# 代数结构笔记 & 题解

Eastwind

# 目录

# 1 集合

这一章的朴素集合论主要是高中数学中集合部分的重述, 新加入的重要内容包括有序组与笛卡尔积的概念, 旨在为后续的数学讨论提供一套基本而常用的语言. 罗素悖论的存在已经指出, 朴素集合论有其不可避免的不自洽之处, 但在绝大多数具体的数学学习中, 我们并不会主动与如此抽象而病态的集合打交道, 自然也可以继续信任朴素集合论的可靠性. 尽管如此, 了解一些关于罗素悖论的内容依然有助于后续内容的学习, 也可以拓宽视野.

此外, 归纳定义为我们提供了 “以有限的语言定义无限的集合” 的手段, 为我们将来讨论无限的集合做了准备.

## 笔记

### 有序组

教材的定义 1.3 给出了判断两个有序组 $a$, $b$ 相等的充要条件: 首先, 这两个有序元组必须同样长, 即都是有序 $n$ 元组; 其次, 每个位置上的分量对应相等, 即 $\forall i \in \{1, 2, \ldots, n\}, a_i = b_i$.

有趣的是, 我们可以仅仅使用集合的语言来定义有限长的有序组. 首先让我们只考虑二元组的情况: 对于有序二元组 $(a, b)$, 我们可以将其定义为嵌套集合 $\{\{a\}, \{a, b\}\}$. 所谓 "可以如此定义" , 指的是这种对有序组的定义完美地符合我们对其性质的要求. 下面我们来验证这一点:

$a = c$ 且 $b = d$ 时, 显然 $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$, 即所谓 $(a, b) = (c, d)$. 所以我们只需证明必要性, 即 $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ 蕴含 $a = c$ 且 $b = d$:

假设现有两有序对 $(a, b) = (c, d)$, 根据 "定义", 即是有 $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. 根据集合相等的定义, 这意味着两集合互相包含, 即两集合中的任一元素都属于另一集合. 由此我们有 $\{a\} \in \{\{c\}, \{c, d\}\}$. 此时无非可能是两种情况: $\{a\} = \{c\}$ 或 $\{a\} = \{c, d\}$.

第二种情况更为基本, 所以我们首先讨论. 由于 $\{c, d\} = \{a\}$, 从而有 $\{c, d\} \subseteq \{a\}$, 也就有 $c \in \{a\}$ 和 $d \in \{a\}$. 此时只能是 $c = d = a$. 从而在等式 $(a, b) = (c, d)$ 中, 右端集合实际上就是 $\{\{c\}, \{c, c\}\} = \{\{c\}, \{c\}\} = \{\{c\}\}$. 与此同时我们还有 $\{a, b\} \in \{\{c\}\}$ 这个没有用上的条件, 从而可以推出 $\{a, b\} = \{c\}$, 也就有 $b \in \{c\}$, 从而只能有 $b = c$. 这就证明了 $a = b = c = d$, 自然蕴含 $a = c$ 且 $b = d$.

对于第一种情况, 我们可以得出 $a = c$. 再考虑 $\{a, b\} \in \{\{c\}, \{c, d\}\}$ 这个条件: 如果是 $\{a, b\} = \{c\}$, 则直接化归到上一种情况; 所以我们只考虑 $\{a, b\} \neq \{c\}$ 即 $b \neq c$. 此时只可能是 $\{a, b\} = \{c, d\}$, 从而有 $b \in \{c, d\}$. 但我们又确定了 $b \neq c$, 所以必然有 $b = d$. 这也证明了 $a = c$ 且 $b = d$.

综上所述, 我们证明了 $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ 蕴含 $a = c$ 且 $b = d$, 进而也就证明了两者等价. 这说明 $(a, b) = \{\{a\}, \{a, b\}\}$ 这种定义满足我们对

“有序二元组” 的一切需求.

最后我们再将情况推广到元组任意长 (但有限长) 的情况: 对于三元组 $(a, b, c)$, 我们可以将其定义为嵌套二元组 $((a, b), c)$. 类似上面的过程, 验证此种定义的合理性是很容易的: 根据我们上文的证明, $((a, b), c) = ((d, e), f)$ 蕴含 $(a, b) = (d, e)$ 且 $c = f$, 前者又蕴含 $a = d$ 且 $c = d$, 这就证明了按照我们的定义 $(a, b, c) = (d, e, f)$ 蕴含每个分量的元素对应相等. 反方向的蕴含推导则是平凡的. 以此类推, 对于任意自然数 $n$, 读者不难自己完成 $n$ 元组的集合定义及其合理性的证明 (使用数学归纳法) .

唯一需要注意的是无限长的有序组 $(a_1, a_2, a_3, \ldots)$. 此时使用二元组来递归地定义是不合适的, 因为递归的过程将是无限长的, 我们将永远无法得到想要的对象. 想要用集合形式化地定义集合 $A$ 上无限长的有序组, 一种可行的方法是将其定义成一个自然数到集合 $A$ 的映射 $f : N \to A$. 在后面的章节中我们会学到, 关系可以用集合形式化地定义为笛卡尔积的子集, 而 $n$ 元映射总可以定义为特殊的 $n + 1$ 元关系. 注意: 尽管笛卡尔积的定义中也用到了有序组, 但这里并没有构成循环定义, 因为定义一个如此的一元映射 $f$ 只需要二元关系, 而二元关系只用到二元有序组. 换言之, 在集合的基础上, 整个形式化的定义的提出顺序为:

集合 $\to$ 二元有序组 $\to$ 有限长的有序组 $\to$ 有限个集合的笛卡尔积 $\to$ 有限的多元关系 $\to$ 自变量数量有限的映射 $\to$ 无限长的有序组 $\to \ldots$

### (集合的) 笛卡尔积

根据有序对的定义所表达的最关键的内涵 “有序”, $(a, b) \neq (b, a)$. 所以, 如果现在有两个无重的非空集合 $A = \{a_1, a_2, \ldots\}, B = \{b_1, b_2, \ldots\}$, 则 $AB \neq BA$, 因为二元组 $(a, b)$ 属于 $AB$ 但不属于 $BA$. 但我们直观上会认为, 进行这种区分是不必要的. 如果将两个集合的笛卡尔积看做一个表, 我们显然应该关注表的结构, 而不会认为仅仅将这个表做一个横竖的转置就产生了什么根本的不同.

同样地, 如果将多个 (但有限个) 集合的笛卡尔积递归地定义为两个集合笛卡尔积的嵌套, 则也有 $(AB)C \neq A(BC)$, 因为 $((a, b), c)$ 属于 $(AB)C$ 但不属于 $A(BC)$. (如果你按照上面给出的形式化定义展开 $((a, b), c)$ 与 $(a, (b, c))$,

会发现它们是不同的集合.) 这使得我们无法写出 $ABC$ 这样的求积式, 因为求和顺序是不明确的. 更过分的是, 我们甚至不能写 $A^3$ 这样的集合幂, 在第四章中也就无法讨论三元以上的关系. 凡此种种都使得我们需要提出一种新的判定两个笛卡尔积 "相同" 的标准, 来规避这类繁文缛节.

我们注意到, 尽管从最原始的定义上看, $AB \neq BA$, 但映射 $f : AB \to BA, f((a,b)) = (b,a)$ 是一个自然的双射, 并且这种映射保持了原有的 "结构" , 原先处在表中同一列/同一行的元素映射后依然处在同一行/同一列. (严格来说, 集合是没有结构的, 但笛卡尔积这里的 "无序性" 显然与一般的集合有一些不同, 我们会认为这里有一些结构在里面) . 同样地, 在 $(AB)C$ 与 $A(BC)$ 之间, 存在着自然的双射 $f(((a,b),c)) = (a,(b,c))$. 如果这种保有结构的双射存在, 我们则称这两个结构**同构**. 在后面的学习中我们会马上看到, 同构和相等一样, 具有自反性 (任何结构都与自身同构) , 对称性 (如果 $A$ 与 $B$ 同构, 则 $B$ 也与 $A$ 同构) , 传递性 (如果 $A$ 与 $B$, $B$ 与 $C$ 分别同构, 则 $A$ 与 $C$ 也同构), 从而是一种等价关系, 可以被看作一种粗略的 "相等" .

在这种意义下, 我们可以粗略地认为, 集合的笛卡尔积运算满足所谓 "交换律" 与 "结合律" . 这使得我们可以将多个集合的笛卡尔积写成 $ABC$ 或 $A^4$ 这样的形式, 而不必标注出多次乘积的先后顺序. 能够这样做的一大好处在于我们可以在谈论多个集合的笛卡尔积时只关注参与运算的每个集合及其数量, 而不必在乎元素的顺序或乘法进行的顺序.

*p.s. 在此后以及其它数学课程的学习中我们会看到, 许多其它结构的笛卡尔积 (如关系的笛卡尔积, 群的笛卡尔积, 图的笛卡尔积, 拓扑空间的笛卡尔积) 也具有这样的特性: 如果我们不关注结构相乘时的顺序/从同构的角度来看待, 则笛卡尔积运算是满足交换律和结合律的. 这将为我们的讨论带来许多方便.*

## 题解

### 1.1

(1) 不相等. $4 \in B$ 但 $4 \notin A$, 从而 $B \not\subseteq A$.

(2) 相等. 证明如下:

从定义出发, 即需证明 $A \subseteq B$ 且 $B \subseteq A$. 逐一验证 $A$ 与 $B$ 中的每一个元素即可:

$A \subseteq B : 1 \in B, 2 \in B, 4 \in B$, 从而 $A \subseteq B$;

$B \subseteq A : 1 \in A, 2 \in A, 2 \in A, 4 \in A$, 从而 $B \subseteq A$.

故有 $A = B$, 证毕.

(3) 相等. 证法同上, 逐一验证即可.

*p.s.* 许多学生在看到这道题的 *(2)* 问时, 会联想到高中数学集合部分所强调的*:* 集合的元素具有互异性, 从而认为 $B$ 不是一个集合, 也就无法谈论相等与否. 但在绝大多数大学数学课程中, 我们默认不再要求集合的互异性, 这样可以带来一些简便.

