}]/\langle 1+\mathrm{i} \rangle$ 共有两个元素

$$\langle 1+\mathrm{i} \rangle \text{ 及 } 1+\langle 1+\mathrm{i} \rangle$$

显见，$\langle 1+\mathrm{i} \rangle$ 与 $1+\langle 1+\mathrm{i} \rangle$ 作成一个 2 元域。

---

22. 设环 R 有一个分类，S 是所有类 $[a],[b],[c],\cdots$ 的集合。证明：如果

$$[x]+[y]=[x+y]$$
$$[x][y]=[xy]$$

是 S 的两个代数运算，则 $[0]$ 是 R 的理想，且给定的分类恰好是关于 $[0]$ 的陪集。

证明 先证 $[0]$ 为 R 的理想。

任意的 $a,b \in [0]$，则 $[a]=[b]=[0]$，故

$$a-b=a+(-b) \in [a]+[-b]=[b]+[-b]=[b-b]=[0]$$

于是

$$a-b \in [0]$$

再任取 $r \in R$，则

$$[ra]=[r][a]=[r][0]=[r0]=[0]$$

即
$$ra \in [0]$$

又

$$[ar]=[a][r]=[0][r]=[0r]=[0]$$

故
$$ar \in [0]$$

综上可知，$[0]$ 为 R 的理想。

下证所给的每一个类恰好是关于理想 $[0]$ 的一个陪集，即证

$$[x]=x+[0]$$

对任意的 $y \in [x]$，有

$y-x=y+(-x) \in [x]+[-x]=[0]$，即 $y \in x+[0]$

故$[x] \leqslant x+[0]$，又由于

$$x+[0] \leqslant [x]+[0]=[x+0]=[x]$$

所以$[x]=x+[0]$，从而所给的每一个类恰好是关于理想$[0]$的一个陪集。

---

23. 令 R 是一个有单位元的可换环，N 是 R 的全体幂零元作成的集合，证明：$N \lhd R$ 且 R/N 不含非零幂零元。

证明　先证 $N \lhd R$。

显见 $N \neq 0$，任 $a,b \in N$，则存在正整数 m,n 使

$$a^m=0, b^n=0$$

从而由 R 可换得

$$(a-b)^{m+n}=a^{m+n}-C_{m+n}^1 a^{m+n-1}b+\cdots+(-1)^n C_{m+n}^n a^m b^n+$$
$$(-1)^{n+1}C_{m+n}^{n+1}a^{m-1}b^{n+1}+\cdots+(-1)^{m+n}b^{m+n}=0$$

故

$$a-b \in N$$

再任取 $r \in R$，则由 R 可换得

$$(ra)^m=(ar)^m=a^m r^m=0$$

即

$$ra、ar \in N$$

综上可知 $N \lhd R$。

下证 R/N 不含非零幂零元。

设 aN 是环 R/N 的任一幂零元，且

$$(aN)^m=\overline{0}，即 a^m N=\overline{0}$$

故 $a^m \in N$，又 N 是 R 的全体幂零元作成的集合，故存在整数 n，使

$$a^{mn}=(a^m)^n=0$$

因此 $a \in N$，$aN=\overline{0}$，从而 R/N 无非零幂零元。

---

24. 设 N_1,N_2 是环 R 的两个理想，规定

$$N_1N_2=\{有限和 \sum a_ib_i \mid a_i \in N_1, b_i \in N_2\}$$

证明：$N_1N_2 \lhd R$，且 $N_1N_2 \subseteq N_1 \cap N_2$。

证明　由$N_1 \lhd R$，$N_2 \lhd R$ 及有限和的差仍为有限和可知 $N_1N_2 \lhd R$。

且由$N_1 \lhd R, N_2 \lhd R$分别有$N_1N_2 \subseteq N_1, N_1N_2 \subseteq N_2$，
故

$$N_1N_2 \subseteq N_1 \cap N_2$$

---

25. 证明：n阶循环环R是域的充分必要条件是，n为素数且R不是零乘环。

证明 设$R = \langle a \rangle = \{0, a, 2a, \cdots, (n-1)a\}$，且

$$|a| = n, a^2 = ka \quad (0 \leqslant k < n)$$

"$\Rightarrow$"若R是域，故可知R不是零乘环，下证n为素数。

若存在$1 < n_1, n_2 < n$，使$n = n_1n_2$，则$n_1a \neq 0, n_2a \neq 0$，而$n_1a \cdot n_2a = n_1n_2a^2 = na^2 = 0$，这与$R$是域矛盾，因此$n$必为素数。

"$\Leftarrow$"若R不是零乘环且n为素数，则由式(*)知$k \neq 0$，从而若存在整数s, t，使

$$sa \cdot ta = sta^2 = (stk)a = 0$$

则由$|a| = n$知$n \mid stk$，而$(k, n) = 1$故$n \mid s$或$n \mid t$，于是

$$sa = 0 \text{ 或 } ta = 0$$

故R无零因子。又n为素数，R的阶必大于1，从而R是一个除环，又R有限(或可换)，故R为一个域。

---

26. 如果环R是单环或者R的所有非平凡理想都是域，则称R为NF-环。证明：若环R的阶为pq(p, q是互异素数)，则

$$R \text{ 是 NF- 环} \Leftrightarrow R \text{ 有单位元}$$

证明 "$\Rightarrow$" 由于环R的阶为pq(p, q为互异素数)，故由本章§1定理3知环R必为循环环，设$R = \langle a \rangle$，因此$a^2 = ka$，k为整数。

① 先证若n阶循环环R有单位元当且仅当$(k, n) = 1$。

若R有单位元$e = ra$，则

$$ae = a$$

$$a = ae = a(ra) = ra^2 = (rk)a$$

$$(rk - 1)a = 0$$

故$n \mid rk - 1$，设$rk - 1 = nq$，则

$$rk + n(-q) = 1$$

因而
$$(k, n) = 1$$

反之，若$(k,n)=1$，则存在整数u,v，使

$$ku+nv=1$$

从而对任意$sa\in R$，有

$$(sa)(ua)=(suk)a=s(1-nv)a=sa$$

又R是可换环，故ua是R的单位元，即单位元存在。

②n阶循环环R有$2^{\psi(n)-\psi(k,n)}$个幂等元。其中$\psi(n)$为n的不同素因数的个数，$\psi(k,n)$为k与n的最大公因数(k,n)的不同素因数的个数。

不妨设n标准分解式为$n=p_1^{s_1}p_2^{s_2}\cdots p_m^{s_m}$，则由$ta$为$n$阶循环环的幂等元当且仅当$n|kt^2-t$可知，$R$中幂等元的个数即为同余式

$$kx^2-x\equiv 0(\bmod n)$$

的解的个数，而这个同余式的解的个数和m个同余式

$$kx^2-x\equiv 0(\bmod p_i^{s_i})\quad (i=1,2,\cdots,m)$$

的解的个数的乘积相等。而对某取定i，当$p_i\mid k$时，上式只有零解，当$p_i\nmid k$时，由于$(p_i^{s_i},k)=1$，可知存在整数u,v，使

$$p_i^{s_i}u+kv=1$$

从而$p_i\nmid v$，$p_i^{s_i}\mid kv-1$，$p_i^{s_i}\mid v(kv-1)=kv^2-v$，故$v$是

$$kx^2-x\equiv 0(\bmod p_i^{s_i})$$

的一个非零解。又显见0也为其解，且上方程不存在别的解，因而该方程只有两个解，所以同余式方程$kx^2-x\equiv 0(\bmod n)$有$2^{\psi(n)-\psi(k,n)}$个解，即R有$2^{\psi(n)-\psi(k,n)}$个幂等元。

③ 再证n阶循环环$R=\langle a\rangle(a^2=ka)$的$T(n)$个子环(理想)中有$2^{\psi(n)-\psi(k,n)}$个有单位元的子环，它们正好都是由幂等生成元生成的子环(参见所证②)。

不妨设e是环R的一个幂等元，$\langle e\rangle$为e生成的一个子环，任$x\in\langle e\rangle$，则$x=re$，且

$$xe=ex=ere=re^2=re=x$$

故e为子环$\langle e\rangle$的单位元。

若e'为环R的另一幂等元，且$\langle e\rangle=\langle e'\rangle$，则由上述证明知$e'$也是子环$\langle e\rangle$的单位元，故$e'=e$，即不同的幂等元生成不同的有单位元的子环。

又设$N\leqslant R$，且N有单位元e，则$\langle e\rangle\subseteq N$。而任$x\in N$，有$xe=x$。又$\langle e\rangle$为子环，故也是理想，从而$xe\in\langle e\rangle$，因此$N\subseteq\langle e\rangle$，故的$N=\langle e\rangle$。

下面证明 pq 阶(p,q 为互异素数)NF-环 R 有单位元。

否则,由上述所证明 ①,k 与 pq 不互素,则 $\psi(pq)=2,\psi(k,pq)=1$。从而由上述所证 ③ 知 R 有 $2^{\psi(pq)-\psi(k,pq)}=2$ 个子环有单位元。

但是 R 有 $T(pq)=4$ 个子环,从而 R 存在无单位元的非平凡子环,当然不能是域,这同 R 是 NF-环矛盾。所以 R 必有单位元。

"$\Leftarrow$" 由必要性证明知 R 为 pq 阶循环环,且有 $T(pq)=4$ 个子环。若 R 有单位元,则这 4 个子环都是有单位元的循环环,由于 p、q 是互异素数,故这四个子环的阶分别为 $1,p,q,pq$。不妨设其中两个非平凡子环为

$$R_1=\{0,e_1,2e_1,\cdots,(p-1)e_1\}$$

$$R_2=\{0,e_2,2e_2,\cdots,(q-1)e_2\}$$

其中 e_i 为 $R_i(i=1,2)$ 的单位元,由上面第 25 题知 R_1 与 R_2 都是域,从而 R 是 NF-环。

---

27. 设 R 为 p^2(p 为素数)阶环。证明:

$$R\text{ 是 NF-环}\Leftrightarrow R\text{ 是域或 }R\cong Z_p\oplus Z_p$$

证明 充分性显然,下仅证必要性。

设 R 是 NF-环,则 R 中不存在 p^2 阶元素,否则若存在 $a\in R$,且 $|a|=p^2$,则

$$\langle pa\rangle=\{0,pa,2pa,\cdots,(p-1)pa\}$$

为 R 的一个 p 阶子环,且是一个零乘环。这同 R 是 NF-环矛盾,因此任 $a\in R$,$|a|=p$。

如果有限阶 NF-环 R 不是域,则由本章 §3 推论知 R 必有零因子:$x\neq 0,y\neq 0,xy=0$,从而由上述所证有 $|x|=|y|=p$,设

$$R_1=\{0,x,2x,\cdots,(p-1)x\},R_2=\{0,y,2y,\cdots,(p-1)y\}$$

如果 $x^2=0$,则 R_1 是 p 阶零乘环,这与 R 是 NF-环矛盾。因此 $x^2\neq 0$,且 $|x^2|=p$。任取 $b\in R_1\cap R_2$,则

$$b=sx=ty$$

其中 $0\leqslant s,t<p$,故

$$sx^2=x(ty)=t(xy)=0$$

从而 $p\mid s$。故 $s=0,b=0$,于是有

$$R_1\cap R_2=\{0\},R=R_1\oplus R_2\text{(作为加群)}$$

又 $x^2 \in R$，故存在 $k_1, k_2(0 \leqslant k_1, k_2 < p)$，使

$$x^2 = k_1 x + k_2 y$$

于是 $x^2 y = k_1 xy + k_2 y^2$，而 $xy = 0$，因此 $k_2 y^2 = 0$。

同理可证 $y^2 \neq 0$，且 $|y^2| = p$，故由 $k_2 y^2 = 0$ 知 $p \mid k_2, k_2 = 0$，因此

$$x^2 = k_1 x + k_2 y = k_1 x \in R_1$$

其中 $1 \leqslant k_1 < p$，从而 R_1 是 R 的一个 p 阶子环，又 R 是 NF- 环，故 R_1 为 p 阶域，于是

$$R_1 \cong Z_p$$

同理可证 $R_2 \cong Z_p$，从而 $R \cong Z_p \oplus Z_p$。

---

28. 证明本章 §2 引理：

设 R 是有单位元的交换环，$|R| > 1$，又

$$\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, \boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, a_{ij} \in R$$

则 R 上齐次线性方程组 $\boldsymbol{Ax} = \boldsymbol{0}$ 在 R 中有非零解的充要条件是

$$r(\boldsymbol{A}) < n$$

证明 “$\Rightarrow$” 设 $\boldsymbol{Ax} = \boldsymbol{0}$ 在 R 中有非零解 $\boldsymbol{x} = (k_1, k_2, \cdots, k_n)^{\mathrm{T}}$，当 $m < n$ 时，显然有 $r(\boldsymbol{A}) < n$，故下设 $m \geqslant n$，且不妨设 $k_1 \neq 0$。

设 D 为 $\boldsymbol{A}$ 的一个 n 阶子式，不妨设

$$D = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

则 D 中元素 a_{i1} 的代数余子式 $\boldsymbol{A}_{i1}(i = 1, 2, \cdots, n)$ 依次分别乘以以下各式

$$a_{11}k_1 + a_{12}k_2 + \cdots + a_{1n}k_n = 0$$
$$a_{21}k_1 + a_{22}k_2 + \cdots + a_{2n}k_n = 0$$
$$\vdots$$
$$a_{n1}k_1 + a_{n2}k_2 + \cdots + a_{nn}k_n = 0$$

的两端并左右分别相加，即可得到

$$Dk_1 + 0 \cdot k_2 + \cdots + 0 \cdot k_n = 0$$

即
$$k_1 D = 0$$

类似可得对于 A 的其它 n 阶子式 M_n 均有 $k_1 M_n = 0$，于是 k_1 是 A 的所有 n 阶子式所作集合 S_n 的一个真零化子，据本章 §2 定义 6 知

$$r(A) < n$$

"$\Leftarrow$" 设 $r(A) = r < n$。

由于可用系数和常数项全为 0 的方程补充，使方程组中方程的个数大于 $r(A)$，故可设

$$r(A) = r < m$$

由 $r(A) = r$ 可知 S_{r+1} 有真零化子 $k(k \neq 0)$。故对 A 的任意 $r+1$ 阶子式 M_{r+1}，均有 $kM_{r+1} = 0$。

若 $r = 0$，则 k 零化 A 中每一元素，故

$$x = (k, k, \cdots, k)^{\mathrm{T}}$$

是 $Ax = 0$ 的一个非零解。

若 $r > 0$，则由 S_r 无真零化子和存在 A 的某 r 阶子式 M_r 使 $kM_r \neq 0$，不妨设

$$M_r = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rr} \end{vmatrix}, M_{r+1} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1,r+1} \\ a_{21} & a_{22} & \cdots & a_{2,r+1} \\ \vdots & \vdots & & \vdots \\ a_{r+1,1} & a_{r+1,2} & \cdots & a_{r+1,r+1} \end{vmatrix}$$

d_i 为 M_{r+1} 中元素 $a_{r+1,i}(i = 1, 2, \cdots, r+1)$ 的代数余子式，则 $d_{r+1} = M_r$。下证

$$x_i = kd_i \quad (i = 1, 2, \cdots, r+1)$$
$$x_i = 0 \quad (i = r+2, \cdots, n)$$

为 $Ax = 0$ 的一个非零解。记上述 $x_i(i = 1, 2, \cdots, n)$ 为分量构成 x_1

由 $x_{r+1} = kd_{r+1} = kM_r \neq 0$ 知 $x_1 \neq 0$。

又当 $i = 1, 2, \cdots, r$ 时，

$$a_{i1}kd_1 + \cdots + a_{i,r+1}kd_{r+1} = k(a_{i1}d_1 + \cdots + a_{i,r+1}d_{r+1}) = k \cdot 0 = 0$$

故 x_1 满足 $Ax = 0$ 中的前 r 个方程。

下取 A 的 $r+1$ 阶子式

$$D_{r+1}=\begin{vmatrix} & & a_{1,r+1} \\ & M_r & \vdots \\ a_{j1} & \cdots & a_{j,r+1}\end{vmatrix}$$

其中 $r<j\leqslant m$，按 D_{r+1} 的最后一行展开得

$$D_{r+1}=a_{j1}d_1+\cdots+a_{j,r+1}d_{r+1}$$

故

$$a_{j1}(kd_1)+\cdots+a_{j,r+1}(kd_{r+1})=k(a_{j1}d_1+\cdots+a_{j,r+1}d_{r+1})=kD_{r+1}=0$$

即 $\boldsymbol{x}_1$ 也满足 $\boldsymbol{Ax}=\boldsymbol{0}$ 的后 $m-r$ 个方程，所以，$\boldsymbol{Ax}=\boldsymbol{0}$ 有非零解。

---

29. 设 $R[x]$ 是有单位元的交换环 R 上的多项式环。证明：

$0\neq f(x)$ 是 $R[x]$ 的零因子 $\Leftrightarrow$ 有 $0\neq c\in R$ 使 $cf(x)=0$

证明 由于充分性显见，故仅证必要性。

设 $f(x)\neq 0$，$f(x)$ 是 $R[x]$ 的零因子。若 $f(x)\in R$，则结论显然成立。下设

$$f(x)=a_0+a_1x+\cdots+a_mx^m$$

其中 $0\neq a_m\in R$，$m\geqslant 1$，且存在 R 上的多项式

$$g(x)=b_0+b_1x+\cdots+b_nx^n\neq 0\quad(0\neq b_n\in R)$$

使
$$g(x)f(x)=0$$

下证存在次数小于 n 的多项式 $h(x)$，使 $h(x)f(x)=0$ 仍然成立。

由 $g(x)f(x)=0$ 可知

$$a_mb_n=0$$

故由 $a_mg(x)f(x)=0$ 可得

$$\begin{aligned}a_mg(x)&=a_m(b_0+b_1x+\cdots+b_{n-1}x^{n-1}+b_nx^n)\\&=a_m(b_0+b_1x+\cdots+b_{n-1}x^{n-1})\end{aligned}$$