例如, 在集合论中, 有序对 $\langle a, b\rangle$ 被完全用集合的方式定义为 $\{\{a\}, \{a, b\}\}$. 在学习了同构的知识后, 读者很容易检验这个定义的确能够表达我们所想要的语义, 即的确有 $\{\{a\}, \{a, b\}\} = \{\{c\}, \{d, d\}\}$ 当且仅当 $a = c$ 且 $b = d$. 此时, 如果还要求集合中元素的互异性, 就必须对 $a = b$ 的情况单独讨论, 从而造成叙述上不必要的麻烦.

当然, 更新了定义, 就必须要检验基于原定义的概念和结论是否能够得到保持. 此时, 由于集合添加任意多已有的元素后依然被视为同一个集合, "势"的定义应由 "集合的元素个数" 改为 "集合中不同元素的个数"; 在这种定义下, 关于幂集元素个数的公式也能得到保持. 对于一些其它的结论 *(*例如关于笛卡尔积元素个数的公式*)*, 读者不妨自行选取几个验证.

*p.p.s.* 在上一条评注中, 我们引入了另一种看待无重集合的观点*:* 承认有重复元素的集合, 但认为同一元素的出现次数不影响集合的性质, 从而两个集合如果出现的元素相同而只是有些元素的出现次数不同, 依然被看作同一个

集合. 并且我们说明了这种观点与原观点 (不承认有重集合) 是等价的. 但即便如此我们仍要问: 为什么要平白无故引入一种相同的理解方式? 如果它与原先的理解方式完全等价, 岂不是完全没有用途吗?

原因在于, 当我们不忽视元素的出现次数, 即认为集合不仅由其中出现的元素种类也由其次数决定, 由此得到的结构 (多重集) 在数学的某些分支中同样有重要的用途. 例如, 在线性代数中, 当我们计算多项式方阵的 Smith 标准型时, 相同的初等因子的出现次数是重要的; 当我们讨论方阵的所有特征值全体时, 同一个特征值的出现次数是重要的; 在图论中, 有时我们需要考虑有重边的图, 那么在边集中, 同一表示的边的出现次数是重要的.

在这种视角下, 我们不妨认为多重集才是最一般的表达方式, 而有意忽视了相同元素的重数的 "集合", 反倒是多重集对 "含有的元素种类相同" 这一等价关系作商得到的概念.

这里提到的 "等价关系" "作商" 等概念, 我们会在第四章的学习中接触.

### 1.2

从定义出发, 即需证明 $A \subseteq C$ 以及 $A \neq C$.

由 $A \subseteq B$, 我们知道 $\forall x \in A$, 有 $x \in B$ 成立; 又由 $B \subset C$, 同样有 $\forall x \in B$, 有 $x \in C$ 成立. 因此, 任取 $x \in A$, 则 $x$ 满足 $x \in B$, 也就满足 $x \in C$. 这就证明了 $A \subseteq C$.

由 $B \subset C$, 我们还知道必然 $\exists y \in C$, 有 $y \notin B$ 成立. 假设 $y \in A$, 则其可以推出 $y \in B$, 矛盾. 从而同时有 $y \notin A$ 与 $y \in C$ 成立, 这就决定了 $C \not\subseteq A$, 自然也就有 $A \neq C$.

### 1.3

(1) 不成立. $0 \in \{0\}$ 但 $0 \notin \emptyset$.

(2) 不成立. 0 不是一个集合.

显然, 这里不需要我们采纳公理集合论的观点.

(3) 不成立. $\emptyset \in \{\emptyset\}$ 但 $\emptyset \notin \emptyset$.

(4) 成立. 左侧包含于右侧必然; 由于不存在任何 $x$ 满足 $x \neq x$, 所以右侧包含于左侧.

不过, 从稍微严谨一点的集合论的角度讲, 这里式子右侧的集合不是良好定义的. 因为它没有指明 $x$ 应该从怎样的对象出发作为基底考虑, 也就无法究其性质.

(5) 不成立. 容易证明, 无论集合 $A$ 为何, 满足如此条件的集合 $B$ 都只能是空集, 所以右侧实际上就是集合 $\{\emptyset\}$. 这与 (3) 的情况是完全一样的.

(6) 不成立. 容易证明, 空集的唯一子集是空集, 所以左式实际上也就是 $\{\emptyset\}$, 这又与 (3) 完全一样.

### 1.4

(1) $\times$. 任取 $A = C \neq B$ 即可构造出反例, 例如 $A = \emptyset, B = \{0\}, C = \emptyset$.

(2) $\surd$. 反证法: 若 $a \in B$, 则由 $B \subseteq A$, 即有 $\forall x \in B, x \in A$. 这就意味着 $a \in A$, 矛盾.

(3) $\surd$.

这里我们假定 $|\mathscr{P}(A)|$ 的写法默认了 $\mathscr{P}(A)$ 是有限集. 如果约定对于任意无限集 $X$, 规定 $|X|$ 大于任一自然数, 不影响本题的结论.

由于 $|\mathscr{P}(A)| = 2^{|A|} > 1$, 可知 $|A| > 0$. 而 $\emptyset$ 恰有 0 个元素, 所以必定有 $A \neq \emptyset$.

### 1.5

(1)

$$\begin{aligned} A \cap (\overline{A} \cup B) &= (A \cap \overline{A}) \cup (A \cap B) \\ &= \emptyset \cup (A \cap B) \\ &= A \cap B \end{aligned}$$

(2)

$A \cap B \subseteq A$, 从而有 $A \cup (A \cap B) = A$.

(3)

命 $B_i = \overline{A_i}$, 则第一个式子可化为 $\overline{\bigcap\limits_i \overline{B_i}} = \bigcup\limits_i B_i$. 对其两端取补集, 则得到 $\bigcap\limits_i \overline{B_i} = \overline{\bigcup\limits_i B_i}$. 这实际上就是第二个式子.

所以我们只需证明前者.

实际上, 用类似的方法也容易证明第二个命题蕴含第一个, 从而两个命题是等价的.

对 $n$ 用数学归纳法证明:

① $n = 2$:

设 $A_1, A_2$ 共同的万有集合为 $U$, 则 $\overline{A_1} = U - A_1, \overline{A_2} = U - A_2$.

从而, $\forall x \in U$, $x \in A_1 \cap A_2$ 成立当且仅当 $x \in A_1$ 且 $x \in A_2$. 换言之, $x \in \overline{A_1 \cap A_2}$ 即 $x \notin A_1 \cap A_2$ 当且仅当 $x \in \overline{A_1}$ 或 $x \in \overline{A_2}$. 这也就是 $x \in \overline{A_1} \cup \overline{A_2}$.

从而我们证明了 $\overline{A_1 \cap A_2} = \overline{A_1} \cup \overline{A_2}$.

② 若 $n \leq k$ 时结论成立, 即已有 $\overline{\bigcap\limits_{i=1}^{k} A_i} = \bigcup\limits_{i=1}^{k} \overline{A_i}$. 则 $n = k + 1$ 时:

设 $\bigcap\limits_{i=1}^{k} A_i = A'$, 则左端 $= \overline{A' \cap A_{k+1}}$. 在 $n = 2$ 的情况中我们已经证明了 $\overline{A' \cap A_{k+1}} = \overline{A'} \cup \overline{A_{k+1}}$. 又 $\overline{A'} = \bigcup\limits_{i=1}^{k} \overline{A_i}$, 也就是左端 $= (\bigcup\limits_{i=1}^{k} \overline{A_i}) \cup \overline{A_{k+1}} =$ 右端.

此即所谓“德摩根定律”, 在处理补集的表示时会带来许多方便.

**1.6**

(1)

$\forall x \in A \cap B$, 有 $x \in A$ 与 $x \in B$ 均成立. 而根据 $B \subseteq C$, $x \in B$ 可以推出 $x \in C$. 从而同时有 $x \in A$ 与 $x \in C$, 也就是 $x \in A \cap C$.

(2)

$\forall x \in A \cup B$, $x \in A$ 与 $x \in B$ 中有至少一者成立. 无论成立的是哪一条, 都蕴含 $x \in C$.

(3)

设 $A \cap B = C$, 则有 $A = (A - C) \cup C, B = (B - C) \cup C$.

$A \cup B = (A - C) \cup (B - C) \cup C$. 由于这三个集合两两不交 (需要验证的只有 $A - C$ 和 $B - C$, 但它们如果有共同元素则与 $C$ 的定义矛盾) , 可以写出 $|A \cup B| = |A - C| + |B - C| + |C|$. 而 $|A| + |B| = |A - C| + |B - C| + 2|C|$, 由此不等关系与取等条件显然.

**1.7**

(1)

定义数字集合 $Digit = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. 由此我们来定义十进制无符号整数集合 $N$:

① 如果 $a \in Digit$, 则 $a \in N$;
② 如果 $a \in Digit$ 且 $b \in N$, 则将数字 $a$ 拼接在 $b$ 前面得到的字符串 $\overline{ab} \in N$;
③ $N$ 中的元素只包括有限次使用①②得到的那些.

注意在这道题里像下面这样使用整数加法来定义是不合适的:

① $0 \in N$;
② 如果 $a \in N$, 则 $a+1 \in N$.
③ $N$ 中的元素只包括有限次使用①②得到的那些.

原因在于: 在逻辑上, "整数加法" 必须在 "整数" 之后定义. 如果还没有说清楚什么是整数, 自然无从谈论 "某两个整数相加的结果是哪个整数", 所以当然也就不能用加法来定义整数.

(当然, 在现代数学中, 整数并非是通过它的十进制表示来定义的, 而是使用皮亚诺公理定义了一个与我们所习惯的整数结构同构的结构. 只不过在小学阶段的学习中, 为了便于学生接受, 我们暂且采用了这样的定义方式. )

请注意此题的情况与教材中关于 "非负偶数集" 一例的不同: 偶数当然是需要在有了整数之后定义的, 并且也必须在有有了加法或乘法后定义, 否则便无法描述这个集合的内涵 (你不能列举出有限的元素 $2, 4, 6, 8, ...$ 然后让你的读者找规律) . 因此在这个例子里使用加法来定义是可取且必需的.

(2)

下面我们假定这道题不允许使用 . 来表示有限小数 0.0, 因为允许这种表示的答案更加简单.

定义集合 $Digit = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. 由此我们来定义无符号有限小数集合 $L$:

① $0., 1., 2., 3., 4., 5., 6., 7., 8., 9. \in L$;
② 如果 $a \in Digit$ 且 $b \in L$, 则将数字 $a$ 拼接在 $b$ 前面或后面得到的字符串 $\overline{ab}$ 与 $\overline{ba}$ 均 $\in L$;
③ $L$ 中的元素只包括有限次使用①②得到的那些.

(3)

我们给出两种方法, 分别用整数加法与二进制表示来定义二进制偶整数 $E$:

法一, 使用整数加法:

① $0 \in E$;
② 如果 $a \in E$, 则 $a+2 \in E$;
③ $E$ 中的元素只包括有限次使用①②得到的那些.

法二, 根据二进制表示:

这样定义的难点在于, 如何在不添加语句的情况下既绕开 0 开头的整数又把特例 0 包含进来. 以下展示了一种巧妙的处理方法.

① $0, 10 \in E$;
② 如果 $a \in E$, 则在 $a$ 中取两个相邻的数字, 向其中插入数字 0 或 1 得到 $a'$, 则 $a' \in E$;
③ $E$ 中的元素只包括有限次使用①②得到的那些.

## 拓展

### 罗素悖论

学朴素集合论不学罗素悖论, 就如同上科大不上大物实验, 是沉湎于凡庸与显然之中, 而错过了真正的洞见与精彩的行径. 尽管罗素悖论与这门课要求的范围关联不大, 但由于它令人拍案叫绝的巧思, 以及在数理逻辑中无法回避的重要地位, 我还是倾向于在这本笔记里加入一些介绍性的内容, 供有兴趣的读者自选阅读.

为了不一上来就让读者陷入令人绝望的抽象, 我们先从一个具体的例子看起:

在先前的讨论中, 我们已经习惯了朴素集合论中以集合为元素的集合 "集合集" 的存在. 这使得我们可以将一些具有同一特征的集合抽取出来, 放进一个集合里. 例如, 我可以定义 "全体无穷集构成的集合" $A = \{\text{ 集合 } X | X \text{ 为无穷集 }\}$. 这个集合中有一些我们所熟知的元素, 例如自然数集 $\mathbb{N}$, 整数集 $\mathbb{Z}$, 有理数集 $\mathbb{Q}$, 实数集 $\mathbb{R}$, 以及对它们稍作调整 (如加入或删去有限多个元素) 得到的集合; 也有一些集合不在 $A$ 中, 例如空集, 以及每个自然数 $n$ 单个所形成的一元集 $\{n\}$, 等等.

现在考虑一个问题, $A$ 是否在 $A$ 中, 即是否有 $A \in A$? (注意我们问的不是 $A \subseteq A$? 这是一个所有集合都具备的平凡性质.) 根据 $A$ 的定义, 这实际上是在问: $A$ 是否是无穷集? 再次根据 $A$ 的定义, 这实际上又是在问: 是否存在无穷多个无穷集?

直观上答案是肯定的, 因为我们可以列举出许多无穷集, 例如上文提到的 $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \ldots$ 但如此列举并不能构成一个证明, 因为我们需要无限地列举下去, 但证明必须是有限的. 想要证明这一点, 我们必须一次性给出无穷多个集合, 且保证每一个都是无穷集. 考虑到无穷集删去一个元素后仍是无穷集, 我们可以考虑所有与自然数集 "差不多" 的集合 $\mathbb{N}_n = \mathbb{N} \backslash \{n\} = \{0, 1, \ldots, n-1, n+1, \ldots\}$: 显然这些集合每一个都是无穷集, 而这无穷多个表示对应的集合两两不同 (严格地证明这一点只需要根据一个有差异的元素证明一个方向上的不包含) . 这就给出了无穷多个不同的无穷集, 也就证明 $A \in A$.

在所有的集合集中, 具有 “自属于” 这一特征的集合还有很多. 例如, 在我们在第四章学到不可列无穷的概念后, 读者可以仿照上文轻易验证 “全体不可列无穷集构成的集合” $B = \{$ 集合 $X|X$ 是不可列无穷集 $\}$ 也是一个自属于的集合, 因为 $\mathbb{R}_x = \mathbb{R}\backslash\{x\}$ 给出了不可列无穷多个不可列集合. 相应地, “全体有限集构成的集合” $C = \{$ 集合 $X|X$ 是有限集 $\}$ 则不属于自身, 因为对于每个自然数 $n$, 一元集 $\{n\}$ 都是有限集, 这就证明了存在无穷多个有穷集.

由此我们得到了另一个划分集合的标准: 是否属于自身. 一个平凡的推论是, 非集合集当然不属于自身, 集合集则需要根据定义具体分析. 此时我们很容易想到定义 “全体自属于的集合构成的集合” $P = \{X|X \in X\}$. 自然要考虑一个问题: 是否有 $P \in P$? 根据 $P$ 的定义, 这实际上就是在问: $P$ 是否是自属于的集合, 即是否有 $P \in P$?

好吧, 看起来单纯的根据定义翻译并不能帮我们判断 $P \in P$ 是否成立, 我们面对的问题变成了一个逻辑推理般的谜题. 分情况讨论, 如果 $P \in P$, 则 $P$ 是自属于的集合, 根据 $P$ 的定义有 $P \in P$ 成立, 不矛盾; 如果 $P \notin P$, 则 $P$ 是自不属于的集合, 也有 $P \notin P$, 同样不矛盾. 看上去无论采取哪种处理都是可以的, 我们既可以规定 $P \in P$, 也可以规定 $P \notin P$. 又或者, 这里实际上存在着两个集合, 分别对应着自属于和自不属于的情况.

然而这种纯理论般的讨论马上就将无法继续下去了, 让我们考虑 $P$ 以 “全体集合” 为母集的补集 $Q = \{X|X \notin X\}$. 由于 $Q$ 是集合, 它必将属于 $P$ 与 $Q$ 中的一个. 试问: 是否有 $Q \in Q$? 如果这一点成立, 则 $Q$ 是自属于的, 从而应该有 $Q \in P$ 即 $Q \notin Q$, 矛盾. 由此我们得知 $Q \notin Q$, 此时又有推论 $Q$ 是自不属于的, 从而有 $Q \notin P$ 即 $Q \in Q$, 同样矛盾.

### 外延原理, 内涵原理与归纳定义

罗素悖论的构思是精彩的, 但这似乎只是一个类似 “万能的上帝能否造出一块自己举不起的石头” 般的逻辑游戏, 并不足以使人生惧或惶恐. 然而读者如果熟悉数学中反证法的使用, 便会知道如果能够导出矛盾, 就说明我们采取的某个假设是错误的, 从而可以证伪一个命题. 例如, 上帝举石悖论的构造, 正是为了对教义中 “万能上帝的存在性” 这一假设发起的攻击. 而在罗素悖论中, 我们似乎并未用到任何暂且不能肯定为真的假设, 整个过程中用

到的无非是 “根据一个确定的性质的有无可以定义一个集合” 这一朴素集合论中最基本的观点 (这似乎甚至不能被称为一个命题, 而仅仅是一种显然的看法) . 然而, 上文已经向我们展现过, 只要我们采纳这种看法, 悖论就会自然出现.

此时, 读者或许会想到采用一些人为性的修正, 在保住集合论的主体部分的同时, 规避掉这类形而上学的逻辑游戏带来的无聊矛盾. 常见的朴素修正方法有: 禁止以集合作为集合中的元素, 或者单纯只是禁止定义定义上文中的集合 $P$ 与 $Q$. 然而这类修正大多不令人满意. 如上的两个修正中, 前者带来的代价是不可接受的 (在后面章节的学习中我们马上会看到, 集合集是多么方便的讨论工具) ; 后者则完全不解决问题: 我可以定义集合 $P' = \{X | X \in X \text{ 且 } |X| \text{ 为不可列无穷 }\}$ 等一系列大同小异的集合来重现悖论.

那么, 我们是否要认为, “给定一个性质可以根据其有无定义一个集合” 这一观点就是不可接受的呢? 假如果真如此认为, 则朴素集合论中大多常用的语言都将不复存在, 基于此的具体数学中得到的结果也必须重新推导, 这同样是难以接受的. 对此, 大部分数学的态度是无视罗素悖论, 毕竟不涉及如此抽象的集合也不妨碍许多数学的蓬勃发展; 而一些涉及同样抽象的集合讨论的数学 (例如实分析, 代数几何, 无限图论) , 则催生了后来的上位 (?) 替代, 公理集合论. 对于本段开头的问题, 朴素集合论无法作出回答, 而其公理集合论对此的回答便是肯定的: 一个 “性质” 未必对应着一个集合, 所有集合的存在性都必须由有限的若干条公理按照相同的模式推导出. 也正因如此, 公理集合论中的集合, 不含有任何具体的元素 (例如 “科大 2023 级的计算机系本科生”) , 而将一切数学对象 (例如自然数) 都表示为空集或其上的嵌套.

深入讨论公理集合论已经远远超出了这本笔记主题的定位, 让我们把目光聚回到罗素悖论对朴素集合论的打击上. 在这一章的笔记部分中, 我们一直在与读者讨论, 仅仅使用集合如何定义出具体数学中需要的许多概念, 如有序组, 关系与映射. 现在读者大概可以理解, 我们之所以如此追求形式化, 便是为了规避罗素悖论这种 “仅从定义出发导出的矛盾” 出现. 例如, 用集合形式化地定义有序组的动机之一, 便是出于 “如果集合的定义没有问题, 那么如此定义有序组也不会有问题” 的信念. 然而, 这些形式化的工作都无法掩盖一个问题: 在朴素集合论中, 唯有 “集合” 本身尚未形式化地定义 (这也正

是公理集合论所作出的关键变革) . (在意识到罗素悖论的存在之前,) 我们之所以还可以无歧义地讨论集合, 是基于以下两条不言自明的观念:

外延原理: 恰好指明了一个集合中含有的所有元素, 则定义了这个集合.