从而若 $a_mg(x)\neq 0$，则由于其次数小于 n，令 $h(x)=a_mg(x)$，则得证。否则，若 $a_mg(x)=0$，则必有

$$a_mb_i=0\quad(i=0,1,\cdots,n-1)$$

于是

$$g(x)f(x)=(b_0+b_1x+\cdots+b_nx^n)\cdot(a_0+a_1x+\cdots+a_{m-1}x^{m-1})=0$$

故

$$a_{m-1}b_n=0$$

类似于上述讨论，若 $a_{m-1}g(x) \neq 0$，则由于其次数小于 n，可令 $h(x) = a_{m-1}g(x)$ 得证。否则若 $a_{m-1}g(x) = 0$，类似也可得到

$$a_{m-2}b_n = 0$$

将这样的讨论继续下去，则或存在次数小于 n 的多项式 $h(x)$，使 $h(x)f(x) = 0$，或者有

$$g(x)f(x) = g(x)a_0 = 0$$

即 $a_m g(x) = a_{m-1}g(x) = \cdots = a_1 g(x) = a_0 g(x) = 0$，从而有

$$a_m b_n = a_{m-1}b_n = \cdots = a_1 b_n = a_0 b_n = 0$$

于是令 $c = b_n$，则 $cf(x) = 0$，其中 $0 \neq c = b_n \in R$。

---

30. 设 Z_n^* 为模 n 剩余类环 Z_n 的单位群，证明：Z_n^* 中每个元素都满足 $x^2 = 1$ 的充要条件是，n 为以下整数：

$$2,3,4,6,8,12,24$$

证明 “$\Leftarrow$” 当 n 为上述 7 个整数时，直接验算即可得 Z_n^* 中每个元素都满足 $x^2 = 1$。

“$\Rightarrow$” 只需证明当 n 不是上述 7 个整数时，Z_n^* 中存在元素不满足 $x^2 = 1$。

为讨论方便，以下将 $\bar{a} \in Z_n^*$ 简记为 $a \in Z_n^*$。

①$n = 2^s \cdot 3^t$ 时，其中 $s \geqslant 4, t = 0$ 或 1。

如果 $t = 0$，则 $n = 2^s$，由 $3 \in Z_n^*$ 及 $s \geqslant 4$ 知

$$3^2 = 9 < 2^4 \leqslant 2^s$$

故
$$3^2 = 9 \neq 1$$

如果 $t = 1$，则 $n = 3 \cdot 2^s$，由 $5 \in Z_n^*$ 及 $s \geqslant 4$ 知

$$5^2 = 25 < 3 \cdot 2^4 \leqslant 3 \cdot 2^s$$

故
$$5^2 = 25 \neq 1$$

②$n = 2^s \cdot 3^t$ 时，其中 $s \geqslant 0, t \geqslant 2$。

若 $s = 0$，则 $n = 3^t$，由 $2 \in Z_n^*$ 及 $t \geqslant 2$ 知

$$2^2 = 4 < 3^2 \leqslant 3^t$$

故
$$2^2 = 4 \neq 1$$

若 $s = 1, t = 2$，则 $n = 2 \cdot 3^2$，由 $5 \in Z_n^*$ 知 $5^2 = 25 \neq 1$

若 $s = 1, t > 2$，则 $n = 2 \cdot 3^t$，由 $5 \in Z_n^*$ 及 $t > 2$ 知

$$5^2=25<2\cdot 3^3\leqslant 2\cdot 3^t$$

故 $$5^2=25\neq 1$$

③ 当 $n=p^k$ 时，其中 $k\geqslant 1$，p 是大于 3 的素数，则由 $2\in Z_n^*$ 知

$$2^2=4<5\leqslant p^k$$

故 $$2^2=4\neq 1$$

④ 当 $n=2^s\cdot p^t$ 时，其中 $s\geqslant 1,t\geqslant 1$，$p$ 为大于 3 的素数，则由 $3\in Z_n^*$ 知

$$3^2=9<2\cdot 5\leqslant 2^s\cdot p^t$$

故 $$3^2=9\neq 1$$

⑤ 当 $n=2^s\cdot p_1^{t_1}p_2^{t_2}\cdots p_m^{t_m}$ 时，其中 $s\geqslant 0,m\geqslant 2,t_i\geqslant 1,p_1p_2\cdots p_m$ 为互异的素数。

由于 Z_n^* 是 $\varphi(n)$ 阶群，其中 $\varphi(n)$ 为欧拉函数，要证明 Z_n^* 中存在元素不满足方程 $x^2=1$，只需证明同余方程

$$x^2\equiv 1(\mathrm{mod}n)$$

的解的个数小于 $\varphi(n)$。

当 $s=0$ 或 1 时，因为同余方程 $x^2\equiv 1(\mathrm{mod}p_i^{t_i})(i=1,2,\cdots,m)$ 都有两个解，故同余方程 $x^2\equiv 1(\mathrm{mod}n)$ 有 2^m 个解。由于 $m\geqslant 2$，故

$$2^m<p_1^{t_1-1}p_2^{t_2-1}\cdots p_m^{t_m-1}(p_1-1)(p_2-1)\cdots(p_m-1)=\varphi(n)$$

当 $s=2$ 时，$n=2^2\cdot p_1^{t_1}p_2^{t_2}\cdots p_m^{t_m}$。因为 $x^2\equiv 1(\mathrm{mod}4)$ 有 2 个解，故同余方程 $x^2\equiv 1(\mathrm{mod}n)$ 有 2^{m+1} 个解，又 $m\geqslant 2$，故

$$2^{m+1}<2p_1^{t_1-1}p_2^{t_2-1}\cdots p_m^{t_m-1}(p_1-1)(p_2-1)\cdots(p_m-1)=\varphi(n)$$

当 $s>2$ 时，因为同余方程 $x^2\equiv 1(\mathrm{mod}2^s)$ 有 4 个解，故 $x^2\equiv 1(\mathrm{mod}n)$ 有 2^{m+2} 个解，由 $m\geqslant 2$ 可得

$$2^{m+2}<2^{s-1}p_1^{t_1-1}p_2^{t_2-1}\cdots p_m^{t_m-1}(p_1-1)(p_2-1)\cdots(p_m-1)=\varphi(n)$$

综上可知若 Z_n^* 中每个元素都满足 $x^2=1$，则 n 必取题中的 7 个整数。

第五章 惟一分解整环

导读

一、基本要求

1. 理解整除、单位、相伴元、平凡因子、真因子、素元、元的惟一分解的概念；

2. 理解公因子、最大公因子、互素等概念，掌握惟一分解整环的定义及性质；

3. 理解并掌握主理想整环和欧氏环的相关概念及基本性质；

4. 了解本原多项式的定义和性质，理解本原多项式的惟一分解。

二、重点与难点

1. 惟一分解整环的概念及性质；

2. 主理想整环和欧氏环的概念及性质。

知识点考点精要

本章中的环 K 为有单位元的整环且 $|K|>1$。

一、相伴元和不可约元

1. 定义

(1) 整除与因子

设 $a,b\in K$，若存在 $c\in K$，使

$$a = bc$$

则称 b 整除 a，或称 b 是 a 的一个因子，记为 $b \mid a$。否则称 b 不能整除 a，记为 $b \nmid a$。

(2) 单位

环 K 中有逆元的元素称为单位，或可逆元。

(3) 相伴与相伴元

在环 K 中，若 $a = b\varepsilon$，其中 ε 是 K 的一个单位，则称 a 与 b 相伴，并称 a 是 b 的相伴元。

注 ① 相伴关系是等价关系。

② 元素 a 与 b 相伴 $\Leftrightarrow a$ 与 b 互相整除。

(4) 平凡因子与真因子

$a \in K$，则 K 的单位及 a 的相伴元称为 a 的平凡因子或当然因子。若存在其他因子，则称为真因子或非平凡因子、非当然因子。

(5) 不可约元与可约元

设 $a \in K$，$a \neq 0$，且 a 不是单位。若 a 只有平凡因子，则称 a 为环 K 的一个不可约元；若 a 有非平凡因子，则称 a 为环 K 的一个可约元。

(6) 设 $a \in K$，若 K 中有不可约元 $p_1, p_2, \cdots, p_r$ 及不可约元 $q_1, q_2, \cdots, q_s$ 使

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

时就有 $r = s$，且适当交换不可约元的次序后，p_i 与 q_i 相伴 $(i = 1, 2, \cdots, r)$，则称元素 a 在 K 中可惟一分解。

注 环 K 中的零元及单位不能惟一分解。

(7) 素元

设 $p \in K$，$p \neq 0$，且 p 不是单位。若

$$p \mid ab \Rightarrow p \mid a \text{ 或 } p \mid b$$

则称 p 是 K 的一个素元。

2. 不可约元与单位的乘积

环 K 中不可约元与任何单位的乘积仍是 K 的不可约元。

3. 有真因子的条件

环 K 中非零元 a 有真因子的充要条件是在 K 中存在非单位 b，c 使

$$a = bc$$

4. 素元与不可约元的关系

整环 K 中的素元必为不可约元。

二、惟一分解整环的定义与性质

1. 定义

(1) 惟一分解整环

设 K 是有单位元的整环，若 K 中非零非单位的元素都能惟一分解，则称 K 为惟一分解整环。

(2) 公因子与最大公因子

在有单位元的整环 K 中，若 c 是每个元素 $a_i(i=1,2,\cdots,n)$ 的因子，则称 c 是这 n 个元素的一个公因子。

设 d 是 $a_i(i=1,2,\cdots,n)$ 的一个公因子，若 $a_1,a_2,\cdots,a_n$ 的任何公因子都是 d 的一个因子，则称 d 是 $a_1,a_2,\cdots,a_n$ 的一个最大公因子，记作

$$(a_1,a_2,\cdots,a_n)=d$$

(3) 互素

在有单位元的整环 K 中，若

$$(a_1,a_2,\cdots,a_n)=d$$

且 d 为单位，则称 $a_1,a_2,\cdots,a_n$ 互素，记作 $(a_1,a_2,\cdots,a_n)=1$。

2. 性质

(1) p 是惟一分解整环 K 的素元 $\Leftrightarrow p$ 是 K 的不可约元。

(2) 设 K 是有单位元的整环，若

①K 中每个非零非单位的元素都可分为不可约元的乘积；

②K 中的不可约元都是素元；

则 K 是一个惟一分解整环。

(3) 惟一分解整环 K 中任二元素都有最大公因子存在，且任二最大公因子间只差一个单位因子。

(4) 惟一分解整环 K 中，若 $a\mid bc$，$(a,b)=1$，则 $a\mid c$。

三、主理想整环

1. 定义

设 K 是有单位元的整环，若 K 的每一个理想都是一个主理想，则称 K

是一个主理想整环。

注 主理想整环的一个例子：Gauss 整环 $Z[i]$ 是主理想整环。

2. 性质

(1) 设 K 是一个主理想整环。若序列

$$a_1, a_2, \cdots, a_i, \cdots \quad (a_i \in K)$$

中，每个元素都是前一个元素的真因子，则这个序列必为有限序列。

(2) 主理想整环中不可约元生成的理想是极大理想。

(3) 主理想整环是惟一分解整环。

四、欧氏环

1. 定义

设 K 是一个有单位元的整环，若

(1) 存在一个从 $K-\{0\}$ 到非负整数集的映射 φ；

(2) φ 满足对任 $a \in K, b \in K$ 且 $b \neq 0$，存在 $q, r \in K$，使

$$a = bq + r, r = 0 \text{ 或 } \varphi(r) < \varphi(b)$$

则称 K 关于 φ 作成一个欧氏环。

2. 欧氏环与主理想整环的关系

欧氏环必是主理想整环，因而是惟一分解整环。

注 欧氏环 $\subset$ 主理想整环 $\subset$ 惟一分解整环 $\subset$ 有单位元整环。

五、惟一分解整环的多项式扩张

1. 定义

(1) 扩环

若环 R 是环 S 的一个子环，则称 S 是环 R 的一个扩环或扩张。

(2) 多项式扩张

设 K 是一个惟一分解整环，则其上的多项式环 $K[x]$ 便是 K 的一个扩张，或称为 K 的多项式扩张。

(3) 本原多项式

设 $f(x) \in K[x]$。若 $f(x)$ 的所有系数的最大公因子是一个单位(即所有系数互素)，则称 $f(x)$ 是一个本原多项式。

注 ① 零次多项式不是本原多项式；

② 零次多项式是本原的 $\Leftrightarrow$ 它是 K 的一个单位。

2. 本原多项式的性质

(1)(Gauss 引理)两个本原多项式的乘积仍是一个本原多项式。

(2)$K[x]$ 中两个本原多项式 $f_1(x)$ 与 $f_2(x)$ 在 $K[x]$ 中相伴的充要条件是二者在 $F[x]$ 中相伴,其中 F 是惟一分解整环 K 的分式域。

(3)$K[x]$ 中的本原多项式 $f(x)$ 在 $K[x]$ 中可约的充要条件是 $f(x)$ 在 $F[x]$ 中可约,其中 F 是惟一分解整环 K 的分式域。

3. 惟一分解整环多项式扩张的性质

(1) 惟一分解整环 K 的多项式扩张 $K[x]$ 也是惟一分解整环。

(2) 惟一分解整环 K 上的 $x_1, x_2, \cdots, x_n$ 是 n 个不相关的未定元,则 $K[x_1, x_2, \cdots, x_n]$ 也是惟一分解整环。

释疑解惑

一、关于素元

1. 素元可以看作整数环中素数的推广。素元 p 具有一个重要的性质,即

$$若\ p \mid ab,则\ p \mid a\ 或\ p \mid b$$

但这一性质对任意整环来说,并不一定成立。如整环

$$R = \{a + b\sqrt{-3} \mid a, b \in Z\}$$

$4 \in R$,且可分解为素元之积,其形式有两种

$$4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$$

故
$$2 \mid (1+\sqrt{-3})(1-\sqrt{-3})$$

又 $2, 1+\sqrt{-3}, 1-\sqrt{-3}$ 都为 R 的素元且 $1+\sqrt{-3}$ 与 $1-\sqrt{-3}$ 都不是 2 的相伴元,从而 $2 \nmid (1+\sqrt{-3}), 2 \nmid (1-\sqrt{-3})$。

2. 素元与素理想的关系

若 K 是一个阶大于 1 的有单位元的整环,p 为 K 中非零非单位的元素,则

$$p \text{ 是素元} \Leftrightarrow \langle p \rangle \text{ 是素理想}$$

这是因为，若 p 是素元且 $ab \in \langle p \rangle$，则由 K 是具有单位元的整环知

$$ab = pc \quad (c \in K)$$

即 $p \mid ab$，因此 $p \mid a$ 或 $p \mid b$，即 $a \in \langle p \rangle$ 或 $b \in \langle p \rangle$，$\langle p \rangle$ 为素理想，反之由素理想定义可知 p 为素元。

3. 素元与不可约元

整环 K 中的素元是不可约元，但不可约元未必是素元。如 3 是有单位元的整环 $Z[\sqrt{5}\mathrm{i}]$ 的不可约元，又由

$$9 = 3 \cdot 3 = (2+\sqrt{5}\mathrm{i})(2-\sqrt{5}\mathrm{i})$$

知 $3 \mid (2+\sqrt{5}\mathrm{i})(2-\sqrt{5}\mathrm{i})$，而 $3 \nmid (2+\sqrt{5}\mathrm{i})$，$3 \nmid (2-\sqrt{5}\mathrm{i})$，故 3 不是 $Z[\sqrt{5}\mathrm{i}]$ 的素元。

二、惟一分解整环与非惟一分解整环常用的例子

1. 惟一分解整环的例子，如

整数环 Z，$Z[x]$，域 F 上的多项式环 $F[x]$，Gauss 整环 $Z[\mathrm{i}]$，以及 $Z[\sqrt{2}\mathrm{i}]$（或 $Z[-\sqrt{2}]$），$Z[\sqrt{2}] = \{a + b\sqrt{2} \mid a,b \in Z\}$，$Z[\sqrt{3}] = \{a + b\sqrt{3} \mid a,b \in Z\}$ 等等。

2. 非惟一分解整环的例子，如

$Z[\sqrt{10}]$，$Z[\sqrt{5}\mathrm{i}]$，$Z[\sqrt{6}\mathrm{i}]$ 及 $Z[\sqrt{2}\mathrm{i}]$ 等。

三、关于主理想整环

1. 主理想整环必是惟一分解整环，但反之不真，如 $Z[x]$ 是一个惟一分解整环，但它不是主理想整环。

2. 主理想整环的子环未必是主理想整环（参见第 5 章 §3 第 3 题）。

3. 主理想整环的一个例子：Gauss 整环 $Z[\mathrm{i}]$。

4. 欧氏环必是主理想环。

四、几种环之间的关系

欧氏环 $\subset$ 主理想整环 $\subset$ 惟一分解整环 $\subset$ 有单位元整环。

典型题精讲

1. 证明:0 不是任何元的真因子。

证明 若 0 是元素 a 的真因子,则存在一个元素 ε,使 $a = 0 \cdot \varepsilon = 0$,由 $0 = \delta \cdot 0$(δ 是单位)可知 0 是 0 的相伴元,因而 0 不是 $a(=0)$ 的真因子。

---

2. 证明:在整环 $Z[i]$ 中 5 有惟一分解,并给出 5 的一种分解。

证法 1 显然 5 有分解

$$5 = (1+2i)(1-2i)$$

其中由本章 §5 第 12 题可知 $1+2i$ 与 $1-2i$(及 $-1+2i$ 与 $-1-2i$)均为不可约元。

下证分解惟一性。若还有

$$5 = d_1 d_2 \cdots d_n$$

其中 $d_i(i = 1,2,\cdots,n)$ 不可约,则

$$5^2 = |d_1|^2 \cdot |d_2|^2 \cdot \cdots \cdot |d_n|^2 \text{ 且 } |d_i|^2 \neq 1,25$$

从而只有 $n = 2$ 且 $|d_i|^2 = 5$,即

$$5 = d_1 d_2 \text{ 且 } |d_1|^2 = |d_2|^2 = 5$$

即 $d_2 = \overline{d}_1$,故 $5 = d_1\overline{d}_1$,从而 5 有惟一分解。

证法 2 因 $Z[i]$ 为主理想整环,从而为惟一分解整环,所以 $Z[i]$ 中每个非零非单位的元素都有惟一分解,于是 5 也有惟一分解。

---

3. 设 R 是一个只有有限个单位的惟一分解整环。证明:R 的任一非零元素仅有有限个因子。

证明 任取 $a(\neq 0) \in R$。

若 a 是单位,由于单位的因子只能是单位及 R 只有有限个单位可知 a 只有有限个因子。

若 a 不是单位,则 a 可惟一分解为 R 中素元的乘积,记为

$$a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$$

其中 $p_i(i=1,2,\cdots,n)$ 为互不相伴的素元,$k_i(i=1,2,\cdots,n)$ 为正整数。由

于 R 是惟一分解整环，则 a 的任一非单位因子 b 可设为

$$b=\varepsilon p_{i_1}^{s_{i_1}}p_{i_2}^{s_{i_2}}\cdots p_{i_t}^{s_{i_t}}$$

其中 ε 为单位，$1\leqslant i_1<i_2\cdots<i_t\leqslant n$，而

$$1\leqslant s_{i_j}\leqslant k_{i_j}\quad(j=1,2,\cdots,t)$$

又 R 的单位只有有限个，故这样的 b 也只能有有限个。

---

4. 证明：若 p 是惟一分解整环 R 的素元，则 p 也是多项式环 $R[x]$ 的素元。

证明　设 $p\mid f(x)g(x)$，则可令

$$f(x)g(x)=p\cdot q(x)$$

其中

$$q(x)\in R[x],f(x)=d_1f_1(x),g(x)=d_2g_1(x),q(x)=d_3q_1(x)$$

$$d_1,d_2,d_3\in R$$

且 $f_1(x),g_1(x),q_1(x)$ 为 $R[x]$ 中的本原多项式，从而

$$d_1d_2f_1(x)g_1(x)=pd_3q_1(x)$$

且 d_1d_2 与 pd_3 相伴（$f_1(x),g_1(x),q_1(x)$ 是本原多项式），即存在单位 $\varepsilon\in R$，使

$$d_1d_2=pd_3\varepsilon$$

又 p 为 R 的素元，从而 $p\mid d_1$ 或 $p\mid d_2$ 于是

$$p\mid f(x)\text{ 或 }p\mid g(x)$$

即 p 也是 $R[x]$ 的素元。

习题全解

§1　相伴元和不可约元(P230)