内涵原理: 给定一个性质, 则满足这个性质的元素可以定义成一个集合.

了解过一些哲学的读者不难联想到 “外延” 与 “内涵” 的词义: 所谓外延, 即是一个集合所包含的所有对象构成的整体; 所谓内涵, 则是划定出这一集合所根据的关键性质. 例如, “2024 春季学期修读了代数结构课程的科大本科生” 是一个内涵, 其所对应的外延则是把所有修了这门课的学生列举出来. 而上述外延/内涵原理便是说: 给出一个集合的外延/内涵, 都可以定义出这个集合.

外延原理的可靠性是无需质疑的, 有集合相等的定义为其背书 (或者不如说, 外延原理本身就是 “所含元素完全相同的集合相等” 的同义) . 出问题的关键在于内涵原理: 罗素悖论的提出, 使得我们不能任意地使用内涵原理来定义集合. 对于具体的数学如数学分析/抽象代数, 即使无视罗素悖论, 也不得不正视这一点, 尽可能规避内涵原理的滥用. 一个自然的想法是: 我们或许可以只使用外延原理来定义集合. 即, 当我们要定义一个集合时, 总是指明这个集合所含有的每个元素.

想要指明一个集合恰好含有的每个元素, 最直观的做法无疑是将其元素逐一列举出来. 这样做的局限也很明显: 对于无限集合, 这甚至理论上就是做不到的, 因此我们需要别的办法来 “指明一个无穷集中的全部元素” . 考虑在过去的学习中我们新接触到的无限集: 在初中关于有理数的学习中, 我们根据 $\mathbb{Q} = \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$ 来定义了无穷集 $\mathbb{Q}$. 但这种做法依旧不能完全解决问题: 定义有理数集 $\mathbb{Q}$ 时所用到的整数集 $\mathbb{Z}$, 同样是一个无穷集, 也需要可靠的定义. 类似地, 用自然数 $\mathbb{N}$ 定义整数 $\mathbb{Z}$ (加法群) , 用有理数 $\mathbb{Q}$ 定义实数 $\mathbb{R}$ (Cauchy 完备化) , 用实数 $\mathbb{R}$ 定义复数 $\mathbb{C}$ (域扩张) , 都是 “无穷集定义无穷集” 的例子. 我们亟需一种方法, 能够基于一个已知的有限集合, 无歧义地定义出一个无限集合, 无论过程多么冗长, 繁琐或刻意. 此时应运而生的, 便是教材第一章末尾所介绍的归纳定义.

**罗素悖论相关：停机问题**

教材关于集合的举例中第 4 例涉及了停机问题, 但只是以一种不知所云的口吻陈述了这个集合的不可判定性. 由于其与罗素悖论的相关性, 这里我们介绍一下停机问题. 以下内容尽量不涉及递归论或可计算性理论的专业知识, 仅使用科大大一通修的 C 语言来陈述情境.

我们约定用语: 一次运行 = 一个程序 + 一个输入. 在运行一个 C 语言程序时, 程序便是你写出的代码编译出的 exe 文件, 输入则是你在终端填入的字符串 (没有输入自然也可以视为一种输入) . 我们也知道, 某些程序在得到某些输入后会进入一个死循环 (例如一个 “重复 +1 直到变量为 0” 的函数和输入 “1” ) . 现在假想你是一个在做 C 语言上机作业的学生, 对于 oj 上的一道题, 你写出了一个自认为完全正确的程序, 并输入了助教给出的第一个样例输入, 但 exe 程序却运行了 1 分钟也没有给出输入. 现在, 你知道自己无非处于以下两种情况之一:

*a. 你的代码正确但只是时间复杂度过高, 或者你的代码错误, 但总之这次运行会在一段时间之后输出一个结果, 好让你知道自己的代码是个什么状况;*

*b. 你的程序陷入了死循环;*

为了继续调整你的代码, 你打算再等上一段时间, 以便得到一个输出. 但由于第二种情况存在的可能, 你知道自己不能无期限地等下去. 看着, 聪明的你开始考虑为了避免眼下的这种困境, 是否能写出一个函数 $f(function, input)$, 它总能够**在有限的时间内**能够判断一个程序 $function$ 在得到一个输入 $input$ 后是否会陷入死循环. 这样每当你测试的时候, 就可以先用函数 $f$ 测试一次你的代码是否有大的错误, 而不必折磨你的计算机来发现这一点. 形式化一点的说, 我们现在考虑的是这样一个字符串变量的二元函数 $f(p, q)$: 如果以字符串 $p$ 为 C 语言代码, 编译得到 exe 程序, 以字符串 $q$ 为输入, 由此得到的运行不会陷入死循环, 则 $f(p, q) = 1$; 否则 $f(p, q) = 0$. 为了后续的讨论简便, 我们称输入 $q$ 不会使程序 $p$ 进入死循环为 “$p$ 对 $q$ 停机”

你发现你的计算机的风扇已经开始在响了, 于是你关掉了 exe 程序, 开始继续思考你的构想. 如果这样的函数 $f$ 存在, 则我们可以规约到它写出另一个一元字符串函数 $f'(p)$. 它的功能是, 如果 $f(p, p) = 0$ 即 $p$ 对自身停机, 则进入死循环 (例如开始运行上文给出的死循环代码) ; 否则如果 $p$ 对自身不停

机, 则 $f'(p)$ 输出 0. 具体的伪代码为:

```
int f'(char[] p)
{
  int i=1;
  if(f(p,p)==1)
  {
    while(true) i++;
  }
  else return 0;
}
```

事情直到这一步都还安好. 但是, 让我们考虑运行 $f'(f')$. 根据 $f'$ 的内容, $f$ 可以在有限时间内判断 $f'$ 是否对自身停机. 如果 $f'$ 对自身停机, 则 $f(f', f') = 0$, 这里的 $f'$ 陷入死循环, 说明 $f'$ 对自身不停机, 矛盾; 如果 $f'$ 对自身不停机, 则 $f(f', f') = 1$, 这里的 $f'$ 在有限时间内结束并输入 0, 说明 $f'$ 对自身停机, 同样矛盾. 由此我们证明了, 一个能够判断任意程序对任意输入是否停机的函数是理论上就不存在的.

读者不难发现, 尽管停机问题不可判定的证明过程中没有直接用到罗素悖论, 但其中矛盾的构造方式却与罗素悖论十分相似. 此即数理逻辑中有名的“对角线方法”, 许多经典定理的证明都直接或间接地与之有关. 在第四章的学习中, 我们将在“任意无穷集合与其幂集不等势”这一定理的证明中再次见到它的身影.

# 2 数论初步

## 笔记

### 线性同余方程的解法

我们来考虑任意线性同余方程 $ax \equiv b(\mathrm{mod}c)$ 的解法. 所谓解决线性同余方程的求解问题, 指的是恰好指出整数集中这个方程的所有解, 并证明之.

在开始求解之前, 让我们先明确一个同余方程的含义. 根据 $\mathrm{mod}n$ 同余关系的定义, 上述方程实际上等价于一个特称命题 $\exists k \in Z\ s.t.\ ax = kc + b$. 理解这一点能够帮我们规避许多初学者容易犯的错误, 例如 *.

然后让我们来开始考虑求解的问题. 首先可以想到的是, 并非所有线性同余方程都是有解的. 考虑 $2x \equiv 1(\mathrm{mod}6)$, 这个方程显然无解, 因为与之对应的等式中左式为偶数, 而右式具有 $6k + 1$ 的形式, 必然为奇数, 两端不可能相等. 可以注意到, 这种无解情况的根源在于 $a$ 和 $c$ 有一个公因子 $m$, 而 $b$ 没有这个因子, 从而等势两端关于 $m$ 所属的同余类必然不相同. 这启发我们一点: $a, b, c$ 中有两者有公因子的情况或许是简单的, 可以直接判断无解或规约到三者互素的情况. 下面我们从这个角度入手考虑:

① $a, b, c$ 三者有非平凡公因子, 即 $(a, b, c) = m > 1$

不妨设 $a = ma', b = mb', c = mc'$, 则对应的特称命题可以写成 $\exists k \in Z\ s.t.\ ma'x = mkc' + mb'$, 而这里的等式等价于 $a'x = kc' + mb'$. 所谓等价, 指的是满足第一个等式的 $k$ 必然也满足第二个等式, 反之亦然. 由此我们得到:

*如果 $a, b, c$ 有非平凡的公因子 $m$, 则 $ax \equiv b(\mathrm{mod}c)$ 的解集等于 $\frac{a}{m}x \equiv \frac{b}{m}(\mathrm{mod}\frac{c}{m})$ 的解集.*

至此我们将所有情况都划归到了三者最大公因子为 1 的情况.

② $a, b$ 有非平凡公因子, 即 $(a, b) = m > 1$

由于我们已经划归了三者有公因子的情况, 这里可以假定 $c$ 没有相同的因

子, 即有 $(c,m)=1$

同样设 $a=ma',b=mb'$, 则对应等式化为 $ma'x=kc+mb'$. 由于左式有因子 $m$, 右式中的 $kc$ 一项也必须有因子 $m$, 但又有 $(c,m)=1$, $c$ 不对 $m$ 的整除性有任何贡献, 所以必然有 $m|k$. 设 $k=mk'$, 则原等式等价于 $a'x=k'c+b'$, 而这里 $x$ 没有发生任何变化, 从而方程的解集也没有任何变化, 有变化的只是特称命题中使等式成立的 $k$ 的情况. 由此我们得到:

如果 $a,b$ 有非平凡的公因子 $m$, 而 $c$ 没有这个因子, 则 $ax\equiv b(\mathrm{mod}c)$ 的解集等于 $\frac{a}{m}x\equiv\frac{b}{m}(\mathrm{mod}c)$ 的解集.