1. 证明：在有单位元的整环 K 中，二元素相伴的充要条件是二者互相整除。

证明　"⇒"　若 $a,b\in K$ 且 a 与 b 相伴，则

$$a=\varepsilon b,b=\varepsilon^{-1}a$$

其中 ε 为 K 的单位，所以 $a \mid b, b \mid a$。

"$\Leftarrow$" 若 $a,b \in K$ 且 $a \mid b, b \mid a$，则存在 $c,d \in K$，使得

$$b = da, a = cb$$

下证 c,d 都是 K 的单位。

若 $a = 0$，则必 $b = 0$，故有 $b = \varepsilon a$ 成立，其中 ε 为 K 的单位。

若 $a \neq 0$，由题意可得

$$a = cb = (cd)a$$

因 K 是一个有单位元的整环，即是一个无零因子环，故在 K 中消去律成立，消去 a 即得

$$cd = 1$$

从而 c,d 都是 K 的单位，故 a 与 b 相伴。

---

2. 设 p 是有单位元整环 K 的素元，ε 是 K 的单位，证明 εp 是 K 的素元。

证明 因为 $\varepsilon \neq 0, p \neq 0$ 及有单位元整环中无零因子，故 $\varepsilon p \neq 0$。

下证 εp 不是单位。否则存在单位 $\varepsilon' \in K$ 使

$$1 = \varepsilon'(\varepsilon p) = (\varepsilon'\varepsilon)p$$

即 p 是单位。与 p 是素元矛盾。故 εp 不是单位。

设 $\varepsilon p \mid ab$，则 $p \mid \varepsilon^{-1}ab$。由于 p 为素元，故 $p \mid \varepsilon^{-1}$ 或 $p \mid a$ 或 $p \mid b$。

若 $p \mid \varepsilon^{-1}$，则 $\varepsilon p \mid 1$，故 εp 为单位，与上面所证矛盾，因此 $p \mid a$ 或$p \mid b$。又由第 1 题知 $\varepsilon p \mid p$，从而 $\varepsilon p \mid a$ 或$\varepsilon p \mid b$。综上可知 εp 是 K 的素元。

---

3. 试指出环 $Z[x]$ 中的单位和不可约元。

解 易知 $Z[x]$ 中的单位仅有 1 与 -1。

设 $f(x) \in Z[x], a \in Z, f_1(x)$ 为本原多项式，且 $f(x) = af_1(x)$，则 $f(x)$ 为不可约元的充要条件是 a 为素数且 $f_1(x)$ 为 $Z[x]$ 的单位，或 a 为 Z 的单位且 $f_1(x)$ 为 $Z[x]$ 上的不可约多项式。从而可知 $Z[x]$ 的不可约元全体是一切（正负）素数及在 $Z[x]$ 上的所有本原不可约多项式（次数大于 0）。

---

4. 证明：在整环 $Z[\sqrt{5}\mathrm{i}] = \{a + b\sqrt{5}\mathrm{i} \mid a,b \in Z\}$ 中，元素 $2 + \sqrt{5}\mathrm{i}$ 不能整除 3。

证明 如果$(2+\sqrt{5}i)\mid 3$，则存在 $a,b\in Z$，使

$$(2+\sqrt{5}i)(a+b\sqrt{5}i)=3$$

整理即得

$$9(a+b\sqrt{5}i)=6-3\sqrt{5}i$$

比较系数可得 $3a=2$，这与 $a\in Z$ 矛盾，所以$(2+\sqrt{5}i)\nmid 3$。

---

5. 令 $K=\left\{\frac{m}{2^n}\middle| m\text{ 为整数},n\text{ 为非负整数}\right\}$，试指出环 K 中的单位和不可约元。

解 不妨设$\frac{m}{2^n}$为K 的一个单位，则存在$\frac{s}{2^t}\in K$，使得

$$\frac{m}{2^n}\cdot\frac{s}{2^t}=\frac{ms}{2^{n+t}}=1$$

即 $ms\mid 2^{n+t}$，从而 $m\mid 2^{n+t}$。令 $m=\pm 2^p$，则$\frac{m}{2^n}=\pm 2^{p-n}$。令 $r=p-n$，则 $r\in Z$。故 $\pm 2^r(r\in Z)$ 为 K 的单位，从而环 K 中所有单位为 $\{\pm 2^r\mid r\in Z\}$。

下面求环 K 中的不可约元。设$\frac{m}{2^n}\in K$ 且$\frac{m}{2^n}=\frac{s}{2^t}$，$2\nmid s$。

依上述过程可知 2^t 为单位，故$\frac{s}{2^t}$在K 中不可约当且仅当 s 在 Z 中不可约，从而 K 的所有不可约元为$\left\{\frac{1}{2^t}p\middle| t\in Z,p\text{ 为素数}\right\}$。

§2 惟一分解整环定义和性质(P235)

1. 证明：整数环上的多项式环 $Z[x]$ 是一个惟一分解整环。

证明 由本章§1第3题知 $Z[x]$ 的单位只有 ± 1，$Z[x]$ 的不可约元为一切(正、负)素数和次数大于0的 $Z[x]$ 上的本原不可约多项式。故任 $f(x)\in Z[x]$，且 $f(x)\neq 0,\pm 1$，则有

$$f(x)=ag(x)$$

(其中，$a\in Z$，$g(x)$ 是最高系数为正整数的本原多项式)且该表达式惟一。

若 $f(x)$ 是本原多项式，则 $f(x)$ 可惟一分解成不可约多项式之积；若

$f(x)$ 不是本原多项式，则上述 $f(x) = ag(x)$ 中的 a 可惟一分解为素数之积，而 $g(x)$ 除了符号差异，可惟一分解为 Z 上的不可约多项式之积。所以 $f(x)$ 可惟一分解为 $Z[x]$ 内不可约元之积，从而 $Z[x]$ 是惟一分解整环。

---

2. 证明本节推论：

惟一分解整环 K 中的元素 $a_1, a_2, \cdots, a_n$ 在 K 中有最大公因子存在，而且其任二最大公因子均相伴。

分析 由定理 3 及数学归纳法即可得证。

证明 （略）

---

3. 设 K 是一个有单位元的整环，$a, b \in K$。证明：主理想 $\langle a\rangle$ 与 $\langle b\rangle$ 相等当且仅当 a 与 b 相伴。

证明 “$\Rightarrow$” 若 $\langle a\rangle = \langle b\rangle$，则 $a \in \langle b\rangle$ 且 $b \in \langle a\rangle$，故存在 $c, d \in K$，使

$$a = bc, b = ad$$

从而有 $a = adc$。

若 $a = 0$，则由 $b = ad$ 知 $b = 0$，显然有 a 与 b 相伴。

若 $a \neq 0$，则由整环无零因子满足消去律知 $dc = 1$，故 c、d 为 K 的单位，从而 a 与 b 相伴。

“$\Leftarrow$” 若 a 与 b 相伴，则存在 K 的一个单位 ε，使 $a = \varepsilon b, b = \varepsilon^{-1} a$，从而

$$a \in \langle b\rangle, \langle a\rangle \subseteq \langle b\rangle$$

且

$$b \in \langle a\rangle, \langle b\rangle \subseteq \langle a\rangle$$

所以

$$\langle a\rangle = \langle b\rangle$$

---

4. 设 K 是一个有单位元的整环。证明：$K = \langle a\rangle \Leftrightarrow a$ 是 K 的单位。

证明 “$\Rightarrow$” 若 $K = \langle a\rangle$，则 $1 \in \langle a\rangle$，故存在 $b \in \langle a\rangle$，使 $ba = 1$，从而 a 是 K 的单位。

“$\Leftarrow$” 若 a 为 K 的单位，则 K 的单位元 $1 \in \langle a\rangle$，从而 $K = \langle a\rangle$。

---

5. 设 $a_1, a_2, \cdots, a_n$ 是惟一分解整环 K 中 n 个不全为 0 的元素，且在 K 中有

$$a_1 = db_1, a_2 = db_2, \cdots, a_n = db_n$$

证明：$(a_1,a_2,\cdots,a_n)=d \Leftrightarrow (b_1,b_2,\cdots,b_n)=1$

证明 "$\Rightarrow$" 设$(a_1,a_2,\cdots,a_n)=d$，且$b \mid b_i(i=1,2,\cdots,n)$。

下证b是单位。

否则，b可惟一分解成素元的乘积，不妨令p是这些素元中的一个，则$p \mid b_i$，可令$b_i=pc_i(i=1,2,\cdots,n)$，故由$a_i=db_i$可得

$$a_i=pdc_i, pd \mid a_i \quad (i=1,2,\cdots,n)$$

又$d=(a_1,a_2,\cdots,a_n)$，从而$pd \mid d$，因此存在$k\in K$，使$d=pdk$，于是由$d\neq 0$及K为整环无零因子可得$pk=1$，故p为单位，与p为素元矛盾，从而b为单位。综合上面所证，有$(b_1,b_2,\cdots,b_n)=1$。

"$\Leftarrow$" 若$(b_1,b_2,\cdots,b_n)=1$，设$(a_1,a_2,\cdots,a_n)=d_0$，则由$a_i=db_i$ $(i=1,2,\cdots,n)$可知$d \mid d_0$，不妨设

$$d_0=dd_1, a_i=d_0c_i \quad (i=1,2,\cdots,n)$$

于是有

$$a_i=db_i=dd_1c_i \quad (i=1,2,\cdots,n)$$

因K中无零因子，由消去律得$b_i=d_1c_i(i=1,2,\cdots,n)$。

故$d_1 \mid b_i(i=1,2,\cdots,n)$，而$(b_1,b_2,\cdots,b_n)=1$，因此$d_1$为单位，$d$也是$a_1,a_2,\cdots,a_n$的最大公因子，即

$$(a_1,a_2,\cdots,a_n)=d$$

§3 主理想整环(P238)

1. 证明：在主理想整环中，P是素理想当且仅当P由素元生成。

证明 "$\Rightarrow$" 设$P=\langle\alpha\rangle$为素理想，且若$\alpha \mid ab$，则

$$ab\in\langle\alpha\rangle=P$$

而P为素理想，故

$$a\in\langle\alpha\rangle \text{ 或 } b\in\langle\alpha\rangle$$

从而 $$\alpha \mid a \text{ 或 } \alpha \mid b$$

故α为素元。

"$\Leftarrow$" 若α为素元，且$ab\in P=\langle\alpha\rangle$，即$\alpha \mid ab$，故

$$\alpha \mid a \text{ 或 } \alpha \mid b$$

因此$a\in\langle\alpha\rangle$或$b\in\langle\alpha\rangle$，从而$P=\langle\alpha\rangle$为素理想。

2. 设 K 是主理想整环，又 $\langle a,b\rangle=\langle d\rangle$，证明：$d$ 是 a,b 的一个最大公因子。由此进一步指出，a 与 b 的任何最大公因子 d' 均可表为

$$d'=as+bt \quad (s,t\in K)$$

证明 由 K 是主理想整环知

$$a,b\in\langle a,b\rangle=\langle d\rangle$$

故 $d\mid a$ 且 $d\mid b$，即 d 是 a,b 的一个公因子。

设 c 是 a,b 的另一公因子，即 $c\mid a$ 且 $c\mid b$，则 $a\in\langle c\rangle,b\in\langle c\rangle$，故

$$d\in\langle d\rangle=\langle a,b\rangle\subseteq\langle c\rangle$$

从而 $c\mid d$，这说明 d 是 a,b 的最大公因子。

又由 $\langle a,b\rangle=\{ak_1+bk_2\mid k_1,k_2\in K\}$ 及上式可得，存在 $s,t\in K$，使

$$d'=as+bt$$

---

3. 问：主理想整环的子环是否仍是主理想整环？请证明或举出反例。

解 在第四章 §6 例 5 中证明了多项式环 $Z[x]$ 的理想 $\langle 2,x\rangle$ 不是主理想，故 $Z[x]$ 不是一个主理想整环，而 $Z[x]$ 是主理想整环 $Q[x]$ 的一个子环，因此可以说明，主理想整环的子环未必是主理想整环。

---

4. 设 K',K 是两个主理想整环，且 $K'\leqslant K$，又 $a,b\in K'$，d 是 a 与 b 在 K' 中的最大公因子，证明：d 也是 a 与 b 在 K 中的一个最大公因子。

证明 显然 d 是 a 与 b 在 K 中的公因子。下证 d 是最大公因子。

不妨设 c 是 K 中 a 与 b 的任一公因子，且 $a=ca',b=cb'$，又由本章 §3 第 2 题知，存在 $s,t\in K'$，使

$$d=as+bt=c(a's+b't)$$

即 $c\mid d$，从而 d 是 a 与 b 在 K 中的一个最大公因子。

---

5. 设 K 是一个主理想整环，又 $0\neq a\in K$。证明：在 K 中仅有有限个理想包含 a。

证明 若 a 不是 K 的单位，则由主理想整环是惟一分解整环可知，存在 $p_1,p_2,\cdots,p_n$（p_i 为素元），使

$$a=p_1p_2\cdots p_n$$

故 $b\mid a$ 的充要条件是存在单位 $\varepsilon\in K$，使

$$b = \varepsilon p_{i_1} p_{i_2} \cdots p_{i_k}$$

其中 $1 \leqslant i_1 < \cdots < i_k \leqslant n$。且若 $k = 0$，则取 $b = \varepsilon$。又 $a \in \langle b \rangle = N \lhd K$ 的充要条件是 $b \mid a$，从而综上可知包含 a 的理想有 2^n 个。

若 a 是 K 的单位，且 $a \in N \lhd K$，显见 $1 = aa^{-1} \in N$，故 $N = K$，即此时只有 K 包含 a。

---

6. 证明：主理想整环 K 中的元素 $a_1, a_2, \cdots, a_n$ 互素的充要条件是，存在 $b_1, b_2, \cdots, b_n \in K$，使

$$\sum_{i=1}^{n} a_i b_i = 1$$

证明 “$\Rightarrow$” 设 $a_i (i = 1, 2, \cdots, n) \in K$ 且 $a_1, a_2, \cdots, a_n$ 互素。由于 K 是主理想整环，故存在 $d \in K$，使

$$\sum_{i=1}^{n} \langle a_i \rangle = \langle d \rangle$$

则 d 是 $a_1, a_2, \cdots, a_n$ 的一个公因子且是单位，从而 $1 \in \langle d \rangle = \sum_{i=1}^{n} \langle a_i \rangle$，故存在$b_i \in K (i = 1, 2, \cdots, n)$，使

$$\sum_{i=1}^{n} a_i b_i = 1$$

“$\Leftarrow$” 设 $d \mid a_i (i = 1, 2, \cdots, n)$，则由 $\sum_{i=1}^{n} a_i b_i = 1$ 知 $d \mid 1$，故 d 为单位，从而 $a_1, a_2, \cdots, a_n$ 互素。

§ 4 欧氏环（P240）

1. 证明：凡域一定是欧氏环。

证明 设 F 是任一域，则 F 是有单位元的整环，定义

$$\varphi: x \longrightarrow 1, x \in F, x \neq 0$$

则 φ 是 F^* 到 N 的一个映射，其中 $F^* = F - \{0\}$，N 是非负整数集，任取 $a \in F^*$，$\forall b \in F$，则

$$b = (ba^{-1})a + 0$$

故 F 是一个欧氏环。

2. 问：有理数域上多项式环 $Q[x]$ 的理想

$$\langle x^2+1, x^5+x^3+1\rangle$$

等于哪个主理想？

解 由于

$$(x^2+1)(-x^3)+(x^5+x^3+1)=1$$

故 $$\langle x^2+1, x^5+x^3+1\rangle=\langle 1\rangle=Q[x]$$

---

3. 证明：Gauss 整环 $Z[\mathrm{i}]$ 关于映射

$$\varphi: a+b\mathrm{i}\longrightarrow a^2+b^2$$

作成一个欧氏环。

证明 不妨设 $\alpha=a+b\mathrm{i}\in Z[\mathrm{i}]^*=Z[\mathrm{i}]-\{0\}$，则 φ 是从 $Z[\mathrm{i}]^*$ 到 N 的一个映射，其中 N 是非负整数集。任 $\alpha\in Z[\mathrm{i}]^*$，$\beta\in Z[\mathrm{i}]$，由于 $\alpha\neq 0$，在数域 $Q[\mathrm{i}]=\{x+y\mathrm{i}\mid x,y\in Q\}$ 中考虑 $\alpha^{-1}\beta=u+v\mathrm{i}$，其中 $u,v\in Q$。在 Z 中取 u' 与 v' 分别为与有理数 u,v 最接近的整数，即

$$|u-u'|\leqslant\frac{1}{2},\ |v-v'|\leqslant\frac{1}{2}$$

令 $k=u-u'$，$h=v-v'$，则 $|k|\leqslant\frac{1}{2}$，$|h|\leqslant\frac{1}{2}$，于是

$$\begin{aligned}\beta&=\alpha(u+v\mathrm{i})=\alpha[(u'+k)+(v'+h)\mathrm{i}]\\&=\alpha(u'+v'\mathrm{i})+\alpha(k+h\mathrm{i})\\&=\alpha q+\gamma\end{aligned}$$

其中 $q=u'+v'\mathrm{i}\in Z[\mathrm{i}]$，$\gamma=\alpha(k+h\mathrm{i})$。因为 $\gamma=\beta-\alpha q$，故 $\gamma\in Z[\mathrm{i}]$。

若 $\gamma\neq 0$，则

$$\begin{aligned}\varphi(\gamma)&=|\gamma|^2=|\alpha|^2\,|k+h\mathrm{i}|^2=|\alpha|^2(k^2+h^2)\\&\leqslant|\alpha|^2\left(\frac{1}{4}+\frac{1}{4}\right)=\frac{1}{2}\varphi(\alpha)\\&<\varphi(\alpha)\end{aligned}$$

综上可知 $Z[\mathrm{i}]$ 是一个欧氏环。

---

4. 设 R 是一个整环。如果有一个 R^* 到非负整数集的映射 φ 满足

(1) 对 R 中任意元素 a 及 $b\neq 0$，有 $q,r\in R$ 使

$$a=bq+r,\ r=0 \text{ 或 } \varphi(r)<\varphi(b)$$

(2) 对 R 中任意非零元素 a,b 都有

$$\varphi(ab) \geqslant \varphi(a)$$

则称 R 是一个 V 欧氏环。证明：V 欧氏环有单位元，从而是欧氏环。

证明　只需证明 R 有单位元。

先证 R 的理想均形如 $\{xb \mid x \in R\}$，其中 $b \in R$。

任 $N \neq \{0\}, N \lhd R$，取 $b \in N$，使 $\varphi(b) = \min\{\varphi(x) \mid 0 \neq x \in N\}$。对任 $a \in N$，令

$$a = bq + r$$

其中 $r = 0$ 或 $\varphi(r) < \varphi(b)$，则 $r = a - bq \in N$。若 $r \neq 0$，则 $\varphi(r) < \varphi(b)$，与 $\varphi(b)$ 的取法矛盾。于是

$$r = 0 \text{ 且 } a = bq \in \{xb \mid x \in R\}$$

从而 R 的理想 N 形如 $\{xb \mid x \in R\}$。

下面证明 R 中存在单位元。

由 $N \lhd R$ 及上述证明可知对任 $a \in R$，有

$$N = \{xa \mid x \in R\}$$

从而由 $a \in R$ 得知存在 $e \in R$ 使 $a = ea$，因此任 $y \in R$，令 $y = xa$，则由 R 为整环因而可换，无零因子可得

$$ye = (xa)e = x(ea) = xa = y$$

于是 e 为 R 的单位元。从而由欧氏环定义可知 R 为欧氏环。

---

5. 证明：对欧氏环 R 可定义一个映射使其成为一个 V 欧氏环。

分析　由 V 欧氏环定义，只需证明本章 §4 第 4 题中映射 φ 的存在。

证明　已知环 R 是欧氏环，故 R 中有单位元且对某映射 φ 作成欧氏环，记 $R^* = R - \{0\}$，则任意 $r \in R^*$，非负整数集 N 的每个子集 $\{\varphi(rd) \mid d \in R^*\}$ 均有最小值。

定义

$$\varphi^* : r \longrightarrow \min\{\varphi(rd) \mid d \in R^*\}$$

则 φ^* 为 R^* 到 N 的一个映射。

任 $a \in R, b \in R^*$，若 $b \mid a$，则存在 $q \in R$，使

$$a = bq + r \quad (r = 0)$$

若 $b \nmid a$，则可令 $\varphi^*(b) = \varphi(bc)(c \in R^*)$。因为 $ac \in R, bc \in R^*$ 及 R 为欧氏环，故存在 $q_1, r_1 \in R$，使

$$ac = bc \cdot q_1 + r_1$$

又因 $b \nmid a$，故 $bc \nmid ac, r_1 \neq 0, \varphi(r_1) < \varphi(bc)$，由上式可知 $c \mid r_1$，故存在 $r_2 \in R^*$，使 $r_1 = r_2 c$，从而由 $c \neq 0$ 及消去律知

$$a = bq_1 + r_2$$

其中 $\varphi(r_2 c) < \varphi(bc)$。于是由 φ^* 定义知

$$\varphi^*(r_2) \leqslant \varphi(r_2 c) < \varphi(bc) = \varphi^*(b)$$

即满足 V 欧氏环定义的条件(1)。

另一方面，由

$$\{\varphi(abd) \mid d \in R^*\} \subset \{\varphi(ad) \mid d \in R^*\}$$

$$\min\{\varphi(abd) \mid d \in R^*\} \in \{\varphi(ad) \mid d \in R^*\}$$

可知

$$\min\{\varphi(abd) \mid d \in R^*\} \geqslant \min\{\varphi(ad) \mid d \in R^*\}$$

即 $\varphi^*(ab) \geqslant \varphi^*(a)$，满足 V 欧氏环定义的条件(2)。

综上可知，存在从 R^* 到 N 的映射 φ^*，满足 V 欧氏环的定义，即 R 对映射 φ^* 来说，作成一个 V 欧氏环。

* §5 惟一分解整环的多项式扩张(P246)

1. 设 K 是惟一分解整环，$0 \neq f(x) \in K[x]$，且

$$f(x) = d_1 f_1(x) = d_2 f_2(x)$$

其中 $d_1, d_2 \in K$，$f_1(x)$ 与 $f_2(x)$ 是本原多项式，证明：d_1 与 d_2 相伴，$f_1(x)$ 与 $f_2(x)$ 也相伴。

证明 不妨设

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

因为 $f(x) = d_1 f_1(x) = d_2 f_2(x)$，且 $f_1(x), f_2(x)$ 是本原多项式，故 d_1 与 d_2 均为 $a_0, a_1, \cdots, a_n$ 的最大公因子，因此存在单位 $\varepsilon \in K$，使

$$d_1 = d_2 \varepsilon$$

即 d_1 与 d_2 相伴。从而有

$$d_1 f_1(x) = d_2 \varepsilon f_1(x) = d_2 f_2(x)$$

由 $f(x) \neq 0$ 可知 $d_2 \neq 0$，由消去律成立即可得

$$f_2(x) = \epsilon f_1(x)$$

于是 $f_1(x)$ 与 $f_2(x)$ 相伴。

2. 设 K 是惟一分解整环，证明：

(1)ϵ 是 K 的单位当且仅当 ϵ 是 $K[x]$ 的单位；

(2) 可约的本原多项式必有次数大于零的多项式为其真因子。

证明 (1)"$\Rightarrow$" 若 ϵ 是 K 的单位，则由 K 与 $K[x]$ 有相同的单位及单位定义即可知 ϵ 也是 $K[x]$ 的单位。

"$\Leftarrow$" 若 ϵ 是 $K[x]$ 的单位，则存在 $f(x) \in K[x]$，使

$$\epsilon f(x) = 1$$

因此 $f(x)$ 为 $K[x]$ 中的零次多项式，即 $f(x) \in K$。记 $f(x) = \epsilon'$，则 $\epsilon' \in K$ 且

$$\epsilon\epsilon' = 1$$

从而 ϵ 也是 K 的单位。

(2) 设 $f(x)$ 为 $K[x]$ 中可约的本原多项式，则存在 $f(x)$ 的非平凡因子 $f_1(x), f_2(x) \in K[x]$ 且

$$f(x) = f_1(x) \cdot f_2(x)$$

其中 $f_1(x)$ 与 $f_2(x)$ 均不是单位。又由 $f(x)$ 是本原多项式可知 $f_1(x)$，$f_2(x)$ 不是零次多项式，综合以上即可得 $f_1(x), f_2(x)$ 必为 $f(x)$ 的次数大于零的真因子。

3. 设 K 是一个惟一分解整环，又 $f(x), g(x) \in K[x]$。证明：若乘积 $f(x)g(x)$ 是本原多项式，则 $f(x)$ 与 $g(x)$ 都是本原多项式。

证明 反证法

不妨设 $\qquad f(x) = af_1(x), \quad g(x) = bg_1(x)$

其中 $a, b \in K$，$f_1(x), g_1(x)$ 为 $K[x]$ 上的本原多项式，由高斯引理可知 $f_1(x)g_1(x)$ 为本原多项式。而

$$f(x)g(x) = abf_1(x)g_1(x)$$

故若 $f(x)$ 与 $g(x)$ 中存在一个不是本原多项式，于是有 ab 不是单位，进而 $f(x)g(x)$ 不是本原多项式，与题设矛盾。所以 $f(x)$ 与 $g(x)$ 均为本原多项式。

4. 设 F 是惟一分解整环 K 的分式域。如果在 $F[x]$ 中有

$$f(x)=g(x)h(x)$$

但其中 $f(x),g(x)\in K[x]$，而且 $g(x)$ 是本原的。证明：

$$h(x)\in K[x]$$

证明 依题意可设

$$h(x)=\frac{b}{a}h_1(x)$$

其中 a 与 b 为 K 中互素元素，$h_1(x)$ 为 $K[x]$ 中的本原多项式，因此

$$f(x)=g(x)h(x)=\frac{b}{a}g(x)h_1(x)$$

又 $g(x)$ 为本原多项式，由高斯引理知 $g(x)h_1(x)$ 为本原多项式，不妨设

$$g(x)h_1(x)=b_0+b_1x+\cdots+b_nx^n\quad(b_i\in K,i=1,2,\cdots,n)$$

但由于题设中 $f(x)\in K[x]$，若令

$$f(x)=c_0+c_1+\cdots+c_nx^n\quad(c_i\in K,i=1,2,\cdots,n)$$

则有$\frac{b}{a}b_i=c_i$ 即 $a\mid bb_i$，又 a 与 b 互素，从而 $a\mid b_i$，这可说明 a 是单位，从而

$$h(x)=\frac{b}{a}h_1(x)\in K[x]$$

---

5. 设 K 是惟一分解整环，又 $u,v\in K,u\neq 0$ 且

$$(u,v)=1,f(x)\in K[x]$$

证明：在 K 的商域 F 中，若$\frac{v}{u}$ 是 $f(x)$ 的根，则

$$(u-v)\mid f(1),(u+v)\mid f(-1)$$

证明 因为 K 是惟一分解整环，所以 $F[x]$ 及 $K[x]$ 都是惟一分解整环。又在 F 中$\frac{v}{u}$ 是 $f(x)$ 的根，故在 $F[x]$ 中$(ux-v)\mid f(x)$，不妨设

$$f(x)=(ux-v)h(x)$$

则由 $f(x)\in K[x]$，$ux-v$ 为 $K[x]$ 中的本原多项式，从本章 §5 第 4 题结论知 $h(x)\in K[x]$，从而将 $x=1$ 及 $x=-1$ 分别代入上式可得

$$f(1)=(u-v)h(1), f(-1)=-(u+v)h(-1)$$

即在 K 中有 $(u-v)\mid f(1),(u+v)\mid f(-1)$。

---

6. 设 α 是 Gauss 整环 $Z[\mathrm{i}]$ 的一个元素，证明：若 $|\alpha|^2=\alpha\bar{\alpha}=p$ 是素数，则 α 是 $Z[\mathrm{i}]$ 的不可约元。又问：反之如何？

证明　不妨设

$$\alpha=(a+b\mathrm{i})(c+d\mathrm{i})$$

其中 $a,b,c,d\in Z$，则

$$\begin{aligned}|\alpha|^2=\alpha\bar{\alpha}&=(a+b\mathrm{i})(a-b\mathrm{i})(c+d\mathrm{i})(c-d\mathrm{i})\\&=(a^2+b^2)(c^2+d^2)\\&=p\end{aligned}$$

由于 p 为素数，故 $a^2+b^2=1$ 或 $c^2+d^2=1$。而 $a,b,c,d\in Z$，因此 $a+b\mathrm{i}=\pm1$ 或 $\pm\mathrm{i}$，或 $c+d\mathrm{i}=\pm1$ 或 $\pm\mathrm{i}$，即 $a+b\mathrm{i}$ 或 $c+d\mathrm{i}$ 中有一个是单位，从而 α 是 $Z[\mathrm{i}]$ 的不可约元。

反之则未必成立。如 $\alpha=5\mathrm{i}$ 为 $Z[\mathrm{i}]$ 的素元，但 $|\alpha|^2=25$ 不是素数。

---

7. 证明：x^2+1 是多项式环 $Z[x]$ 中的不可约元，但商环 $Z[x]/\langle x^2+1\rangle$ 不是域。

证明　若 x^2+1 在 $Z[x]$ 中可约，则必存在一次多项式

$$f(x)=ax+b\in Z[x], g(x)=cx+d\in Z[x]$$

使 $x^2+1=f(x)g(x)$，即

$$x^2+1=acx^2+(ad+bc)x+bd$$

从而

$$ac=1, ad+bc=0, bd=1$$

由 $ac=1$ 以及 $a,c\in Z$ 知 $a=c=\pm1$，同理 $b=d=\pm1$，故 $ad+bc=\pm2$，与 $ad+bc=0$ 矛盾，所以一次多项式 $f(x)$ 与 $g(x)$ 不存在，即 x^2+1 在 $Z[x]$ 中不可约。

又 $\langle x^2+1\rangle\subset\langle x\rangle\subset Z[x]$，故 $\langle x^2+1\rangle$ 不是 $Z[x]$ 的极大理想，而 $Z[x]$ 为一个有单位元的交换环，因此 $Z[x]/\langle x^2+1\rangle$ 不是域。

---

8. 设 M 是主理想整环 K 的一个非零理想。证明：

$$M \text{ 是 } K \text{ 的极大理想} \Leftrightarrow M \text{ 是 } K \text{ 的素理想}$$

证明 "$\Rightarrow$" 因为有单位元的交换环中的极大理想为素理想，而主理想整环 K 是有单位元的交换环，M 是 K 的极大理想，所以 M 是 K 的素理想。

"$\Leftarrow$" 设 M 是 K 的素理想，$M=\langle a\rangle$，若存在 $N\trianglelefteq K$，使 $M=\langle a\rangle\subset N$，则由于 K 是主理想整环，设 $N=\langle b\rangle$，则 $a\in\langle a\rangle\subset\langle b\rangle$，从而存在 c，使 $a=bc\in\langle a\rangle$，而 $\langle a\rangle$ 为素理想，所以 $b\in\langle a\rangle$ 或 $c\in\langle a\rangle$。

但 $\langle a\rangle\subset\langle b\rangle$，故有 $c\in\langle a\rangle$。因此存在 d，使 $c=ad$，于是

$$a\cdot 1=a=bc=bad=abd$$

在主理想整环 K 中，消去律成立，则由 $a\cdot 1=abd$ 可得 $1=bd\in\langle b\rangle$，故

$$N=\langle b\rangle=K$$

从而 $M=\langle a\rangle$ 是 K 的极大理想。

---

9. 设 K 是一个阶大于 1 且有单位元的整环。证明：K 中元素 $a\neq 0$ 是不可约元的充要条件是，$\langle a\rangle$ 在 K 的全体真主理想中是极大的。

证明 "$\Rightarrow$" 由 $a\neq 0$ 为 K 的不可约元知 a 不是单位，故 $\langle a\rangle$ 是 K 的真主理想。不妨设 $\langle a\rangle\subseteq\langle b\rangle$，则存在 $c\in K$ 使 $a=bc$。于是由 a 是不可约元知 b 或者 c 为单位。若 b 是单位，则 $\langle b\rangle=K$；若 c 是单位，则 $\langle b\rangle=\langle a\rangle$，从而 $\langle a\rangle$ 在 K 的全体真主理想中是极大的。

"$\Leftarrow$" 若 $\langle a\rangle$ 在 K 的全体真主理想中是极大的，则 $a\neq 0$ 且 a 不是单位。

现设 $a=bc$，则 $\langle a\rangle\subseteq\langle b\rangle$，而 $\langle a\rangle$ 在 K 的全体真主理想中极大，故 $\langle a\rangle=\langle b\rangle$，因此 a 与 b 相伴，即存在单位 ε，使 $b=\varepsilon a$，故

$$a=bc=\varepsilon ac=a\varepsilon c$$

又 $a\neq 0$，K 中无零因子，由消去律得 $1=\varepsilon c$，即 c 为 K 的单位，a 也就是 K 的不可约元。

---

10. 设 K 是一个阶大于 1 且有单位元的整环。证明：

$$K\text{ 是域}\Leftrightarrow K[x]\text{ 是主理想整环}$$

证明 必要性显然，下面证明充分性。

设 $K[x]$ 是主理想整环，任 $a\in K$ 且 $a\neq 0$，则存在 $f(x)\in K[x]$，使 $\langle f(x)\rangle=\langle a,x\rangle$，故 $f(x)\mid a$ 且 $f(x)\mid x$。

由 $f(x)\mid a$ 知 $f(x)=b\in K$ 且 $b\neq 0$。由 $f(x)\mid x$ 知 $b\mid x$，b 为可逆

元。从而

$$\langle a,x\rangle=\langle f(x)\rangle=\langle b\rangle=\langle 1\rangle$$

故存在 $s(x),t(x)\in K[x]$，使

$$s(x)a+t(x)x=1$$

令 $x=0$ 得 $s(0)a=1$，即 a 为 K 的可逆元。故 K 是域。

---

11. 证明：实数域 R 上的二元多项式环 $R[x,y]$ 不是主理想整环。

证明 $R[x,y]$ 是一个具有单位元，无零因子的交换环，要证 $R[x,y]$ 不是主理想整环，只需证存在 $R[x,y]$ 的理想不是主理想。

设 A 是常数项为 0 的所有二元多项式作成的集合，则 A 是 $R[x,y]$ 的理想。

如果 A 是 $R[x,y]$ 的主理想，不妨设存在 $f(x,y)\in R[x,y]$，使

$$A=\langle f(x,y)\rangle$$

显见 $x\in A$，则存在 $g(x,y)\in R[x,y]$，使

$$x=f(x,y)g(x,y)$$

从而

$$\begin{cases}\deg_y f(x,y)=\deg_y g(x,y)=0\\ \deg_x f(x,y)=1\\ \deg_x g(x,y)=0\end{cases}$$

或

$$\begin{cases}\deg_y f(x,y)=\deg_y g(x,y)=0\\ \deg_x f(x,y)=0\\ \deg_x g(x,y)=1\end{cases}$$

其中 $\deg_x f(x,y)$ 表示 $f(x,y)$ 中 x 的最高次数，其余同。

又由 $f(x,y)\in A$ 可知 $f(x,y)$ 中的常数项为 0，故若 $\deg_x f(x,y)=0$，则必 $f(x,y)=0$，于是 $A=\{0\}$，显见不可能。因此 $\deg_x f(x,y)=1$，此时 $\deg_x g(x,y)=\deg_y g(x,y)=\deg_y f(x,y)=0$，故设

$$f(x,y)=a_1x+a_0,g(x,y)=g_0$$

其中 $a_1\neq 0,a_0,g_0\in R$。从而由 $x=f(x,y)g(x,y)$ 得

$$x=a_1g_0x+a_0g_0(\in A)$$

比较系数可得 $g_0 \neq 0, a_0 = 0$，于是有

$$f(x,y) = a_1 x$$

其中 $a_1 \neq 0$。

同理由 $y \in A = \langle f(x,y) \rangle$ 可得

$$f(x,y) = b_1 y$$

其中 $b_1 \neq 0$。显然 $a_1 x = b_1 y$ 是不可能的。

综上可知 A 不是主理想，从而 $R[x,y]$ 也不是主理想整环。

---

12. 设 $Z[\mathrm{i}]$ 是 Gauss 整环。证明：

(1) 当 $mn \neq 0$ 时，$m+n\mathrm{i}$ 是 $Z[\mathrm{i}]$ 的素元 $\Leftrightarrow m^2+n^2$ 是素数；

(2) 当 $mn = 0$ 时，$m+n\mathrm{i}$ 是 $Z[\mathrm{i}]$ 的素元 $\Leftrightarrow |m+n\mathrm{i}|$ 是素数且

$$4 \mid |m+n\mathrm{i}| - 3$$

证明 (1) 记 $\alpha = m+n\mathrm{i}$，若 $m^2+n^2 = |\alpha|^2$ 为素数。由本章 §5 第 6 题知 α 是 $Z[\mathrm{i}]$ 的不可约元，从而是其素元。下面证明必要性成立。