③ $b,c$ 有非平凡公因子, 即 $(b,c)=m>1$

同样假定 $(a,m)=1$, 并设 $b=mb',c=mc'$, 则对应等式化为 $ax=mkc'+mb'$. 同上理, 必须有 $m|ax$ 从而 $m|x$. 设 $x=mx'$, 则等式等价于 $ax'=kc'+b'$. 这里 $x$ 发生了变化, 因此我们在求出新方程的解集后, 必须通过变换来得到原方程的解集. 换言之, 我们得到:

如果 $b,c$ 有非平凡的公因子 $m$, 而 $a$ 没有这个因子. 设 $ax\equiv\frac{b}{m}(\mathrm{mod}\frac{c}{m})$ 的解集为 $X\subseteq\mathbb{Z}$, 则原方程的解集为其数乘 $mX=\{mx|x\in X\}$.

④ $a,c$ 有非平凡公因子, 即 $(a,c)=m>1$

同样假定 $(b,m)=1$, 并设 $a=ma',c=mc'$, 则对应等式化为 $ma'x=mkc'+b$. 由于 $b$ 没有因子 $m$, 因此左式被 $m$ 整除而右式则不然, 两侧不可能相等, 即原方程无解. 由此我们得到

如果 $a,c$ 有非平凡的公因子 $m$, 而 $b$ 没有这个因子, 则方程 $ax\equiv b(\mathrm{mod}c)$ 无解.

至此我们也划归了所有 $a,b,c$ 中任意两者不互素的情况. 下面我们只需关注 $a,b,c$ 两两互素的情况, 解决了这种情况就解决了整个线性同余方程的求解问题.

⑤ $a,b,c$ 两两互素

此时等式 $ax=ck+b$ 已经无法简化. 为了求解 $x$, 我们需要确定所有的满足 $a|ck+b$ 的整数 $k$, 与之对应的整数 $\frac{ck+b}{a}$ 便是原方程的解. 然而, 找出这

样的 $k$ 本身就意味着解一个线性同余方程 $ck \equiv -b(\mathrm{mod}a)$, 这里 $a, b, c$ 同样是两两互素的, 回到了我们目前考虑的问题本身.

这说明我们或许无法给出一个直接求解的计算方法, 而必须逐个尝试所有的整数 $k$. 然而整数集是无限集, 在有限的时间内尝试每一个元素是不可能的. 此时我们可以想到, 在这里关键的仅仅是 $k$ 所属的 $\mathrm{mod}a$ 同余类, 因此只需尝试 $a$ 的完系中的每个同余类 $\overline{0}, \overline{1}, \ldots, \overline{a-1}$ 的代表元各一个即可, 而最简便的便是 $0, 1, \ldots, a-1$. 如果一个整数 $k_0$ 是 $k$ 的解, 那么所有形如 $k_0 + al(l \in \mathbb{Z})$ 的整数都是解, 反之亦然. 这就使得我们可以通过 $a$ 次尝试确定所有 (无穷个) 符合要求的 $k$, 并代回解出对应的 $x$. 当然, 你也可以更直接一些, 直接将 $c$ 的每个同余类的代表元代入 $x$ 来求解.

至此我们给出了一个求解同余线性方程的算法. 除此之外, 我们还可以得到一个十分重要的结果:

*如果 $a, c$ 互素, 则方程 $ax \equiv b(\mathrm{mod}c)$ 的解在 $\mathrm{mod}c$ 同余的意义下唯一.*

下面我们来证明这一点. 我们已经知道, 如果整数 $x$ 是原方程的解, 则 $x$ 所在的同余类中的所有元素都是解. 这确保了我们可以将每个同余类看作一个整体. 上述定理则说明了, $(a, c) = 1$ 时, 解恰好只有一个同余类.

我们采用反证法来证明这一点: 假定存在两个同余类都是原方程的解, 则在 $\mathrm{mod}c$ 的完系 $\{0, 1, \ldots, c-1\}$ 中可以找到两个不同的整数 $x_1, x_2$ 满足原方程, 即有:

$$\begin{cases} x_1 \equiv b(\mathrm{mod}c) \\ x_2 \equiv b(\mathrm{mod}c) \end{cases}$$

使用前文提到的特称命题的观点, 这意味着分别存在整数 $k_1, k_2$, 使得 $x_1 = k_1c + b, x_1 = k_2c + b$ 同时成立. 于是就有 $x_1 - x_2 = (k_1 - k_2)c$, 从而有 $c|x_1 - x_2$. 然而, $0 \leq x_1, x_2 < c$, 这意味着两者之差绝对值小于 $c$, 但又不可能是 0, 从而不可能被 $c$ 整除. 由此导出矛盾.

根据上文情况①与③的讨论, 我们还可以得出一个自然的推论:

*如果 $a, c$ 不互素, 即 $(a, c) = m > 1$, 则方程 $ax \equiv b(\mathrm{mod}c)$ 要么无解, 要么解在 $\mathrm{mod}c$ 同余的意义下不唯一.*

如果 $m|b$, 则解不唯一;

如果 $m \not| b$, 则无解.

至此我们不仅给出了判断解的存在情况的充要条件, 也给出了有解情况下求出解的算法, 可以说完全地解决了线性同余方程求解的问题.

*p.s.* 回顾我们求解的整个过程, 我们所做的无非是在尝试最基本的情况时探索出一些我们想要的 "好" 的性质, 将不满足此种性质的 "不好" 的情况的求解划归到 "好" 的情况, 然后只关注 "好" 的情况, 此后不断重复这种划归. 当情况无法再理想化的时候, 我们便考虑是否可以直接求解, 如果意识到不存在直接给出解的算法, 便承认必须回到机械的尝试.

*p.p.s.* 如果仅仅关注解的存在与分布, 上述过程中情况②与③的讨论似乎是不必要的, 仅根据④也能将我们带向同余方程的求解. 然而, 在研究一个问题的初期, 指望直接发现最有价值, 最快通向答案的方向是不现实的, 适当做一些简单的划归则是一个不错的选择. 尽管这两种情况的讨论不是必要的, 但在最后尝试得出所有解时, 它们给出的结论依然能够为我们提供许多便利.

### 线性同余方程组的解法

解决了线性同余方程的问题, 随之而来的自然是线性同余方程组. 所谓方程组的求解, 便是对每个方程的解集取交集, 得到满足所有方程的 $x$ 构成的集合. 尽管如此, 我们还是不能就此认为只要写一句 "取交集" 就给出了解, 至少在现阶段应该追求将解写为 $x \equiv m(\mathrm{mod} n)$ 的简单形式.

由于线性同余方程的求解问题已经解决, 所以下面我们可以默认方程组中的方程都具有 $x \equiv b_i(\mathrm{mod} c_i)$ 的形式. 假如我们已经可以解出两个线性同余方程构成的方程组, 则对于一个由 $n$ 个方程构成的线性同余方程组, 我们可以先解出前两个方程, 并以其解为一个新的方程联立第三个方程, 得到一个新的由两个方程构成的方程组... 由此归纳下去, 我们总可以解出由 $n$ 个方程构成的同余方程组. 所以我们可以只考虑两个方程构成的方程组, 即:

$$\begin{cases} x \equiv b_1 (\mathrm{mod} c_1) \\ x \equiv b_2 (\mathrm{mod} c_2) \end{cases}$$

容易想到, 在几种特殊的情况下, 求出两个线性同余方程组解集的交集是容易的:

① 若 $c_1, c_2$ 互素, 即 $(c_1, c_2) = 1$

命 $c = c_1 c_2$. 我们知道, 对于一个整数 $x$, 如果确定了其 $\mathrm{mod} c$ 所属的同余类, 则对于 $c$ 的因子 $c_1, c_2$, $x$ 的 $\mathrm{mod} c_1$ 与 $\mathrm{mod} c_2$ 的同余类也是确定的. 由此我们自然的想问, 反过来的对应关系是否也成立? 换言之, 是否存在一个从 $\mathrm{mod} c$ 的完系 $\{0, 1, \ldots, c-1\}$, 到 $\mathrm{mod} c_1$ 的完系 $\{0, 1, \ldots, c_1 - 1\}$ 和 $\mathrm{mod} c_2$ 的完系 $\{0, 1, \ldots, c_2 - 1\}$ 的笛卡尔积之间, 是否存在一个双射 (显然这两个集合的元素个数是相同的) , 使得映射之前和之后的元素同余情况是对应的?

我们给出一个断言, 当 $(c_1, c_2)$ 互素时, 答案是肯定的: 知道了任一整数 $\mathrm{mod} c_1$ 与 $\mathrm{mod} c_2$ 所属的同余类, 就确定了其除以 $c = c_1 c_2$ 得到的余数. 下面我们来证明这一点:

使用反证法, 假定这种决定关系不成立, 即存在 $x_1$ 与 $x_2$ 满足:

$$\begin{cases} x_1 \equiv x_2 \equiv b_1 (\mathrm{mod} c_1) \\ x_1 \equiv x_2 \equiv b_2 (\mathrm{mod} c_2) \\ x_1 \not\equiv x_2 (\mathrm{mod} c_1 c_2) \end{cases}$$

此时我们考虑 $x_1 - x_2$. 根据条件, 有 $c_1 | x_1 - x - 2$ 与 $c_2 | x_1 - x_2$ 同时成立, 故有 $[c_1, c_2] | x_1 - x_2$. 又因为 $(c_1, c_2) = 1$, 故有 $[c_1, c_2] = c_1 c_2$, 即 $c_1 c_2 | x_1 - x_2$. 这就与 $x_1 \not\equiv x_1 (\mathrm{mod} c_1 c_2)$ 矛盾, 证毕.

由此我们知道:

当 $(c_1, c_2) = 1$ 时, 方程 $x \equiv b_1 (\mathrm{mod} c_1)$ 与 $x \equiv b_2 (\mathrm{mod} c_2)$ 的联立方程组的解集必含有 $c_1 c_2$ 的同余类中的恰好一个元素.