设 $(m,n) = d$。若 $d \neq 1$，则

$$\alpha = d(m_1 + n_1 \mathrm{i})$$

其中 $m = dm_1, n = dn_1$，故此时 α 不是 $Z[\mathrm{i}]$ 的素元，从而 $d = 1$，即

$$(m,n) = 1$$

又可证 $Z[\mathrm{i}]/\langle m+n\mathrm{i} \rangle$ 中共有 m^2+n^2 个元素，且每一元素可惟一表示为

$$\overline{a+b\mathrm{i}}, 0 \leqslant a < m^2+n^2, 0 \leqslant b < 1$$

亦可惟一表示为

$$\bar{a}, 0 \leqslant a < m^2+n^2$$

定义

$$\varphi: \bar{a} \longrightarrow [a]$$

则 φ 是 $Z[\mathrm{i}]/\langle m+n\mathrm{i} \rangle$ 到模 m^2+n^2 剩余类环 $Z_{m^2+n^2}$ 的一个同构映射，故

$$Z[\mathrm{i}]/\langle m+n\mathrm{i} \rangle \cong Z_{m^2+n^2}$$

由 $m+n\mathrm{i}$ 为素元知 $m+n\mathrm{i}$ 生成的理想为素理想，又主理想整环 $Z[\mathrm{i}]$ 中的素理想与极大理想一致，故 $\langle m+n\mathrm{i} \rangle$ 为 $Z[\mathrm{i}]$ 的极大理想，于是环 $Z[\mathrm{i}]/\langle m+n\mathrm{i} \rangle$ 为域，从而环 $Z_{m^2+n^2}$ 也是域，因此 m^2+n^2 必为素数。

(2)“⇒” 若 $m+ni$ 为 $Z[i]$ 的素元，则 $|m+ni|=p$ 为素数。下证 $4\mid(p-3)$。对素数 p 有

$$p\equiv 1(\mathrm{mod}4)\Leftrightarrow p \text{ 可表示为正整数的平方和}$$

若 $4\nmid(p-3)$，即 $p\not\equiv 3(\mathrm{mod}4)$，则 $4\mid(p-2)(p=2)$ 或 $4\mid(p-1)$，从而总有

$$p=a^2+b^2=(a+bi)(a-bi)$$

即可知 $m+ni$ 不是 $Z[i]$ 的素元，与题设矛盾，故 $4\mid(p-3)$。

“⇐” 若 $m+ni$ 不是 $Z[i]$ 的素元，则由 $|m+ni|=p$ 是素数，p 为 Z 的素元知 $|m+ni|$ 与 $m+ni$ 至多相差一个单位。故 $|m+ni|$ 也不是 $Z[i]$ 的素元，则其在 $Z[i]$ 中有真因子分解：

$$p=|m+ni|=(a+bi)(a_1+b_1i)$$

从而

$$p^2=(a^2+b^2)(a_1{}^2+b_1{}^2)$$

又 p 为素数，故 $p=a^2+b^2=a_1^2+b_1^2$，由必要性中素数 p 满足 $p\equiv 1(\mathrm{mod}4)$ 的充要条件得 $4\mid(p-1)$ 或 $p=2$，即 $p\nmid 4,4\nmid(p-3)$。与题设中 $4\mid(p-3)$ 矛盾。故 $m+ni$ 为 $Z[i]$ 的素元。

---

13. 证明：当 $m=-2,-1,2,3$ 时，整环

$$D=\{a+b\sqrt{m}\mid a,b\in Z\}$$

对于 $\varphi(\alpha)=|N(\alpha)|=|a^2-b^2m|$ 作成欧氏环。其中 $\alpha=a+b\sqrt{m}$。

证明 显见 D 有单位元。不妨设 $\alpha\in D,\beta(\neq 0)\in D$，记

$$\frac{\alpha}{\beta}=x+y\sqrt{m}$$

其中 $x,y\in Q$。选择整数 r,s，使得

$$|x-r|\leqslant\frac{1}{2},\ |y-s|\leqslant\frac{1}{2}$$

并记

$$\gamma=r+s\sqrt{m}(\in D),\rho=\beta((x-r)+(y-s)\sqrt{m})$$

从而

$$\alpha=\beta(x+y\sqrt{m})=\rho+\beta(r+s\sqrt{m})=\rho+\beta\gamma$$

于是由 $\alpha,\beta,\gamma\in D$ 可知 $\rho=\alpha-\beta\gamma\in D$。

若 $\rho\neq 0$，则可知

$$\begin{aligned}\varphi(\rho)&=|N(\rho)|=|N(\beta((x-r)+(y-s)\sqrt{m}))|\\&=|N(\beta)||(x-r)^2-(y-s)^2m|\\&\leqslant\varphi(\beta)[(x-r)^2+(y-s)^2|m|]\\&\leqslant\frac{1}{4}\varphi(\beta)(1+|m|)\end{aligned}$$

显见，$m=-2,-1,2$ 时，$1+|m|\leqslant 3$，故 $\varphi(\rho)\leqslant\frac{3}{4}\varphi(\beta)<\varphi(\beta)$，因此此时 D 对 φ 作成欧氏环。

$m=3$ 时，若 $|x-r|=|y-s|=\frac{1}{2}$，则

$$\varphi(\rho)=\varphi(\beta)\left|\frac{1}{4}-\frac{3}{4}\right|=\frac{1}{2}\varphi(\beta)<\varphi(\beta)$$

若 $|x-r|<\frac{1}{2}$ 或 $|y-s|<\frac{1}{2}$ 至少一个成立，则

$$\varphi(\rho)<\frac{1}{4}\varphi(\beta)(1+3)=\varphi(\beta)$$

所以 $m=3$ 时，D 对 φ 也作成欧氏环。

第六章 域的扩张

导读

一、基本要求

1. 了解扩域的定义，理解单扩域与素域的定义，掌握扩域的有关定理；
2. 了解超越元、单超越扩域、代数元、单代数扩域的定义；
3. 理解多项式分裂域的概念与性质；
4. 理解有限域的构造及基本事实；
5. 了解可离元、可离扩域、完备域的定义及相关结论。

二、重点与难点

1. 扩域与素域的相关结论；
2. 单扩域的构造；
3. 多项式的分裂域及有限域的构造。

知识点考点精要

一、扩域和素域

1. 定义

(1) 扩域

若域 F 是域 E 的一个子域，则称 E 为子域 F 的一个扩域。

(2) 素域

若域 Δ 不含真子域，则称 Δ 是一个素域。

2. 一个扩域的构造

设域 E 是域 F 的一个扩域，$S \subseteq E$，$F(S)$ 表示 E 中含 $F \cup S$ 的所有子域的交，则 $F(S)$ 是 E 中包含 F 及 S 的最小子域，并称其为添加子集 S 于 F 所得到的域。

3. 素域的性质

(1) 设 Δ 是一个素域，则

① 当 $\mathrm{char}\Delta = \infty$ 时，$\Delta \cong Q$；

② 当 $\mathrm{char}\Delta = p$ 时，$\Delta \cong Z_p$，其中 p 为素数。

(2) 每个域包含且只包含一个素域。

(3) 设 E 是一个域，则

① 当 $\mathrm{char}E = \infty$ 时，E 包含一个与 Q 同构的素域；

② 当 $\mathrm{char}E = p$ 时，E 包含一个与 Z_p 同构的素域，其中 p 为素数。

4. 扩域的性质

域 E 是域 F 的一个扩域，$S_1, S_2 \subseteq E$，则

$$F(S_1)(S_2) = F(S_2)(S_1) = F(S_1 \cup F_2)$$

二、单扩域

1. 定义

(1) 代数元与超越元

设 E 是域 F 的一个扩域，$\alpha \in E$。若存在 F 上非零多项式 $f(x)$ 使

$$f(\alpha) = 0$$

则称 α 为 F 上的一个代数元。否则，称 α 为 F 上的一个超越元。

(2) 单扩域

扩域 $F(\alpha)$ 称为域 F 的单扩域(单扩张)。

① 单代数扩域

若 α 为 F 上的代数元，则扩域 $F(\alpha)$ 称为域 F 的单代数扩域(张)。

② 单超越扩域

若 α 为 F 上的超越元，则扩域 $F(\alpha)$ 称为域 F 的单超越扩域(张)。

(3) 最小多项式

若 α 为域 F 的一个代数元，则 F 上首系数为 1 且有根 α，次数最低的多项式是存在的，称为 α 在 F 上的最小多项式。

(4)n 次代数元

若 α 的最小多项式的次数是 n，则称 α 是 F 上的一个 n 次代数元。

2. 最小多项式的性质

域 F 上的代数元 α 在 F 上的最小多项式 $p(x)$ 是惟一的，且

①$p(x)$ 在 F 上不可约；

② 若 $f(x)$ 为 F 上一个多项式且 $f(\alpha)=0$，则 $p(x)\mid f(x)$。

3. 单扩域的结构

设 $F[x]$ 为域 F 上未定元 x 的多项式环，$F(x)$ 为其分式域，则

① 当 α 为 F 上的超越元时，$F(\alpha)=F[\alpha]\cong F(x)$；

② 当 α 为 F 上的代数元时，$F(\alpha)=F[\alpha]\cong F[x]/\langle p(x)\rangle$，其中 $p(x)$ 为 α 在 F 上的最小多项式。

③ 当 α 为 F 上的 n 次代数元，$p(x)$ 为 α 在 F 上的最小多项式时

$$F(\alpha)=F[\alpha]\cong F[x]/\langle p(x)\rangle$$

且 F 的单代数扩域 $F(\alpha)=F[\alpha]$ 是 F 上的一个 n 维空间

$$F(\alpha)=F[\alpha]=\{a_0+a_1\alpha+\cdots+\alpha_{n-1}\alpha^{n-1}\mid a_i\in F, i=0,1,\cdots,n-1\}$$

其中 $1,\alpha,\cdots,\alpha^{n-1}$ 为 $F(\alpha)$ 的一个基。

4. 单代数扩域的存在性

设 F 是一个域，$p(x)$ 是 F 上任意一个给定的首系数为 1 的不可约多项式，则存在 F 上单代数扩域 $F(\alpha)$，其中 α 在 F 上的最小多项式是 $p(x)$。

三、代数扩域

1. 定义

(1) 代数扩域、超越扩域与纯超越扩域

设 E 是 F 的一个扩域，如果 E 中每个元素都是 F 上的代数元，则称 E 是 F 的一个代数扩域(张)。否则，称 E 是 F 的一个超越扩域(张)。

若 E 是 F 的超越扩域，又 E 中除 F 的元素外，都是 F 的超越元，则称 E 是 F 的纯超越扩域(张)。

(2) 扩域次数与有(无)限次扩域

设 E 是域 F 的一个扩域，则 E 作为 F 上向量空间的维数，叫做 E 在 F 上的次数，记为 $(E:F)$。

若 $(E:F)$ 有限，则称 E 为 F 的有限次扩域；

若$(E:F)$无限，则称E为F的无限次扩域。

2. 扩域的次数定理

(1) 若E是K的扩域，K是F的扩域，则

$$(E:F)=(E:K)(K:F)$$

(2) 设$F_i(i=1,2,\cdots,m)$均为域，且$F_1\leqslant F_2\leqslant\cdots\leqslant F_m$，则

$$(F_m:F_1)=(F_m:F_{m-1})(F_{m-1}:F_{m-2})\cdots(F_2:F_1)$$

3. 有限次扩域的性质

(1) 有限次扩域必为代数扩域；

(2)E是域F的有限次扩域$\Leftrightarrow$存在F上的代数元$\alpha_i(i=1,2,\cdots,n)$，使

$$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$$

(3) 域F上代数元的积、差、和、商仍是F上的代数元。

4. 代数扩域的性质

(1) 设E是域F的一个扩域，$S\subseteq E,S\neq\varnothing$，且$S$是$F$上代数元的集合。则$F(S)$是域$F$的代数扩域。

(2) 设$F\leqslant E,K\leqslant E,F\subseteq K$，其中$E$为域，若$E$是$K$的代数扩域，$K$是$F$的代数扩域，则$E$是$F$的代数扩域。

(3) 设E是域F的超越扩域，则在E中存在子域K，满足

$$F\subseteq K\subset E$$

其中K是F的代数扩域，E是K的纯超越扩域。

四、多项式的分裂域

1. 定义

(1) 代数闭域

若域E上每个多项式都能分解成E上一次多项式的乘积，则称这样的E为代数闭域。

(2) 分裂域

设E是域F的一个扩域，$f(x)$是F上一个次数大于零的多项式。如果$f(x)$在E中可完全分解，在其他任何包含F但比E小的子域上不能完全分解，则称E是$f(x)$在F上的一个分裂域。

(3) 分裂域的等价定义

设 E 是域 F 上多项式 $f(x)$ 的一个分裂域，且

$$f(x) = a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

其中 $a_0 \in F, \alpha_i \in E$，则 $E = F(\alpha_1, \alpha_2, \cdots \alpha_n)$，即 $f(x)$ 在 F 上的分裂域就是把 $f(x)$ 的全部根添加于 F 所得的扩域。

(4) 映射的扩张，设域 $F \leqslant E, \overline{F} \leqslant \overline{E}$，$\sigma$ 是 F 与 $\overline{F}$ 的同构映射，若存在 E 与 $\overline{E}$ 的同构映射 φ 使 $\varphi(a) = \sigma(a)(\forall a \in F)$，则称 φ 是 σ 的一个扩张。

2. 分裂域的存在性

设 $f(x)$ 是域 F 上一个 $n(n>0)$ 次多项式，则 $f(x)$ 在 F 上的分裂域存在，且在同构意义下惟一。

3. 域间的同构映射及扩张的性质

(1) 设 σ 是域 F 与 $\overline{F}$ 的一个同构映射，则

①$g(x) \mid f(x) \Leftrightarrow \overline{g}(x) \mid \overline{f}(x)$；

②$p(x)$ 在 F 上不可约 $\Leftrightarrow \overline{p}(x)$ 在 $\overline{F}$ 上不可约

其中

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$$
$$\overline{f}(x) = \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_nx^n \in \overline{F}[x]$$
$$\overline{a}_i = \sigma(a_i) \quad (i = 0, 1, \cdots, n)$$

(2) 设 σ 是域 F 与域 $\overline{F}$ 的同构映射，$F(\alpha)$ 是 F 的单代数扩域，$p(x)$ 是 α 在 F 上的最小多项式，$\overline{F}(\overline{\alpha})$ 是 $\overline{F}$ 的单代数扩域，$\overline{p}(x)$ 是 $\overline{\alpha}$ 在 $\overline{F}$ 上的最小多项式，则

$$F(\alpha) \cong \overline{F}(\overline{\alpha})$$

且此同构为 σ 的扩张，把 α 变为 $\overline{\alpha}$。

(3) 设 σ 是域 F 与域 $\overline{F}$ 的同构映射，$f(x)$ 与 $\overline{f}(x)$ 分别为 F 与 $\overline{F}$ 上的 $n>0$ 次多项式，则 $f(x)$ 在 F 上的分裂域 $E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 与 $\overline{f}(x)$ 在 $\overline{F}$ 上的分裂域 $\overline{E} = \overline{F}(\overline{\alpha}_1, \overline{\alpha}_2, \cdots, \overline{\alpha}_n)$ 同构，且为 σ 的扩张。

(4) 域 F 上多项式 $f(x)$ 的分裂域彼此同构。

五、有限域

1. 有限域的定义

只含有限个元素的域称为有限域，也称为伽罗瓦域，记为 $GF(p^n)$，其

中素数 p 为其特征，n 是它在素域上的次数。

2. 有限域的阶

有限域 E 的元素个数是一个素数 p 的方幂 p^n，其中 $p = \mathrm{char}E$，n 是 E 在它所含素域上的次数。

3. 有限域的存在性

设 Δ 是特征为素数 p 的素域，$q = p^n$，n 为正整数，则 $x^q - x$ 在 Δ 上的分裂域 E 是一个有 q 个元素的有限域。

即对任给素数 p，正整数 n，p^n 阶有限群存在。

4. 有限域的性质

(1) 有限域 $E = GF(p^n)$ 是多项式

$$x^q - x \quad (q = p^n)$$

在其所含素域 Δ 上的分裂域。

(2) 有限域的乘群

有限域 F 的非零元素作成的乘群是一个循环群。

注 任何有限域 F 均可表为

$$F = \{0, 1, \alpha, \cdots, \alpha^{q-2}\} = \Delta(\alpha)$$

即 F 是其素域 Δ 的一个单扩域，其中 α 称为 $q = p^n$ 阶有限域 F 的一个原根，它是 Δ 上的 n 次代数元。

(3) 有限域的子域

设 E 为 p^n 阶有限域，则对 n 的每个正因子 m，存在且只存在一个 p^m 阶子域。

5. 有限域的构造方法

任给一个素数 p 和一个正整数 n，在域 Z_p 上任取一个 n 次不可约多项式 $p(x)$，则域 Z_p 上多项式环 $Z_p[x]$ 的商环 $Z_p[x]/\langle p(x)\rangle$ 即为一个 p^n 阶的有限域。

六、可离扩域

1. 定义

(1) 可离元与不可离元

设 F 是一个域，E 是 F 的一个代数扩域。若 E 的元素 α 在 F 上的最小多项式(在其分裂域中)无重根，则称 α 为域 F 上的可离元；否则称为不可

离元。

(2) 可离扩域与不可离扩域

设域 E 是域 F 的一个代数扩域，若 E 中每个元素都是 F 上的可离元，则称 E 是 F 的可离扩域；否则称 E 是 F 的不可离扩域。

(3) 完全域

若域 F 的任何代数扩域都是可离扩域，则称 F 为完全域或完备域。

2. 可离元与不可离元的特征

(1) 设 $p(x)$ 是域 F 上的一个不可约多项式，则

①$\mathrm{char}F=\infty$ 时，$p(x)$（在其分裂域中）无重根，即域 F 上任何代数元都是可离元。

②$\mathrm{char}F=$ 素数 p 时，$p(x)$ 有重根 $\Leftrightarrow p(x)=g(x^p)$，$g(x)\in F[x]$，即 F 上代数元 α 是不可离元 $\Leftrightarrow \alpha$ 在 F 上的最小多项式可表为 F 上关于 x^p 的多项式。