此时问题变为如何求出这个元素. 一个简单粗暴的方法是在 $c_1c_2$ 的整个完系里尝试, 但这意味着我们上面的工作并没有降低问题的复杂度, 我们依然希望找到一个直接的算法. 求解线性同余方程的过程给我们以启发: 如果有 $x \equiv b_1(\mathrm{mod}c_1)$, 则也有 $c_2x \equiv c_2b_1(\mathrm{mod}c_1c_2)$. 同样地, 第二个方程也可以转化为 $c_1x \equiv c_1b_2(\mathrm{mod}c_1c_2)$. 由此我们得到方程:

$$(c_2 - c_1)x \equiv (c_1b_1 - c_1b_2)(\mathrm{mod}c_1c_2)$$

我们断言: 这个方程的解就是原方程组的解. 由于已经知道原方程组的解在 $\mathrm{mod}c_1c_2$ 的意义下唯一, 而原方程组又蕴含此方程, 因此只需证明此方程 (有解且) 解唯一.

由于 $(c_1, c_2) = 1$, 故有 $(c_2 - c_1, c_2) = 1$, 否则 $c_1$ 与 $c_2$ 有相同的非平凡因子. 同理, $(c_2 - c_1, c_1) = 1$, 于是就有 $(c_2 - c_1, c_1c_2) = 1$. 根据同余线性方程中解分布情况的讨论, 我们可以知道此方程解存在且唯一. 证毕.

② 若 $c_1, c_2$ 之间存在整除关系

不妨设 $c_1|c_2$ 即 $c_2 = mc_1$. 此时, $x \equiv b_1(\mathrm{mod}c_1)$ 等价于 $mx \equiv mb_1(\mathrm{mod}\ c_2)$, 后者也是一个同余方程, 可以在 $\mathrm{mod}c_2$ 的意义下写出解集. 对这两个解集直接求交集, 就得到了方程组的解集.

③ 一般情况

我们知道, 已知一个整数 $x$ 在 $\mathrm{mod}c$ 中所属的同余类 $b$, 可以将其拆分成其在 $c$ 的两个互质因子 $c = c_1c_2$ 中各自的同余类 $b_1, b_2$ 而不丢失信息. 归纳易证这种拆分可以进行任意有限次. 而要将一个整数尽可能拆分成若干互质因子的积, 不难联想到素因子分解. 因此, 假定 $c$ 的质因数分解为 $c = \prod_{i=1}^{\infty} p_i^{a_i}$ (其中 $p_i$ 表示第 $i$ 个素数, $a_i$ 表示 $c$ 中含有该素因子的数量), 则我们可以将方程 $x \equiv b_1(\mathrm{mod}c)$ 改写为一系列方程 $x \equiv b_{1i}(\mathrm{mod}p_i^{a_{i1}})$ 的联立.

对于原先方程组里的两个方程均作如此处理, 则得到了两列方程 (当然, 由于正整数 $c_i$ 一定有最大的素因子, 所以每一列方程中均只有有限个) . 两列方程的第 $i$ 个都是 $\mathrm{mod}p_i^{a_{i1}}$ 的形式, 因此这两个方程满足上述情况②的条件, 可以简单地取交集得到在 $\mathrm{mod}p_i^{max\{a_{i1},a_{i2}\}}$ 意义下的解. 而不同素因子的幂对应的同余状况, 又可以联立作为一组新的方程. 由于两个不同素数

的任意幂总是互素的, 可以根据上述情况①的结论, 确定所有方程联立后在 $\mod \prod_{i=1}^{\infty} p_i^{max\{a_{i1},a_{i2}\}}$ 意义下的解

## 题解

### 2.1

(1)

先由题给的 $a|b$ 以及平凡的 $a|a$, 可以证出 $a$ 的确是二者的公因子.

再由 $a > 0$ 可知 $a$ 的最大正因子就是 $a$ 本身, 从而任何比 $a$ 更大的正整数不可能是 $a$ 的因子, 自然更不可能同时是 $a, b$ 的因子.

(2)

由定义 $(a, b)$ 是 $b$ 的因子且 $(a, b) > 0$, 直接将 $(a, b)$ 视作 (1) 中的 $a$ 套用 (1) 的结论即证.

### 2.2

(1)

利用辗转相减法的思想:

命 $(n, n+1) = a$. 若 $a > 1$, 则必有 $a|(n+1-n)$ 即 $a|1$. 但这是不可能的, 因为 1 仅有 1 和 $-1$ 两个因子.

(2)

同上理, 命 $(n, n+k) = b$, 则必有 $b|(n+k-n)$ 即 $b|k$, 故 $(n, k)$ 只能在 $k$ 的所有因子中取值.

为了证明可取的值恰好的确是 $k$ 的所有正因子 (负因子由定义当然舍去) , 任取 $k$ 的正因子 $c$, 令 $n = c$ 即可给出了一个构造 ($c$ 是 $c$ 和 $c+k$ 的公因子, 同时它又是 $c$ 的最大因子) .

### 2.3

计算题, 略.

### 2.4

命 $f(n) = n^3 - n$. 对 $n$ 使用数学归纳法证明:

① $n = 1$ 时, 显然成立;

② 若 $n = k$ 时成立, 则 $n = k + 1$ 时:

$f(k+1) - f(k) = ((k+1)^3 - (k+1)) - (k^3 - k) = 3k^2 + 3k = 3(k^2 + k)$

注意到 $k^2$ 与 $k$ 的奇偶性相同, 故 $k^2 + k$ 必为偶数, 即该式必为 6 的倍数, 故证.

### 2.5

由题设, $3^m \equiv 9(\mathrm{mod}10)$.

又有 $3^{m+4n} = 3^m * 3^{4n} = 3^m * 81^n$.

而 $81 \equiv 1(\mathrm{mod}10)$, 故无论 $n$, 乘以 $81^n$ 不影响 $3^m$ 所在的同余类.

### 2.6

trivial 的, 略.

### 2.7

它大于 $n$ 的平方而小于 $n+1$ 的平方, 而 $f(n)=n^2$ 在 $n>0$ 上无疑具有单调性.

### 2.8

由阶乘 (!) 的定义, 易证所有不大于 $m$ 的正整数都是 $m!$ 的因子.

故 $5!$ 同时是 $2,3,4,5$ 的倍数.

那么它分别加上 $2,3,4,5$ 后分别还是 $2,3,4,5$ 的倍数.

*p.s.* 由于上述断言对任意 $m$ 成立, 题目中的结论实际上有个很有意思的推广: 对于任意给定的长度 $m$, 存在连续 $m$ 个正整数全为合数.

证明: 考虑从 $(m+1)!+2$ 到 $(m+1)!+m+1$ 的正整数.

### 2.9

略.

### 2.10

略.

### 2.11

建模, 然后用得到的两个方程中的一个表示出一个元, 代入另一个, 由此划归到单个不定方程的情况.

**2.12**

略.

**2.13**

略.

**2.14**

对任意自然数 $n$:

若 $n \equiv 0(\mathrm{mod}6)$, 显然 6 是 $n$ 的因子, 从而 2 是 $n$ 的一个非平凡因子, 与质数的定义矛盾.

若 $n \equiv 2$ 或 $4(\mathrm{mod}6)$, 则 $n$ 可表示为 $6m+2$ 或 $6m+4$ 的形式, 则 $n$ 必定是一个偶数 (有 2 作为因子) . 又 $n > 3$ 故 $n \neq 2$, 即 2 是 $n$ 的非平凡因子, 同样 $n$ 不可能是质数.

$n \equiv 3(\mathrm{mod}6)$ 的情况同上理.

**2.15**

$n^3$ 与 $(n+1)^3$ 之差为 $3n^2+3n+1$, 显然.

**2.16**

设一个整数 $a$ 的十进制表示对应的字符串为 $a_n a_{n-1}...a_1 a_0$, 则 $a = \sum_{i=0}^{n} 10^i a_i$.

容易验证 $10 \equiv 1(\mathrm{mod}3)$, 从而 $10^n \equiv 1(\mathrm{mod}3)\forall n \in \mathbb{N}$, 故 $a \equiv \sum_{i=0}^{n} a_i(\mathrm{mod}3)$.

**2.17**

(1)

$10 \equiv -1(\mathrm{mod}11)$ 是显然的.

而实际上, $a \equiv b(\mod c)$ 蕴含 $a^n \equiv b^n(\mod c)\forall n \in \mathbb{N}$, 这对任意整数 $a, b, c(c \neq 0)$ 总是成立的. 本题的结论不过是其一个具体的情况.

(2)

偶数位与奇数位分别的数字和之差是 11 的倍数.

*附加题: 分别给出一个整数能被 99 或 101 整除的判别法.*

**2.18**

trivial 的计算题, 略.

**2.19**

同上.

**2.20**

设余数构成的这个等比数列中项为 $k$, 则可根据条件列出不定方程如下:

$$\begin{cases} 3x = 20(k-1) + (k-1) \\ 5y = 20k + k \\ 7z = 20(k+1) + (k+1) \end{cases}$$

(且根据“余数”的定义, 还有不等式 $0 \leq k-1, k+1 < 20$)

方程看似非常纷繁, 但可以注意到第一条与第三条是废话, 因为其右端总是 21 的倍数. 故有用的信息仅仅是 $21k$ 是 5 的倍数, 即 $21k \equiv 0 (\mathrm{mod} 5)$.

再联系 $0 < k < 19$ 的条件, 可知 $k$ 只能取 5, 10, 15. 代入求出 $x$ 等即可.

**2.21**

首先容易注意到 $n = 2$ 是一个解, 并且也显然是最小的正整数解. 但是题目很不要脸地让我们找下一个.

我们知道 $[2, 3, 4, 5, 6] = 60$, 故 $\forall n$ 是原方程的解, $n' = 60m + n$ 也是原方程的解 ($m \in \mathbb{Z}$) , 且这里的 “60” 不能更小, 故 62 是大于 2 的最小的正整数解.

*p.s.* 题目说找整数解, 但显然如果不排除负整数解则解集没有最小元素. 因为当 $n$ 是一个解, $n' = n - 60$ 总是一个比 $n$ 更小的解.

**2.22**

trivial 的, 略.

**2.23**

略.

**2.24**

出于方便起见, 我们考虑 $m$ 与 $n$ 的素因子分解. 由于 $(m,n)=p$, 它们的素因数分解除一个 $p$ 外不交, 故可以写成:

$m=p^{i_0}p_1^{i_1}p_2^{i_2}...$

$n=p^{j_0}q_1^{j_1}q_2^{j_2}...$

这里 $p,p_k,q_k$ 均为素数且两两不同, $i_k,j_k$ 均为正整数, 且 $i_0$ 与 $j_0$ 中至少一者恰为 1.

由此我们有:

$\phi(m)=m*\frac{p-1}{p}*\frac{p_1-1}{p_1}*\frac{p_2-1}{p_2}...$

$\phi(n)=n*\frac{p-1}{p}*\frac{q_1-1}{q_1}*\frac{q_2-1}{q_2}...$

现在考虑 $mn$. 由于 $m$ 与 $n$ 的素因子中除 $p$ 外没有相同的, 故 $mn$ 的素因子分解几乎就是将 $m$ 与 $n$ 的分解连在一起, 只不过 $p$ 的幂次要叠加. 换言之, $mn$ 的全部素因子正是 $p,p_1,q_1,p_2,q_2....$ 故:

$\phi(mn)=mn*\frac{p-1}{p}*\frac{p_1-1}{p_1}*\frac{q_1-1}{q_1}*\frac{p_2-1}{p_2}*\frac{q_2-1}{q_2}...$

比较以上三式可知 $\phi(mn)$ 比起 $\phi(m)$ 与 $\phi(n)$ 相乘只是少了一项 $\frac{p-1}{p}$.

**2.25**

(1)

法一:

连续的 6 个整数内一定有至少 4 个不在 $n$ 的缩系里, 因为 mod6 同余 0, 2, 3, 4 的数总会与 $n$ 有非平凡公因子 (参考 2.14) .

又 $\leq n$ 的正整数的个数为 6 的倍数, 故一定可以被恰好划分成若干个这样的连续的 6 个整数所成的组, 而每组中有资格算进 $\phi(n)$ 的比例总不超过 $\frac{1}{3}$.

法二:

可知 $n$ 有素因子 2,3, 直接套用 $\phi(n)$ 的计算公式即可.

当然这两种做法本质上是一回事.

(2)

由 2.14, 在充分大的时候, 素数 $p$ 的 mod6 的同余类只能是 1 或 5.

考虑 $n$mod6 的同余等价类, 容易验证只能有 $n \equiv 0(\text{mod}6)$. 根据 (1) 的结论即得.

**2.26**

(1) 略.

(2) $\sum\limits_{(i,n)=1} i = \frac{n\phi(n)}{2}$.

(3)

可以断言: 在 $n$ 的缩系中, $k$ 与 $n-k$ 必成对出现 (请读者自行验证, 如果其中一者与 $n$ 不互素即有非平凡公因子, 则另一者必定也有与 $n$ 有同样的公因子) . 这样的元素对数量为 $\frac{\phi(n)}{2}$, 而每一对的和为 $n$.

**2.27**

$314 = 7 \times 44 + 6$, 而乘 6 关于 mod7 的周期为 2.

### 2.28

同上理, 只不过题目问的变成了 mod10 与 mod100.

### 2.29

对 $(k+1)^p$ 作二项式展开, 则从低次到高次第 i 项为 $\binom{p}{i} * k^i$. 展开式第 p 项恰好与后面的 $-k^p$ 抵消.

(这里 $\binom{n}{m}$ 代表组合数 $C(n,m)$, 即从 $n$ 个元素中不计顺序地选取其中 $m$ 个的方法数, 公式为 $\binom{n}{m} = \frac{n*(n-1)*(n-2)*...*(n-m+1)}{m*(m-1)*(m-2)*...*1}$. )

注意 p 是质数, 它唯一的素因子就是它自己, 无法通过将比它小的正整数做乘法得到它. 那么当 $1 \leq i < p$ 时, $\binom{p}{i}$ 的分子里恰有 1 个 $p$, 而分母 (即 $i!$) 里一定不会有哪个数的哪个素因子能把 $p$ 的哪个素因子约掉, 故 $\binom{p}{i}$ 的素因子分解中一定含有 $p$, 即它一即定是 $p$ 的倍数.

则展开相减所得的项里只有 $\binom{p}{0} * k^0 = 1$ 这一项不是 $p$ 的倍数, 故其和 mod$p$ 同余 1.

### 2.30

(1)

由欧拉定理, 左侧每一项都有 $i^{p-1} \equiv 1 (\mathrm{mod}\, p)$, 而总共有 $p-1$ 项, 故同余于 $-1$.

(2)

同上理, 左侧 $\equiv 1+2+3+...+(p-1) (\mathrm{mod}\, p)$. 由于 $p$ 是奇数, 头尾结对求和后恰好有 $\frac{p-1}{2}$ 个 $p$. 总和当然同余于 0.

### 2.31

计算题, 略.

### 2.32

考虑 $n$ 的素因子分解:

$n = p_1^(m_1) * p_2^(n_2) * ...$

这里 $p_i$ 为第 $i$ 大的素数.

则应有 $(m_1 + 1) * (m_2 + 1) * (m_3 + 1)... = 60$.

对各种可能的分解逐一求出其对应的 $n$, 并检查是否满足 $n < 10^4$ 即可.

### 2.33

左式的含义十分明确, 我们来看右式:

$\sigma(n) = d_1 + d_2 + ... + d_{d(n)}$.

注意到如果 $n$ 不是完全平方数, 则 $n$ 的因数中 $d_i$ 与 $d_{d(n)-i} = \frac{n}{d_i}$ 必成对出现, 而 $\frac{d_i}{n} = \frac{1}{d_{d(n)-i}}$ , 故左式的第 $i$ 项恰好与右式的第 $d - i$ 项对应相等.

$n$ 为完全平方数的情况: 对于最中间的因数 $\sqrt{n}$, 左式中的 $\frac{1}{\sqrt{n}}$ 恰好与右式中的 $\frac{\sqrt{n}}{n}$ 相等.

### 2.34

利用定理 2.15.

将 $2^{p-1}$ 换元为 $a$, 则 $a \bmod 10$ 必定同余 2, 4, 6, 8 之一, 而对应的 $2^p - 1$ 即 $2a - 1 \bmod 10$ 同余 3, 7, 1, 5.

容易看出最后一种情况不可能满足 “$2^p - 1$ 为素数” 这一条件. 而其余三种情况下, $a(2a-1) \bmod 10$ 均同余 6 或 8.

### 2.35

想法与上一题类似.

命 $a = 2^{p-1}(p > 2)$ , 则 $n = a(2a-1)$.

由于 $a$ 是 2 的幂, 容易算出 $a \bmod 9$ 的同余类可能且只可能是 1, 2, 4, 5, 7, 8.

又 $2a-1$ 是素数, 不会有因子 3 (注意这里体现了条件 $n > 6$ 的用意) , $\bmod 9$ 的同余类也不可能是 0, 3 或 6, 故 $a$ 所属的同余类还可以排除 5, 2 与 8, 只剩下 1, 4, 7.

此时已经可以验证 $a(2a-1) \bmod 9$ 的同余类必定是 1.

### 2.36

这道题好像改过好几遍, 但是每一版都有每一版的错.

### 2.37

计算题.

### 2.38

无聊的计算题.

**2.39**

显然 $(11, 911) = 1$, 故所给命题等价于 $457^{911} \equiv 1(\mathrm{mod}11) \wedge 457^{911} \equiv 1(\mathrm{mod}911)$ .

对于前者算出循环节即可, 对于后者利用欧拉定理.

**2.40**

比 2.38 还要无聊的计算题.

**2.41**

这道题比较难想, 我们使用 Cayley 图辅助思考:

列举出 $\mathrm{mod}q$ 同余类中的所有元素 $\{0, 1, ..., q-1\}$. 对于每一对元素 $b, c$, 如果 $ab \equiv c(\mathrm{mod}q)$, 则画一条从 $b$ 出发指向 $c$ 的带箭头的边 (称为有向边) , 表示 "元素 $b$ 在做一次 $\mathrm{mod}q$ 乘 $a$ 后变为元素 $c$" .

由此我们得到了一个有向图, 其中每个元素是恰好一条有向边的起点. 由于 $q$ 是素数, 对于任意同余类元素 $r$, 同余方程 $ax \equiv r(\mathrm{mod}q)$ 必定有界且解唯一, 从而每个元素也应该是恰好一条有向边的终点. 这就意味着整张图的所有有向边构成了若干不交的同方向的圈 (称为轨道) , 而每个同余类在且仅在一个轨道上.

*("每个元素恰好作为一条有向边的终点与一条有向边的起点, 则整个图是若干同向圈之并. " 这件事情直观上很好理解, 而严格的陈述与证明需要用到图论的语言, 因此我们在此略过. 感兴趣的读者可以自行了解. )*

显然, 由于 $0a \equiv 0(\mathrm{mod}q)$, 元素 0 指向自身, 自成一个长为 1 的轨道 (称为平凡轨道) .

然后我们来考虑非平凡轨道的长度. 首先考虑 1 所在的轨道, 其上的元素从 1 开始分别为 $1, a, a^2, a^3, ..., a^n, ...$ 由于总的同余类个数是有限的, 因此这个无限序列中的元素不可能两两不同, 从而必定存在一些正整数 $n$ 满足

$a^n \equiv 1(\mathrm{mod}q)$. 由于自然数的良序性, 可以在这些 $n$ 中选出最小的那一个 (仍然记为 $n$) , 这就是 $a \bmod q$ 的阶.

接下来我们考虑一件事情: 其它非平凡轨道的长度可能是多少? 任取另一个非平凡轨道上的一个元素 $b$, 设该轨道的长度是 $m$, 则 $m$ 是满足 $ba^m \equiv b(\mathrm{mod}q)$ 的最小正整数. 由于 $q$ 是素数, $\mathrm{mod}q$ 同余乘法只要乘的不是 0 就都满足消去律, 可以得到 $a^m \equiv 1(\mathrm{mod}q)$, 即 1 经历 $m$ 次乘 $a$ 后回到了 1. 由于 $n$ 是 $a$ 的阶, 也就意味着有 $n \leq m$.