(2) 特征为 ∞ 的域的任何代数扩域都是可离扩域。

3. 可离元的条件

设 $\mathrm{char}F=p$，α 是域 F 的某一扩域的元素，则

$$\alpha \text{ 是 } F \text{ 上可离元} \Leftrightarrow F(\alpha)=F(\alpha^p)$$

4. 可离元的性质

(1) 设 $E=F(\beta)$ 是域 F 的单扩域，且 β 是 F 上的可离元，则 E 上的可离元也是 F 上的可离元。

(2) 若 α 与 β 是域 F 上的可离元，则 $F(\alpha,\beta)$ 是 F 的一个可离扩域。

(3) 可离元的和、差、积、商（分母不为零）仍为可离元。

5. 可离扩域的主要结论

域 F 的有限次可离扩域必是 F 的单扩域。

6. 完全域判定

(1) 特征为 ∞ 的任何域，特别是数域都是完全域。

(2) 有限域都是完全域。

(3) 设 $\mathrm{char}F=p$，则域 F 是完全域的充要条件是 F 中每个元素都是 F 中某个元素的 p 次幂。

释疑解惑

一、关于代数元和超越元的判定

1. 要判定元素 α 是域 F 上的代数元，一般方法是找出 F 上以 α 为根的非零多项式(在特殊情况下，可采用其他判别法)。

2. 要判定元素 α 是域 F 上的超越元，一般是用反证法，即假设存在 F 上的非零多项式以 α 为根，由此推出矛盾。

二、关于域 F 上代数元 α 的最小多项式的存在性及最小多项式的判定

1. 存在性是显然的，只需对 F 上所有以 α 为根的非零多项式的次数应用自然数最小数原理，即可得出 α 的最小多项式的存在性。

2. 判定

设 α 是域 F 的扩域中的元素，$\varphi(x)$ 是 F 上的首系数是 1 的多项式。若能证明 α 是 $\varphi(x)$ 的根，再证明 $\varphi(x)$ 在 F 上是不可约多项式，则可断定 $\varphi(x)$ 是 α 在 F 上的最小多项式。

三、几种扩域间的关系

$$
\text{扩域}\begin{cases}
\text{超越扩域}\begin{cases}\text{纯超越扩域} \rightarrow \text{单超越扩域}\\ \text{非纯超越扩域}\end{cases}\\[2ex]
\text{代数扩域}\begin{cases}\text{有限次扩域}\\ \text{无限次扩域}\\ \text{单代数扩域}\\ \text{可离扩域}\\ \text{不可离扩域}\end{cases}
\end{cases}
$$

注　① 确定两种扩域(扩张)间的关系，应从定义的严格论证出发。

② 设 E 是 F 的扩域，E 是不是 F 的有限次扩域，是由 E 作为 F 上的向量空间时 E 的维数来决定的。当 E 是 F 的有限次扩域时，确定扩域次数的一个方法就是寻找 E 在 F 上的一组基底，判断基底元素的个数。但是应当

注意域 F 的扩张次数与在 F 中添加元素的个数是两个截然不同的概念。

四、关于分裂域

(1) 域 F 上多项式 $f(x)$ 的分裂域，不仅要求 $f(x)$ 可在其中完全分解，还要求它是包含 F 及 $f(x)$ 全部根的最小域。即，若一个域包含了 F 及 $f(x)$ 的所有根，则其必包含 $f(x)$ 在 F 上的分裂域。

(2) 同一多项式在不同域上的分裂域可能不同，也可能相同。如 $f(x)=x^2-3$ 在 Q 上的分裂域与在 $Q(\sqrt{3})$ 上的分裂域均为 $Q(\sqrt{3})$，相同。而 $f(x)=x^3-1$ 在 Q 上的分裂域与在实数域上的分裂域分别为 $Q(\sqrt{3}\mathrm{i})$ 与复数域，二者不同。

典型题精讲

1. 设 E 是域 F 的代数扩域。证明：若 α 是 E 上的一个代数元，则 α 也是 F 上的一个代数元。

证明　已知 α 是域 E 上的一个代数元，故存在 E 上的多项式 $f(x)\neq 0$，使

$$f(\alpha)=a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_0=0$$

其中 $a_i\in E(i=0,1,\cdots,n)$。又 E 为 F 的一个代数扩域，故 $a_i(i=0,1,\cdots,n)$ 为 F 上的代数元，而 E 的子域

$$E'=F(a_0,a_1,\cdots,a_n)$$

是 F 上一个有限扩域，但由 $f(\alpha)=0$ 知 α 也是 E' 上的一个代数元，故 $E'(\alpha)$ 是 E' 上一个有限扩域，从而是 F 上的一个有限扩域，因此

$$E'(\alpha)=F(a_0,a_1,\cdots a_{n-1},\alpha)$$

是 F 上一个代数扩域，α 是 F 上的一个代数元。

---

2. 设 E 是域 F 的有限扩域。证明：存在 E 的有限个元 $\alpha_1,\alpha_2,\cdots,\alpha_m$，使

$$E=F(\alpha_1,\alpha_2,\cdots,\alpha_m)$$

证明　依题意，不妨设 $(E:F)=m$，则存在 E 在 F 上的一组基：$\alpha_1,\alpha_2,\cdots,\alpha_m$，显见有

$$E = F(\alpha_1, \alpha_2, \cdots, \alpha_m)$$

---

3. 设 P 是一个特征为素数 p 的域，$F = P(\alpha)$ 是 P 的一个单扩域，其中 α 是 $P[x]$ 的多项式 $x^p - a$ 的一个根。证明：$P(\alpha)$ 是 $x^p - a$ 在 P 上的分裂域。

证明 因 α 是 $x^p - a$ 的一个根，故

$$\alpha^p = a$$

又域 P 的特征为 p，故域 F 的特征也为 p，因此在 $F[x]$ 中

$$x^p - a = x^p - \alpha^p = (x - \alpha)^p$$

即 $P(\alpha)$ 是添加 $x^p - a$ 的 p 个相同的根于 P 得到的，从而 $P(\alpha)$ 是 $x^p - a$ 在 P 上的分裂域。

---

4. 设 $p_i(x)(i = 1,2,\cdots,m)$ 是域 F 上的 m 个最高系数为 1 的不可约多项式。证明：存在 F 的一个有限扩域

$$F = F(\alpha_1, \alpha_2, \cdots, \alpha_m)$$

其中 $\alpha_i(i = 1,2,\cdots,m)$ 在 F 上的极小多项式为 $p_i(x)$。

证明 设 $f(x) = p_1(x)p_2(x)\cdots p_m(x)$，$E$ 为 $f(x)$ 在域 F 上的分裂域，E 含有 $f(x)$ 的所有根，故含有 $\alpha_1, \alpha_2, \cdots, \alpha_m$，其中 α_i 是 $p_i(x)$ 的一个根($i = 1,2,\cdots,m$)。故

$$F(\alpha_1, \alpha_2, \cdots, \alpha_m) \subset E$$

又 $p_i(x)(i = 1,2,\cdots,m)$ 是 F 上最高系数为 1 的不可约多项式，故它们分别是 $\alpha_i(i = 1,2,\cdots,m)$ 在 F 上的极小多项式。而 $\alpha_i(i = 1,2,\cdots,m)$ 都是 F 上的代数元，因此

$$F = F(\alpha_1, \alpha_2, \cdots, \alpha_m)$$

是 F 上的一个有限扩域。

---

5. 证明：一个有限域必有比它大的代数扩域。

证明 设 F 是一个有 p^n 个元的有限域，在 F 上作多项式 $x^{p^{2n}} - x$ 的分裂域 E，则 $F \subseteq E$ 且 E 是 F 的一个代数扩域。又 E 至少含有多项式 $x^{p^{2n}} - x$ 的 p^{2n} 个不同的根，故 E 大于 F。

习题全解

§1　扩域和素域(P252)

1. 设E是域F的一个扩域，而M与N是扩域E的两个子集。证明：$F(M\cup N)=F(M)$当且仅当$N\subseteq F(M)$。

证明　"$\Leftarrow$"　$F(M\cup N)$表示E中包含$F\cup M\cup N$的最小子域，$F(M)$表示E中包含$F\cup M$的最小子域，从而若$N\subseteq F(M)$，则有$F(M\cup N)\subseteq F(M)$，故$F(M\cup N)=F(M)$。

"$\Rightarrow$"　若$F(M\cup N)=F(M)$，据$F(M\cup N)$与$F(M)$的定义，显见有$N\subseteq F(M)$。

---

2. 设E是特征为素数p的一个域。证明：

$$\Delta=\{0,e,2e,\cdots,(p-1)e\}$$

作成E的一个子域，且为E中的素域。

证明　记$Z_p=\{\bar{0},\bar{1},\bar{2},\cdots,\overline{p-1}\}$，任$\bar{x}\in Z_p$，定义

$$\varphi:\bar{x}\longrightarrow xe$$

则φ是素域Z_p到Δ的一个同构映射，即$Z_p\cong\Delta$，由定理1即可知Δ是包含在E中的素域。

---

3. 设a是一个正有理数，Q是有理数域。证明：

$$Q(\sqrt{a},\mathrm{i})=Q(\sqrt{a}+\mathrm{i})$$

证明　显见$\sqrt{a}+\mathrm{i}\in Q(\sqrt{a},\mathrm{i})$ 故 $Q(\sqrt{a}+\mathrm{i})\subseteq Q(\sqrt{a},\mathrm{i})$

又$\sqrt{a}+\mathrm{i}\in Q(\sqrt{a}+\mathrm{i})$，故$\sqrt{a}-\mathrm{i}=\dfrac{1}{1+a}(\sqrt{a}+\mathrm{i})\in Q(\sqrt{a}+\mathrm{i})$，于是可知$\sqrt{a}\in Q(\sqrt{a}+\mathrm{i})$，$\mathrm{i}\in Q(\sqrt{a}+\mathrm{i})$，所以$Q(\sqrt{a},\mathrm{i})\subseteq Q(\sqrt{a}+\mathrm{i})$，从而

$$Q(\sqrt{a},\mathrm{i})=Q(\sqrt{a}+\mathrm{i})$$

4. 设 Q 是有理数域。证明

$$Q\left(\frac{1}{5},\sqrt{2}+3,7\sqrt{3}\right)=Q(\sqrt{2},\sqrt{3})$$

证明　由于$\frac{1}{5}$,3,7 $\in Q$,故有

$$\sqrt{2},\sqrt{3}\in Q\left(\frac{1}{5},\sqrt{2}+3,7\sqrt{3}\right)$$

从而
$$Q(\sqrt{2},\sqrt{3})\subseteq Q\left(\frac{1}{5},\sqrt{2}+3,7\sqrt{3}\right)$$

同理可得 $Q\left(\frac{1}{5},\sqrt{2}+3,7\sqrt{3}\right)\subseteq Q(\sqrt{2},\sqrt{3})$。所以

$$Q\left(\frac{1}{5},\sqrt{2}+3,7\sqrt{3}\right)=Q(\sqrt{2},\sqrt{3})$$

---

5. 证明:$Q(\sqrt{2}+\sqrt{3})$ 是由一切形如

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$$

的数作成的数域,其中 $a,b,c,d\in Q$。

证明　不妨设$\sqrt{2}+\sqrt{3}=x$,则易得 $x^4-10x^2+1=0$。而 $p(x)=x^4-10x^2+1$ 在 Q 上不可约,故 $p(x)$ 是$\sqrt{2}+\sqrt{3}$ 在 Q 上的最小多项式,因此任 $t\in Q(\sqrt{2}+\sqrt{3})$,均可由

$$1,\sqrt{2}+\sqrt{3},(\sqrt{2}+\sqrt{3})^2,(\sqrt{2}+\sqrt{3})^3$$

线性表示。

又由$(\sqrt{2}+\sqrt{3})^2=5+2\sqrt{6}$ 可知$\sqrt{6}\in Q(\sqrt{2}+\sqrt{3})$;

由$(\sqrt{2}+\sqrt{3})^3=2\sqrt{2}+9(\sqrt{2}+\sqrt{3})$ 可知$\sqrt{2}\in Q(\sqrt{2}+\sqrt{3})$,进而可知$\sqrt{3}=\sqrt{2}+\sqrt{3}-\sqrt{2}\in Q(\sqrt{2}+\sqrt{3})$。所以

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

§ 2　单扩域(P257)

1. 设 α 是域 F 中的任一元素。证明:α 是域 F 上的代数元,且

$$F(\alpha)=F$$

证明　$f(x)=x-\alpha$ 为 $F(x)$ 的一个非零多项式且 $f(\alpha)=0$,所以 α 是 F

上的一个代数元。

由于 F 是含 F 和 α 的一个 E 的子域，而 $F(\alpha)$ 是含 F 和 α 的 E 的最小子域，故 $F(\alpha)\subset F$。又显见 $F(\alpha)$ 包含 F 与 α，$F\subset F(\alpha)$，故 $F(\alpha)=F$。

2. 设 $p(x)$ 为域 F 上首系数为 1 的多项式，且有根 α。证明：若 $p(x)$ 在 F 上不可约，则 $p(x)$ 是 α 在 F 上的最小多项式。

证明　不妨设 $g(x)$ 是 α 在 F 上的最小多项式，由于 $p(x)$ 在某扩域上满足 $p(\alpha)=0$，故由定理 1 知 $g(x)\mid p(x)$。又 $p(x)$ 不可约，且 $p(x)$ 与 $g(x)$ 的首系数均为 1，故 $p(x)=g(x)$，即 $p(x)$ 是 α 在 F 上的最小多项式。

3. 求$\sqrt{2}+\sqrt{3}$ 在有理数域 Q 上的最小多项式，并证明：

$$Q(\sqrt{2},\sqrt{3})=Q(\sqrt{2}+\sqrt{3})$$

证明　由本章 §1 第 5 题知$\sqrt{2}+\sqrt{3}$ 的最小多项式为 x^4-10x^2+1。

由$\sqrt{2},\sqrt{3}\in Q(\sqrt{2},\sqrt{3})$ 可知$\sqrt{2}+\sqrt{3}\in Q(\sqrt{2},\sqrt{3})$，从而

$$Q(\sqrt{2}+\sqrt{3})\subseteq Q(\sqrt{2},\sqrt{3})$$

又$\sqrt{2}+\sqrt{3}\in Q(\sqrt{2}+\sqrt{3})$，以及 $Q(\sqrt{2}+\sqrt{3})$ 为域，所以

$$(\sqrt{2}+\sqrt{3})^{-1}=\sqrt{3}-\sqrt{2}\in Q(\sqrt{2}+\sqrt{3})$$

因此$(\sqrt{2}+\sqrt{3})+(\sqrt{3}-\sqrt{2})=2\sqrt{3}\in Q(\sqrt{2}+\sqrt{3})$。又 $Q\subseteq Q(\sqrt{2}+\sqrt{3})$，故$\sqrt{3}\in Q(\sqrt{2}+\sqrt{3})$，于是$\sqrt{2}=(\sqrt{2}+\sqrt{3})-\sqrt{3}\in Q(\sqrt{2}+\sqrt{3})$，从而$\sqrt{2},\sqrt{3}\in Q(\sqrt{2}+\sqrt{3})$，$Q(\sqrt{2},\sqrt{3})\subseteq Q(\sqrt{2}+\sqrt{3})$，所以

$$Q(\sqrt{2},\sqrt{3})=Q(\sqrt{2}+\sqrt{3})$$

4. 设 $F(\alpha)$ 与 $F(\beta)$ 是域 F 上两个单代数扩域，并且 α 与 β 在 F 上有相同的最小多项式。证明：$F(\alpha)\cong F(\beta)$。又问：反之如何？

证明　设 α 与 β 在 F 上的最小多项式为 $p(x)$，且 $\deg p(x)=n$，则

$$F(\alpha)=\left\{\sum_{i=0}^{n}a_i\alpha^i\,\middle|\,a_i\in F\right\},F(\beta)=\left\{\sum_{i=0}^{n}a_i\beta^i\,\middle|\,a_i\in F\right\}$$

定义

$$\varphi:f(\alpha)\longrightarrow f(\beta)$$

其中 $f(\alpha)\in F(\alpha)$，$f(\beta)\in F(\beta)$，则 φ 是 $F(\alpha)$ 到 $F(\beta)$ 的保持加法的一一映射。

对于乘法，任 $f(\alpha)g(\alpha)\in F(\alpha)$，用 $p(x)$ 对 $f(x)g(x)$ 作带余除法，得

$$f(x)g(x)=q(x)p(x)+r(x)$$

其中 $r(x)=0$，或 $\deg r(x)\leqslant \deg p(x)$，则

$$f(\alpha)g(\alpha)=r(\alpha),f(\beta)g(\beta)=r(\beta)$$

从而

$$\varphi(f(\alpha)g(\alpha))=\varphi(r(\alpha))=r(\beta)=f(\beta)g(\beta)=\varphi(f(\alpha))\varphi(g(\alpha))$$

即 φ 也保持乘法运算。由此即可得 $F(\alpha)\cong F(\beta)$。

反之不成立。例如虚数单位 i 在有理数域 Q 上的最小多项式为 x^2+1，$\frac{1}{2}+\frac{3}{2}\mathrm{i}$ 在 Q 上的最小多项式为 $x^2-x+\frac{5}{2}$，又易验证 $Q(\mathrm{i})=Q\left(\frac{1}{2}+\frac{3}{2}\mathrm{i}\right)$。二者同构，但 i 与 $\frac{1}{2}+\frac{3}{2}\mathrm{i}$ 的最小多项式不同。

---

5. 问：复数 i 及 $\frac{2\mathrm{i}+1}{\mathrm{i}-1}$ 在有理数域 Q 上的最小多项式各为何？又单扩域

$$F(\mathrm{i})\text{ 与 }F\left(\frac{2\mathrm{i}+1}{\mathrm{i}-1}\right)$$

是否同构？

解 $\frac{2\mathrm{i}+1}{\mathrm{i}-1}=\frac{1}{2}-\frac{3}{2}\mathrm{i}$，则由本章 §2 第 4 题可知在 Q 上 i 的最小多项式为 x^2+1，$\frac{1}{2}-\frac{3}{2}\mathrm{i}$ 的最小多项式为 $x^2-x+\frac{5}{2}$。

由 $\mathrm{i}=\frac{1}{3}-\frac{2}{3}\left(\frac{1}{2}-\frac{3}{2}\mathrm{i}\right)\in F\left(\frac{2\mathrm{i}+1}{\mathrm{i}-1}\right)$ 知 $F(\mathrm{i})\subseteq F\left(\frac{2\mathrm{i}+1}{\mathrm{i}-1}\right)$。又显见

$$F\left(\frac{2\mathrm{i}+1}{\mathrm{i}-1}\right)=F\left(\frac{1}{2}-\frac{3}{2}\mathrm{i}\right)\subseteq F(\mathrm{i})$$

所以 $F(\mathrm{i})=F\left(\frac{2\mathrm{i}+1}{\mathrm{i}-1}\right)$。二者当然同构。

---

6. 设 $p(x)$ 是域 F 上的 n 次不可约多项式。证明：域 $F[x]/\langle p(x)\rangle$ 中的每一个元素都可以惟一地表示成

$$a_0+a_1x+\cdots+a_{n-1}x^{n-1}+\langle p(x)\rangle, a_i\in F$$

证明 任 $f(x)\in F[x]$，令

$$f(x)=p(x)q(x)+r(x)$$

其中 $r(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$。则任 $\bar{f}(x)\in F[x]/\langle p(x)\rangle$ 有

$$\begin{aligned}\bar{f}(x)&=f(x)+\langle p(x)\rangle\\&=p(x)q(x)+r(x)+\langle p(x)\rangle\\&=r(x)+\langle p(x)\rangle\end{aligned}$$

下证表示法惟一。若还有

$$\bar{f}(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}+\langle p(x)\rangle$$

则可得 $(a_0-b_0)+(a_1-b_1)x+\cdots+(a_{n-1}-b_{n-1})x^{n-1}\in\langle p(x)\rangle$

即 $p(x)\mid((a_0-b_0)+(a_1-b_1)x+\cdots+(a_{n-1}-b_{n-1})x^{n-1})$，又 $\deg p(x)=n$，于是必有

$$(a_0-b_0)+(a_1-b_1)x+\cdots+(a_{n-1}-b_{n-1})x^{n-1}=0$$

故 $$a_i=b_i\quad(i=0,1,\cdots,n-1)$$

即表示法惟一。

§ 3 代数扩域(P265)

1. 证明：(1) 复数域是实数域的代数扩域；

(2) 实数域是有理数域的超越扩域，但不是纯超越扩域。

证明 (1) 显见复数域 C 为实数域 R 的扩域，任 $\alpha=a+bi\in C$，则存在 R 上的非零多项式 $f(x)=x^2-2ax+(a^2+b^2)$，使 $f(\alpha)=0$，即任 $\alpha\in C$ 均为 R 的代数元，所以域 C 为域 R 的代数扩域。

(2) 显见实数域 R 是有理数域 Q 的扩域，又 $\pi\in R$ 为 Q 的超越元，故域 R 为域 C 的超越扩域。而 $\sqrt{3}\in R$，$\sqrt{3}\notin Q$，存在 Q 上的多项式 $f(x)=x^2-3$ 使 $f(\sqrt{3})=0$，即 $\sqrt{3}$ 为域 Q 的代数元，从而域 R 不是域 Q 的纯超越扩域。

---

2. 证明：域 F 上未定元 x 的有理分式域 $F(x)$ 是 F 的一个纯超越扩域。

证法 1 任取

$$f(x)=a_mx^m+\cdots+a_1x+a_0\in F(x)$$

其中 $a_m \neq 0, m \geqslant 1$。再令

$$b_n f^n(x) + b_{n-1} f^{n-1}(x) + \cdots + b_1 f(x) + b_0 = 0$$

其中 $b_i \in F$。则上式左端最高项系数 $b_n a_m^n = 0$，而 $a_m \neq 0$，因此 $b_n = 0$，于是

$$b_{n-1} f^{n-1}(x) + \cdots + b_1 f(x) + b_0 = 0$$

类似于上面讨论知 $b_{n-1} = b_{n-2} = \cdots = b_0 = 0$，故 $f(x)$ 是 F 上的超越元。

如果

$$b_n \left(\frac{f(x)}{g(x)}\right)^n + \cdots + b_1 \frac{f(x)}{g(x)} + b_0 = 0$$

则可化为以上情况，故 $b_n = \cdots = b_1 = b_0 = 0$。即$\dfrac{f(x)}{g(x)}$也是 F 上的超越元。

从而 $F(x)$ 是 F 的纯超越扩域。

证法 2 任取$\dfrac{f(x)}{g(x)} \in F(x)$，其中 $f(x)$ 与 $g(x)$ 是既约多项式。若$\dfrac{f(x)}{g(x)}$为 F 的代数元，则有某

$$a_n \left(\frac{f(x)}{g(x)}\right)^n + \cdots + a_1 \frac{f(x)}{g(x)} + a_0 = 0$$

其中 $a_i \in F$，上式可化为

$$a_n f^n(x) + a_{n-1} f^{n-1}(x) g(x) + \cdots + a_1 f(x) g^{n-1}(x) + a_0 g^n(x) = 0$$

由此可知 $f(x) \mid g(x)$ 且 $g(x) \mid f(x)$，于是有$\dfrac{f(x)}{g(x)} \in F$，从而 $F(x)$ 是 F 的纯超越扩域。

---

3. 设 p 是一个素数，证明：

$$Q(\sqrt{p}, \sqrt[3]{p}, \sqrt[4]{p}, \cdots)$$

是有理数域 Q 上的一个无限次代数扩域。

证明 显见$\sqrt[n]{p}$满足 Q 上 $f(x) = x^n - p = 0$，故$\sqrt[n]{p}(n = 2, 3, \cdots)$为 Q 上的代数元，从而 $Q(\sqrt{p}, \sqrt[3]{p}, \sqrt[4]{p}, \cdots)$为 Q 上的代数扩域。

下证其为 Q 的无限次扩域。否则，不妨设

$$(Q(\sqrt{p}, \sqrt[3]{p}, \sqrt[4]{p}, \cdots) : Q) = n$$

则由$\sqrt[n+1]{p}$在 Q 上的最小多项式为 $x^{n+1} - p$ 知

$$(Q(\sqrt[n+1]{p}):Q)=n+1$$

这与 $Q\subseteq Q(\sqrt[n+1]{p})\subseteq Q(\sqrt{p},\sqrt[3]{p},\sqrt[4]{p},\cdots)$ 相矛盾，从而 $Q(\sqrt{p},\sqrt[3]{p},\sqrt[4]{p},\cdots)$ 为 Q 上的无限次代数扩域。

---

4. 求有理数域 Q 的扩域 $Q(\sqrt[3]{2}+\sqrt[3]{4})$ 在 Q 上的次数。

解 设 $\sqrt[3]{2}+\sqrt[3]{4}=\alpha$，则

$$\alpha^3=6\sqrt[3]{2}+6\sqrt[3]{4}+6=6\alpha+6$$

因此 α 是 Q 上多项式 $p(x)=x^3-6\alpha-6$ 的根。又 $p(x)$ 在 Q 上不可约，故 $p(x)$ 为 α 在 Q 上的最小多项式。从而 α 是 Q 上的一个 3 次代数元，于是有

$$(Q(\sqrt[3]{2}+\sqrt[3]{4}):Q)=3$$

---

5. 不利用本节结论，直接证明代数数的和仍为代数数。

证明 不妨设 α,β 为任两个代数数，且分别为域 Q 上多项式 $f(x)$ 与 $g(x)$ 的根，其中 $f(x)$ 与 $g(x)$ 的全部根分别为

$$\alpha_1,\alpha_2,\cdots,\alpha_m \text{ 与 } \beta_1,\beta_2,\cdots,\beta_n$$

则由对称多项式基本定理可得

$$h(x)=\prod_{i=1}^{m}\prod_{j=1}^{n}(x-(\alpha_i+\beta_j))\in Q[x]$$

且 $\alpha+\beta$ 为其根，因此 $\alpha+\beta$ 仍是 Q 上的代数数。

§ 4 多项式的分裂域(P270)

1. Q 上的单扩域 $Q(\sqrt[3]{2})$ 是不是 Q 上某个多项式在 Q 上的分裂域？

解 $\sqrt[3]{2}$ 在域 Q 上的最小多项式为 x^3-2，而

$$x^3-2=(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+\sqrt[3]{4})$$

有虚根，但是 $Q(\sqrt[3]{2})$ 中不含虚数，因此 $Q(\sqrt[3]{2})$ 不是 Q 上任何多项式的分裂域。

---

2. 求 $f(x)=x^3-x^2-x-2$ 在 Q 上的分裂域。

解 由 $f(x)=(x-2)(x^2+x+1)$ 知其有根 $2,-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}$ 与 $-\frac{1}{2}-$

$\frac{\sqrt{3}}{2}\mathrm{i}$，从而 $f(x)$ 在 Q 上的分裂域为

$$Q\left(2, -\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}, -\frac{1}{2}-\frac{\sqrt{3}}{2}\mathrm{i}\right)=Q(\sqrt{3}\mathrm{i})$$

---

3. 证明：x^4+1 在有理数域 Q 上的分裂域是一个单扩域 $Q(\alpha)$，其中 α 是 x^4+1 的一个根。

证明 记 $\alpha=\frac{\sqrt{2}}{2}(1+\mathrm{i})$，则易知 x^4+1 的全部根为 $\pm\alpha$，$\pm\alpha\mathrm{i}$，因此 x^4+1 在 Q 上的分裂域为 $Q(\alpha,-\alpha,\alpha\mathrm{i},-\alpha\mathrm{i})=Q(\alpha,\mathrm{i})$

而 $\mathrm{i}=\alpha^2\in Q(\alpha)$，故 $Q(\alpha,\mathrm{i})=Q(\alpha)$。于是 x^4+1 在 Q 上的分裂域是单扩域 $Q(\alpha)$。

或易知 x^4+1 的 4 个根分别为 $\alpha_1=\frac{\sqrt{2}}{2}(1+\mathrm{i})$，$\alpha_2=\frac{\sqrt{2}}{2}(1-\mathrm{i})$，$\alpha_3=-\alpha_1$，$\alpha_4=-\alpha_2$，且 $\alpha_2=-\alpha_1{}^3$，从而 $Q(\alpha_1,\alpha_2,\alpha_3,\alpha_4)=Q(\alpha_1)$，令 $\alpha=\alpha_1$，则单扩域 $Q(\alpha)$ 即为 x^4+1 在 Q 上的分裂域。

---

4. 设 x^3-a 是 Q 上一个不可约多项式，而 α 是 x^3-a 的一个根。证明：$Q(\alpha)$ 不是 x^3-a 在 Q 上的分裂域。

证明 易知 x^3-a 的所有根为 α，$\alpha\omega$，$\alpha\omega^2$，其中

$$\omega=\frac{-1+\sqrt{3}\mathrm{i}}{2}$$

假设 $Q(\alpha)$ 是 $\varphi(x)=x^3-a$ 的分裂域，则 $\alpha\omega\in Q(\alpha)$，从而

$$\omega\in Q(\alpha)$$

于是有

$$Q\subset Q(\omega)\leqslant Q(\alpha)$$

由定理 2，$(Q(\omega):Q)$ 应该是 $(Q(\alpha):Q)$ 的约整数，而 ω 在 Q 上的最小多项式为 x^2+x+1，则

$$(Q(\omega):Q)=2$$

但 α 在 Q 上的最小多项式为 $\varphi(x)=x^3-a$，故

$$(Q(\alpha):Q)=3$$

显见$(Q(\omega):Q)$不是$(Q(\alpha):Q)$的约数，矛盾。从而$Q(\alpha)$不是x^3-a在Q上的分裂域。

5. 设E是域F上$n>0$次多项式在F上的分裂域。证明：

$$(E:F)\leqslant n!$$

证明　对多项式$f(x)$的次数用数学归纳法。

$n=1$时，$f(x)$是F上的不可约多项式，是其惟一根α_1在F上的最小多项式，故$f(x)$的分裂域$E=F(\alpha_1)$关于F的次数为$1=1!$，即$(E:F)=1!$。

假设结论对$n-1$成立。令$\alpha_1,\alpha_2,\cdots,\alpha_n$是$f(x)$在其分裂域$E$中的$n$个根，则$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$。现考虑$E$的子域$F(\alpha_1)$。显然$\alpha_1$在$F$上的最小多项式的次数$\leqslant n$，故

$$(F(\alpha_1):F)\leqslant n$$

在$F(\alpha_1)$上，$f(x)$可分解为

$$f(x)=(x-\alpha_1)\varphi(x)$$

其中$\varphi(x)$是$F(\alpha_1)$上的$n-1$次多项式，且$\alpha_2,\alpha_3,\cdots,\alpha_n$恰好为$\varphi(x)$在$F$中的所有$n-1$个根。由归纳假设，$\varphi(x)$在$F(\alpha_1)$上的分裂域$F(\alpha_1)(\alpha_2,\cdots,\alpha_n)$关于$F(\alpha_1)$的次数

$$(F(\alpha_1)(\alpha_2,\cdots,\alpha_n):F(\alpha_1))\leqslant(n-1)!$$

从而有

$$\begin{aligned}(F(\alpha_1,\alpha_2,\cdots,\alpha_n):F)&=(F(\alpha_1):F)(F(\alpha_1)(\alpha_2,\cdots,\alpha_n):F(\alpha_1))\\&\leqslant n(n-1)!=n!\end{aligned}$$

即

$$(E:F)\leqslant n!$$

6. 设p是一个素数，E是x^p-1在Q上的分裂域。证明

$$(E:Q)=p-1$$

证明　不妨设α为一个p次原根，则

$$x^p-1=\prod_{i=0}^{p-1}(x-\alpha^i)=(x-1)(x^{p-1}+\cdots+x+1)$$

故x^p-1在Q上的分裂域E为

$$E = Q(1, \alpha, \cdots, \alpha^{p-1}) = Q(\alpha)$$

而 α 在 Q 上的最小多项式为 $x^{p-1} + \cdots + x + 1$，次数为 $p-1$，因此 $(E : Q) = p-1$。

§5 有限域(P276)

1. 证明：多项式 x^2+x+1 与 x^3+x+1 在 Z_2 上不可约，再求出 8 阶有限域 $Z_2[x]/\langle x^3+x+1\rangle$ 的所有元素。

证明 由于 x^2+x+1 与 x^3+x+1 在 Z_2 上可约的充要条件是它们在 Z_2 内有根，但 $Z_2 = \{0,1\}$ 的元素都不是这两个多项式的根，所以它们在 Z_2 上不可约。

又 $Z_2[x]/\langle x^3+x+1\rangle$ 中元素都可惟一表为

$$a_0 + a_1 x + a_2 x^2 + \langle x^3+x+1\rangle$$

其中 $a_i \in Z_2$，故 $Z_2[x]/\langle x^3+x+1\rangle$ 中的 8 个元素分别为

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

---

2. 试求出域 Z_2 上全部的三次不可约多项式。

解 由本章 §5 第 1 题的讨论可知，即需求出使 x^3+ax^2+bx+c 在 Z_2 中无根的所有多项式，其中 $a,b,c \in Z_2$，从而 Z_2 上所有三次不可约多项式为

$$x^3+x+1, x^3+x^2+1$$

---

3. 证明：包含域 Z_p 的每个有限域都是 Z_p 的单扩域。

证明 不妨设 F 是任一个包含 Z_p 的有限域，由本章 §5 定理 4 知，乘群 F^* 是循环群。令 $F^* = \langle\alpha\rangle$，从而由已知可得

$$Z_p \subseteq \{0, 1, \alpha, \cdots, \alpha^n\} = F$$

故 $F = Z_p(\alpha)$ 为 Z_p 的单扩域。

---

4. 设 F 是一个域。证明：乘群 F^* 为循环群 $\Leftrightarrow F$ 为有限域。

证明 由定理 4 知充分性成立。下证必要性。

若 F^* 为循环群，令 $F^* = \langle\alpha\rangle$，则

$$F = \{\cdots, \alpha^{-2}, \alpha^{-1}, 0, \alpha, \alpha^2, \cdots\}$$

记 F 中的素域为 Δ，则 $F=\Delta(\alpha)$。

若 $\mathrm{char}F=\infty$，则 $\Delta\cong Q$，故 $Q^*\cong\Delta^*\leqslant F^*$，又由 F^* 为循环群，可知其子群 Δ^* 也为循环群，从而 Q^* 为循环群，矛盾。

如果 $\mathrm{char}F=p$，则 $\Delta\cong Z_p$，而若 $\alpha+\alpha^2\in F$，则

$$\alpha+\alpha^2=0 \text{ 或 } \alpha+\alpha^2=\alpha^n \quad (n\neq 1,2)$$

因此 α 为 Δ 上的代数元，故 $F=\Delta(\alpha)$ 为有限域。

5. 设 F 为 q 阶有限域，$f(x)$ 为 F 上一个 n 次不可约多项式。证明：$f(x)$ 整除 $x^{q^n-1}-1$。

证明　因为 $f(x)$ 为 F 上一个 n 次不可约多项式，其中 F 为 q 阶有限域，故

$$F[x]/\langle f(x)\rangle$$

为 q^n 元域，于是其所有非零元作成一个 q^n-1 阶群。从而对于 $x+\langle f(x)\rangle\in F[x]/\langle f(x)\rangle$，有

$$x^{q^n-1}+\langle f(x)\rangle=1+\langle f(x)\rangle$$

$$x^{q^n-1}-1\in\langle f(x)\rangle$$

于是

$$f(x)\,\Big|\,x^{q^n-1}-1$$

§6　可离扩域(P286)

1. 设 Q 是有理数域，i 是虚数单位。证明

$$Q(\sqrt{2},\mathrm{i})=Q(\sqrt{2}+\mathrm{i})$$

证明　显见 $\sqrt{2},\mathrm{i}\in Q(\sqrt{2},\mathrm{i})$，故 $\sqrt{2}+\mathrm{i}\in Q(\sqrt{2},\mathrm{i})$，从而

$$Q(\sqrt{2}+\mathrm{i})\subseteq Q(\sqrt{2},\mathrm{i})$$

由 $(\sqrt{2}+\mathrm{i})\in Q(\sqrt{2}+\mathrm{i})$ 知 $(\sqrt{2}+\mathrm{i})^{-1}\in Q(\sqrt{2}+\mathrm{i})$，即

$$\frac{1}{3}(\sqrt{2}-\mathrm{i})\in Q(\sqrt{2}+\mathrm{i})$$

于是 $(\sqrt{2}-\mathrm{i})\in Q(\sqrt{2}+\mathrm{i})$。从而结合 $(\sqrt{2}+\mathrm{i})\in Q(\sqrt{2}+\mathrm{i})$ 知 $\sqrt{2},\mathrm{i}\in Q(\sqrt{2}+\mathrm{i})$，故有

$$Q(\sqrt{2},\mathrm{i}) \subseteq Q(\sqrt{2}+\mathrm{i})$$

所以
$$Q(\sqrt{2},\mathrm{i}) = Q(\sqrt{2}+\mathrm{i})$$

---

2. 设 p,q 都是素数。证明：

$$Q(\sqrt{p},\sqrt{q}) = Q(\sqrt{p}+\sqrt{q})$$

证明 一方面，显见$\sqrt{p},\sqrt{q} \in Q(\sqrt{p},\sqrt{q})$，故$\sqrt{p}+\sqrt{q} \in Q(\sqrt{p},\sqrt{q})$，从而

$$Q(\sqrt{p}+\sqrt{q}) \subseteq Q(\sqrt{p},\sqrt{q})$$

另一方面若 $p = q$，易知 $Q(\sqrt{p},\sqrt{q}) \subseteq Q(\sqrt{p}+\sqrt{q})$。

若 $p \neq q$，由$(\sqrt{p}+\sqrt{q}) \in Q(\sqrt{p}+\sqrt{q})$ 知$(\sqrt{p}+\sqrt{q})^{-1} \in Q(\sqrt{p}+\sqrt{q})$，即

$$\frac{\sqrt{p}-\sqrt{q}}{p-q} \in Q(\sqrt{p}+\sqrt{q})$$

于是$\sqrt{p}-\sqrt{q} \in Q(\sqrt{p}+\sqrt{q})$。结合$\sqrt{p}+\sqrt{q} \in Q(\sqrt{p}+\sqrt{q})$ 知$\sqrt{p},\sqrt{q} \in Q(\sqrt{p}+\sqrt{q})$，从而

$$Q(\sqrt{p},\sqrt{q}) \subseteq Q(\sqrt{p}+\sqrt{q})$$

所以

$$Q(\sqrt{p},\sqrt{q}) = Q(\sqrt{p}+\sqrt{q})$$

---

3. 设 $\mathrm{char}F = p$，且域 F 不是完全域。证明：$p(x) = x^{p^n} - a$ 在域 F 上不可约的充要条件是，a 不是 F 中任何元素的 p 次幂。

证明 "$\Rightarrow$" 设 $p(x)$ 在域 F 上不可约，若存在 $b \in F$，使 $a = b^p$，则由 $\mathrm{char}F = p$ 可知

$$p(x) = x^{p^n} - a = x^{p^n} - b^p = (x^{p^{n-1}} - b)^p$$

即 $p(x)$ 在 F 上可约，矛盾，故任 $b \in F$，$a \neq b^p$。

"$\Leftarrow$" 设任 $b \in F$，$a \neq b^p$。若 $p(x)$ 在 F 上可约，不妨设

$$p(x) = h(x)g(x)$$

其中 $h(x),g(x) \in F[x]$，$\deg g(x) = k \leqslant p^n - 1$，$\beta$为 $p(x)$ 在域 F 上的分裂域 E 内的一个根，故有 $\beta^{p^n} = a$，且在 E 上

$$p(x) = (x-\beta)^{p^n} = h(x)g(x)$$

又可知

$$g(x) = (x-\beta)^k = x^k + \cdots + (-1)^k\beta^k \in F[x]$$

因此 $\beta^k \in F$。

其中设 $k = p^m k_1$，$p \nmid k_1$。则易知 $m < n$ 且 $(p,k_1) = 1$，于是存在整数 s,t，使

$$ps + k_1 t = 1, p^n s + p^{n-1}k_1 t = p^{n-1}$$

于是可得

$$\beta^{p^{n-1}} = \beta^{p^n s + p^{n-1}k_1 t} = (\beta^{p^n})^s \cdot (\beta^k)^{tp^{n-m-1}} \in F$$

从而 $b = \beta^{p^{n-1}} \in F$，因此

$$a = \beta^{p^n} = (\beta^{p^{n-1}})^p = b^p$$

与 $a \neq b^p$ 矛盾，所以 $p(x)$ 在 F 上不可约。

---

4. 令 $F = Z_p(u)$ 是例 3 中的域。证明：F 上多项式 $f(x) = x^p - u$ 在 F 上不可约，但在其分裂域中有重根。

证明　假设 $f(x)$ 在域 F 上可约，不妨令

$$f(x) = h(x)g(x)$$

其中 $h(x),g(x) \in F[x]$，$g(x)$ 为首系数为 1 的 k 次多项式，$1 \leqslant k < p$，b 是 $f(x)$ 在 F 上的分裂域 E 内的一个根，则

$$u = b^p$$

$$f(x) = x^p - u = x^p - b^p = (x-b)^p = h(x)g(x)$$

$$g(x) = (x-b)^k = x^k + \cdots + (-1)^k b^k \in F[x]$$

因此 $b^k \in F$。由 $1 \leqslant k < p$ 及 $(k,p) = 1$ 可知存在常数 s,t，使 $ks + pt = 1$，结合 $b^k, u \in F$ 即得

$$b = b^{ks+pt} = (b^k)^s \cdot (b^p)^t = (b^k)^s \cdot u^t \in F$$

即 $u = b^p$，这同上例所证 $u \neq b^p$（任 $b \in F$）相矛盾，故 $x^p - u$ 在 F 上不可约。

由于 $u = b^p$，故在分裂域 E 中

$$x^p - u = x^p - b^p = (x-b)^p$$

显见 $x^p - u$ 在 E 中是有重根的。

---

5. 设 $\mathrm{char}F = p$，a 是域 F 上的可离元。证明：a^p 也是 F 上的可离元。

证明 由 α 是域 F 的可离元及定理 4 可知 $F(\alpha)=F(\alpha^p)$。要证 α^p 是 F 上的可离元，只需证明 $F(\alpha)=F(\alpha^p)$ 为域 F 的可离扩域，而这由定理 5 即可知(如，若 α 与 1 是 F 的可离扩域，则 $F(\alpha,1)=F(\alpha)$ 是可离扩域)，从而 α^p 是 F 的可离元。

---

6. 设 $\mathrm{char}F=p$，α 是域 F 上的不可离元。证明：若 $p\nmid r(r>0)$，则 α^r 也是 F 上的不可离元。

证明 利用反证法证明。假设 α^r 是 F 上的可离元，则其 F 上的最小多项式 $f(x)$ 无重根，不妨设

$$f(x)=(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)=\prod_{i=1}^{n}f_i(x)$$

其中 $i\neq j$ 时，$\beta_i\neq\beta_j$，$f_i(x)=x-\beta_i(i,j=1,2,\cdots,n)$。由 $f(x)$ 在 F 上不可约可知 $\beta_i\neq 0(i=1,2,\cdots,n)$。而 $\mathrm{char}F=p$，$p\nmid r$，故 $f_i(x^r)=x^r-\beta_i$ 与 $f'_i(x^r)=rx^{r-1}\neq 0$ 互素，$f_i(x)$ 无重根$(i=1,2,\cdots,n)$，于是 $f(x^r)=\prod_{i=1}^{n}f_i(x^r)$ 也无重根。

设 α 在 F 上的最小多项式为 $g(x)$，依题设可知 $g(x)$ 在 F 上不可约且有重根，但 $f(x^r)=0$，因此 $g(x)\mid f(x^r)$，而这与 $g(x)$ 有重根而 $f(x^r)$ 无重根矛盾，故 α^r 是 F 上的不可离元。

---

7. 问：映射 $\varphi: a+b\sqrt{2}\longrightarrow a+b\sqrt{3}$ 是否是有理数域 Q 上的单扩域 $Q(\sqrt{2})$ 与 $Q(\sqrt{3})$ 的同构映射？这两个单扩域是否同构？

解 如果单扩域 $Q(\sqrt{2})$ 与 $Q(\sqrt{3})$ 同构，不妨设 Ψ 为 $Q(\sqrt{2})$ 到 $Q(\sqrt{3})$ 的一个同构映射。则令

$$\Psi(\sqrt{2})=a+b\sqrt{3}$$

其中 $a,b\in Q$，且 $a^2+b^2\neq 0$，由同构映射的性质(即单位元的象是单位元，逆元的象是象的逆元)可知任一有理数的象为自身，从而由上述映射知

$$2=(a+b\sqrt{3})^2=a^2+3b^2+2ab\sqrt{3}$$

因此 $ab=0$，$2=a^2+3b^2$，故 $a=\pm\sqrt{2}$，$b=0$，或 $a=0$，$b=\pm\sqrt{\frac{2}{3}}$，这与

$a, b \in Q$ 矛盾。

于是假设不成立，故 $Q(\sqrt{2})$ 与 $Q(\sqrt{3})$ 不同构。从而题设中的 Ψ 也不是 $Q(\sqrt{2})$ 到 $Q(\sqrt{3})$ 的同构映射。

---

8. 设有域 $F \subseteq K \subseteq E$，且 $(K:F)=m$，$\alpha \in E$ 是 F 上一个 n 次代数元，$(m, n)=1$。证明：α 也是 K 上的 n 次代数元。

证明　由 α 是 F 上的 n 次代数元知，若 $f(x)$ 为 F 上的最小多项式，则 $\deg f(x)=n$，又 $F \subseteq K$，故 α 也是 K 上的代数元。设 $g(x)$ 为 α 在 K 上的最小多项式，且 $\deg g(x)=s$，则有

$$(K(\alpha):K)=s$$

易知 $f(x)$ 也是 α 在 K 上的多项式，故在 F 上 $f(\alpha)=g(\alpha)=0$，于是由 $g(x)$ 为 α 在 K 上的最小多项式知

$$g(x) \mid f(x)$$

因此 $\deg g(x) \leqslant \deg f(x)$，即 $s \leqslant n$。

又 $F \subseteq K \subseteq K(\alpha)$，$F \subseteq F(\alpha) \subseteq K(\alpha)$，因此由次数定理及 $(K:F)=m$ 可得

$$(K(\alpha):F)=(K(\alpha):K)(K:F)=sm$$
$$(K(\alpha):F)=(K(\alpha):F(\alpha))(F(\alpha):F)=tn$$

其中 $t=(K(\alpha):F(\alpha))$，从而 $sm=tn$，$n \mid sm$，而 $(m,n)=1$，故 $n \mid s$，结合已证得的 $s \leqslant n$ 可知 $s=n$。因此 α 在 K 上的最小多项式的次数也是 n，即 α 也是 K 上的 n 次代数元。

---

9. 设 E 是域 F 的一个扩域。证明：若 $\alpha \in E$ 是 F 上的一个奇次代数元，则 α^2 也是 F 上的一个奇次代数元，并且

$$F(\alpha)=F(\alpha^2)$$

证明　由 $\alpha^2 \in F(\alpha)$ 可知 $F \subseteq F(\alpha^2) \subseteq F(\alpha)$，故

$$(F(\alpha):F)=(F(\alpha):F(\alpha^2))(F(\alpha^2):F)$$

又由 α 是 F 上的奇次代数元可知上式左端 $(F(\alpha):F)$ 是奇数，故上式右端中 $(F(\alpha^2):F)$ 是奇数，α^2 是域 F 上的奇次代数元。

若设 α 在域 $F(\alpha^2)$ 上的最小多项式为 $f(x)$，$\deg f(x)=m$，则也可由

上式得 m 为奇数(这是因为

$$F(\alpha)=F(\alpha^2,\alpha)=F(\alpha^2)(\alpha)$$

即 $F(\alpha)$ 为 $F(\alpha^2)$ 上的单扩域)。

而 α 为多项式 $x^2-\alpha^2(\in F(\alpha^2)[x])$ 的根,故 $f(x)\mid(x^2-2)$, $\deg f(x)=m\leqslant 2$,又已证 m 为奇数,所以 $m=1$,于是

$$(F(\alpha):F(\alpha^2))=1$$

即有 $F(\alpha)=F(\alpha^2)$。

---

10. 设 E 是域 F 的一个 4 次扩域,且 $\mathrm{char}F\neq 2$。证明:存在一个满足 $F\subseteq K\subseteq E$ 的 F 的 2 次扩域 K 的充要条件是:$E=F(\alpha)$,而 α 在 F 上的最小多项式是

$$x^4+ax^2+b\quad(a,b\in F)$$

证明 "⇒" 依题意,$(K:F)=2$,$(E:F)=4$,故 $(E:K)=2$。任取 $\beta\in K$, $\beta\notin E$,显见 β 在 K 上的最小多项式为 2 次的,不妨设为

$$x^2+e_1x+e_2$$

其中 $e_1,e_2\in K$,则 $\beta^2+e_1\beta+e_2=0$。由 $\mathrm{char}F\neq 2$ 可知 $\beta+\frac{e_1}{2}$ 及 $\frac{e_1^2}{4}-e_2$ 均有意义且分别为 E 和 K 中的元素。记 $\beta+\frac{e_1}{2}=\alpha$,则

$$\alpha^2=\left(\beta+\frac{e_1}{2}\right)^2=(\beta^2+e_1\beta+e_2)+\frac{e_1^2}{4}-e_2$$

记上式右端为 d,则 α 是 K 上多项式 x^2-d 的根,于是 x^2-d 为 α 在 K 上的最小多项式且 $E=K(\alpha)$。下对 d 进行讨论。

① 因为 $(K:F)=2$,故若 $d\notin F$,则 d 在 F 上的最小多项式可设为如下形式:

$$x^2+ax+b$$

其中 $a,b\in F$ 且 $K=F(d)$,故 $d^2+ad+b=0$,即 $\alpha^4+a\alpha^2+b=0$,又 $E=K(\alpha)$,结合 $K=F(d)$ 知 $E=F(\alpha)$,由已知 $(E:F)=4$,因此 α 在 F 上的最小多项式为

$$x^4+ax^2+b\quad(a,b\in F)$$

② 若 $d\in F$,同样由 $(K:F)=2$ 知存在元素 $e_3\in K$,使 $e_3\notin F$,

$e_3^2 \in F$，设 $\alpha = \omega(1+e_3)$，则有

$$\alpha^2 = \omega^2(1+2e_3+e_3^2)$$

故由 $e_3 \notin F, e_3^2 \in F$ 得 $\alpha^2 \notin F$。从而同①，有 $E = F(\alpha)$，其中 α 在 F 上的最小多项式为

$$x^4+ax^2+b \quad (a,b \in F)$$

"$\Leftarrow$"　由已知 $E = F(\alpha)$，其中 α 在 F 上的最小多项式为 x^4+ax^2+b，若令 $K = F(\alpha^2)$，则

$$F \subseteq K \subseteq E$$

且 x^2+ax+b 是 α^2 在 F 上的最小多项式。所以

$$(K:F) = (F(\alpha^2):F) = 2$$

即 K 为 F 的 2 次扩域。

---

11. 证明：$\varphi: a \longrightarrow a^p$ 是伽罗瓦域 $GF(p^n)$ 的一个自同构，且这个自同构在 $GF(p^n)$ 的自同构群中的阶是 n。

证明　因伽罗瓦域 $GF(p^n)$ 的特征为素数 p，故任取 $GF(p^n)$ 的非零乘群生成元 α，以下三个结论相互等价：

$$①\alpha^{mp} = \alpha^{np}; ②(\alpha^m-\alpha^n)^p = 0; ③\alpha^m = \alpha^n$$

从而若记 $q = p^n$，则

$$GF(p^n) = \{0,1,\alpha,\cdots,\alpha^{q-2}\} = (0,1,\alpha^p,\cdots,\alpha^{p(q-2)})$$

故 φ 为双射，又

$$(a+b)^p = a^p+b^p, (ab)^p = a^pb^p$$

因此 φ 是域 $GF(p^n)$ 的自同构。

由于 α 是域 $GF(p^n)$ 的非零乘群生成元，故 $|\alpha| = p^n-1, \alpha^{p^n} = \alpha$，又

$$\varphi^n(\alpha) = \alpha^{p^n} = \alpha, \varphi^m(\alpha) = \alpha^{p^m} \neq \alpha \quad (1 \leqslant m < n)$$

从而 α 在域 $GF(p^n)$ 的自同构群中的阶为 n。

---

12. 设 p 是一个素数。证明：对任何正整数 n，都存在一个在域 Z_p 上不可约的 n 次多项式。

证明　设 m 为小于 n 的正整数，则由本章 §5 第 5 题知任意 m 次不可约多项式均为 $x^{p^m-1}-1$ 的一个因式。记 $f_i(x)(i=1,2,\cdots,s)$ 为所有首项系数为 1 的 m 次不可约多项式(其中 $i \neq j, f_i(x) \neq f_j(x))(i,j=1,2,\cdots,$

s)。则它们两两互素，其乘积也为 $x^{p^n-1}-1$ 的因式，故

$$\sum_{i=1}^{s}\deg f_i(x)\leqslant p^n-1$$

又 $x^{p^n-1}-1$ 与其导数互素，故 $x^{p^n-1}-1$ 没有重因式，所以在其分解中，次数小于 n 的一切不可约因式的次数之和 s 至多为

$$(p-1)+(p^2-1)+\cdots+(p^{n-1}-1)$$

即为 $\dfrac{p^n-1}{p-1}-n$，又 $\dfrac{p^n-1}{p-1}-n<p^n-1$，于是

$$s<\deg(x^{p^n-1}-1)=p^n-1$$

而 $x^{p^n-1}-1$ 不存在次数大于 n 的不可约因式，故它必存在 n 次不可约因式，即域 Z_p 上必有 n 次不可约多项式。

---

13. 令 F 是一个有限域，Δ 是它所含的素域，且 $F=\Delta(\alpha)$。问：α 是否一定是乘群 F^* 的生成元？

解 α 未必是乘群 F^* 的生成元。

例如，F 是特征为 2 的有限域，且 $(F:\Delta)=4$，若 α 为 F^* 的生成元，即 $F^*=\langle\alpha\rangle$，则

$$F=\Delta(\alpha)=\{0,1,\alpha,\alpha^2,\cdots,\alpha^{14}\}$$

即 $F=\Delta(\alpha)$ 为 16 阶有限域。而

$$F^*=\langle\alpha\rangle=\{1,\alpha,\cdots,\alpha^{14}\}$$

为 15 阶循环群，故 α^3 不是 F^* 的生成元。又

$$4=(F:\Delta)=(F:\Delta(\alpha^3))(\Delta(\alpha^3):\Delta)$$

于是上式右端中 $(\Delta(\alpha^3):\Delta)=1,2$ 或 4。记 $t=(\Delta(\alpha^3):\Delta)$，

① 当 $t=1$ 时，则 $\alpha^3\in\Delta=\{0,1\}$，矛盾。

② 当 $t=2$ 时，则 α^3 为 Δ 上二次代数元，其最小多项式仅有两种形式，即 x^2+1 或 x^2+x+1。

若其最小多项式为 x^2+1，则 $(\alpha^3)^2+1=0$，即 $\alpha^{12}=1$，矛盾；

若其最小多项式为 x^2+x+1，则 $(\alpha^3)^2+\alpha^3+1=0$，故

$$\alpha^9-1=(\alpha^3-1)((\alpha^3)^2+\alpha^3+1)=0$$

即 $\alpha^9=1$，矛盾。

③ $t=4$ 时，则必有 $(F:\Delta(\alpha^3))=1$，即 $F=\Delta(\alpha^3)$。这与 α^3 不是 F^* 的

生成元矛盾。

14. 证明：任何有限域都有比它大的代数扩域。

证明 设 F 为任一有限域，由上述第 12 题知在 F 上存在 $n(n>1)$ 次不可约多项式，其在 F 上的分裂域就是比 F 大的代数扩域。

15. 设 α,β 分别是域 F 上的 m,n 次代数元。证明：

(1) $(F(\alpha,\beta):F)\leqslant mn$；

(2) 若 $(m,n)=1$，则 $(F(\alpha,\beta):F)=mn$。

证明 (1) 因为 β 是域 F 上的代数元，而 $F\subseteq F(\alpha)$，故 β 也是 $F(\alpha)$ 上的代数元，且

$$(F(\alpha)(\beta):F(\alpha))\leqslant(F(\beta):F)$$

从而有

$$\begin{aligned}(F(\alpha,\beta):F)&=(F(\alpha)(\beta):F(\alpha))(F(\alpha):F)\\&\leqslant(F(\beta):F)(F(\alpha):F)\\&=mn\end{aligned}$$

(2) 由

$$(F(\alpha,\beta):F)=(F(\alpha)(\beta):F(\alpha))(F(\alpha):F)$$

知 $(F(\alpha):F)\mid(F(\alpha,\beta):F)$，即 $m\mid(F(\alpha,\beta),F)$。同理有 $n\mid(F(\alpha,\beta):F)$。而 $(m,n)=1$，故

$$mn\mid(F(\alpha,\beta):F)$$

于是 $mn\leqslant(F(\alpha,\beta):F)$。又已证 $(F(\alpha,\beta):F)\leqslant mn$，于是必有

$$(F(\alpha,\beta):F)=mn$$