但, 如果 $n < m$, 则有 $ba^n \equiv b \cdot 1 \equiv b(\mathrm{mod}q)$, 从而 $b$ 所在的轨道长度至多是 $n$, 比 $m$ 更小, 矛盾. 这就说明 $n \geq m$ 从而 $n = m$. 换言之: 我们证明了: 在这个若干同向圈之并形成的有向图中, 除了 0 所在的长为 1 的平凡轨道, 其余所有轨道长度都应该恰为 $a$ 的阶 $n$.

根据题目条件, 我们知道 $a^p \equiv -1(\mathrm{mod}q)$, 从而有 $a^{2p} \equiv (-1)^2 \equiv 1(\mathrm{mod}q)$. 显然 $a^p$ 这个同余类在 1 所在的轨道上, 而这个条件告诉我们它正好在这条轨道距离起点 1 的一半处 (从而 $n$ 必是偶数) . 如果我们从 1 开始不断乘 $a$, 则乘到第 $p$ 次时, 这个过程正好在 1 所在的轨道上 “跑了若干圈半” . 设它恰好跑了 $s$ 圈再加一半, 则可以写出 $p = (s + \frac{1}{2})n = (2s + 1)\frac{n}{2}$.

然而, $p$ 本身是一个素数! 如果素数 $p = (2s + 1)\frac{n}{2}$, 而 $2s + 1$ 和 $\frac{n}{2}$ 又都是正整数, 那么它们中必须恰好有一者是 1.

如果 $\frac{n}{2} = 1$ 即 $n = 2$, 说明非平凡轨道长即 $a$ 的阶恰为 2, 从而有 $a^2 \equiv 1(\mathrm{mod}q)$. 又知进行 $p$ 次乘 $a$ 后应恰好停在 $-1$ 的位置, 而 $p$ 是奇数, 从而也应有 $a^1 \equiv -1(\mathrm{mod}q)$;

如果 $2s + 1 = 1$ 即 $s = 0$, 说明作 $p$ 次乘 $a$ 恰好足够在非平凡轨道上走一半, 从而轨道长 $n = 2p$. 由于每条非平凡轨道长度相同, 平凡轨道只有一条仅由 0 构成, 故所有轨道之长应为 $2kp + 1$, 其中 $k$ 为非平凡轨道的数量. 由于整张图中恰有 $q$ 个点, 故有向边的数量也应该是 $q$. 从而存在正整数 $k$ 满足 $q = 2kp + 1$, 这自然也就蕴含了 $q|2kp + 1$.

由此, 两种情况分别蕴含了题给的两种结论. 故而命题得证.

**2.42**

由题意, $a^3 \equiv 1(\mathrm{mod}p)$ 即 $a^3 - 1 \equiv (a-1)(a^2+a+1) \equiv 0(\mathrm{mod}p)$.

由于 $p$ 是素数, 左式的因子 $p$ 不可能由两个因式共同贡献相乘而得, 必然完全来自其中至少一个因式.

若 $a - 1 \equiv 0(\mathrm{mod}p)$, 则 $a$ 的阶应为 1, 与题意矛盾. 故只能是 $a^2 + a \equiv -1(\mathrm{mod}p)$.

下面先证 $(a+1)^6 \equiv 1(\mathrm{mod}p)$:

$(a+1)^6 \equiv a^6 + 6a^5 + 15a^4 + 20a^3 + 15a^2 + 6a + 1 \equiv 22 + 21a^2 + 21a \equiv 22 - 21 \equiv 1(\mathrm{mod}p)$

再证不存在比 6 小的阶, 方法是反复利用上文得到的两个同余式:

若 $a + 1 \equiv 1(\mathrm{mod}p)$, 与 $(a, p) = 1$ 矛盾;

若 $(a+1)^2 \equiv a^2 + 2a + 1 \equiv a \equiv 1(\mathrm{mod}p)$, 与 $a$ 的阶为 3 矛盾;

若 $(a+1)^3 \equiv a^3 + 3a^2 + 3a + 1 \equiv -1 \equiv 1(\mathrm{mod}p)$, 则只可能有 $p = 2$, 但显然不会有哪个数 mod2 的阶为 3;

此后, 如果有 $(a+1)^i \equiv 1(\mathrm{mod}p)$, 则由 mod$p$ 同余乘法的消去律, 也应有 $(a+1)^{6-i} \equiv 1(\mathrm{mod}p)$, 回到如上情形.

## 拓展

### mod$n$ 同余乘法的结构

借用第三章的观点, 我们知道 mod$n$ 同余乘法可以看作 mod$n$ 的所有同余类构成的集合上的一个二元运算. 对于一个有限集上的二元运算, 仅仅写出一个乘法表不足以提供所有的洞见, 我们更希望洞析这个运算的结构.

为了探索同余乘法的结构, 我们引入 Cayley 图来辅助思考. 首先定义如下一种图:

给定正整数 $n$ 及其完系中的一个元素 $a$, 以 $\mod n$ 的每个同余类 $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ 为一个点. 如果两个同余类 $x, y$ 满足 $ax \equiv y (\mod n)$, 则连一条 $x$ 走向 $y$ 的有向边 *(在 $x, y$ 对应的两个点)*

例如, 给定 $n = 7, a = 2$, 则下图为 mod7 同余乘 2 的 Cayley 图:

*graph

当然, 群论中真正的 *Cayley* 图要比这种图广泛得多. 在第五章中我们会再次涉及.

*

# 3 映射

## 笔记

## 题解

### 3.1

(1) 否. 对于 $x_1 = 0$, $x_2 = 0$ 或 1 都能与之对应, 与映射的定义矛盾.

(2) 是.

(3) 否. 理由与上类似.

### 3.2

(1) $R_f = \{0, 1, -1\}$.

(2) $A$ 中共有 4 个不同的元素, 而决定一个映射的过程就是给每个元素指定一个像, 由组合中的乘法原理可知有 $3^4 = 81$ 种映射.

### 3.3

(1) 满射; 非单射: $g(1) = g(-1)$.

(2) 非满射: $3 \in \mathbb{N}$ 没有原像; 非单射: $f(0) = f(3)$.

(3) 都是双射.

(4) 满射: 非单射: $f(0) = f(2)$.

(5) 不是映射: $f(1)$ 不在 $\mathbb{N}$ 中.

### 3.4

$f : A \times B \to B \times A, f(\langle a, b\rangle) = \langle b, a\rangle$.

由于这里 $A \times B$ 与 $B \times A$ 是对称的, $f$ 的良定义本身就蕴含了单射与满射.

*p.s.* 显然这个双射在 $A, B$ 中有无限集合时也是成立的. 之所以这道题里要强调有限集合, 是因为我们还没有严格定义 "无限集合的元素数量", 从而无法讨论无限情况下的 $|A \times B|$, 也就无法将 $|A \times B| = |B \times A|$ 拓展到无限的情况. 关于 "无穷集合的大小", 会在第四章详细讨论.

### 3.5

(1)

值域为 $\mathbb{R}[x]$. 对于任意 $f(x) \in \mathbb{R}[x]$, 记 $f(x) = \sum_{i=0}^{n} a_i x^i$, 则 $F(x) = \sum_{i=1}^{n+1} \frac{a_i}{i+1} x^{i+1} \in \mathbb{R}[x]$ 是它的一个原像.

是满射; 不是单射 (从而不是双射) : $f(x)$ 与 $g(x) = f(x) + 1$ 的像相同.

(2)

值域: 所有常数项为 0 的实系数多项式.

不是满射, 自然也不是双射.

### 3.6

本题要证的结论看上去是形而上学的车轱辘话, 实际上是在向学习者传达 "一般的映射可以看作对每个原像指派一个像" "描述了一个指派就定义了一个映射" 这种观念. 避免刚进入大学的学习者在微积分等其它课程中形成 "函数 (映射) 就是要写出表达式" 的偏差认知.

书写形式上的证明, 只需紧扣定义, 验证单射和满射的性质即可.

假设 $g$ 不是单射, 意味着存在映射 $f_1 \neq f_2$, 使得 $g(f_1) = g(f_2)$, 即:

$(f_1(a_1), f_1(a_2), ..., f_1(a_n)) = (f_2(a_1), f_2(a_2), ..., f_2(a_n))$.

这就是说, 对于每一个 $a_j$, $f_1(a_j) = f_2(a_j)$ 都成立. 但这就意味着 $f_1$ 与 $f_2$ 是相同的映射, 与反证假设矛盾. 故证 $g$ 是单射.

假设 $g$ 不是满射, 意味着存在 $B$ 上长为 $n$ 的数组 $\vec{b} = (b_{i_1}, b_{i_2}, ..., b_{i_n}) \in S(B)$ 不存在原像.

然而, 我们当然这样定义出一个 $A \to B$ 的映射 $f$: 将每个 $a_j$ 的像指派为 $b_{i_j}$. 这是一种最自然的定义映射的方式, 所定义出的 $f$ 无疑是合理的, 而 $f$ 便满足 $g(f) = \vec{b}$. 从而 $S(B)$ 中每个元素都有原像, 即 $g$ 是满射.

综上, $g$ 是双射.

*p.s.* 实际上, 对于 "集合 $B$ 的元素构成的长为 $n$ 的数组", 我们通常采用笛卡尔积的思想, 将它们构成的集合记为 $B^n$, 即 $n$ 个 $B$ 作笛卡尔积. 而 $S$ 通常和置换挂钩, 表示 "$B$ 上全体置换构成的集合", 虽然我不知道为什么这道题里采用了非惯用的记号.

### 3.7

$\cup$ 一条的证明很简单, 略.

注意关于 $\cap$ 一条的结论为什么不是二者相等: 我们可以刻意构造出一组互不包含的 $A$ 与 $B$, 取它们各一个独有的元素 $a$ 与 $b$, 使得 $\alpha(a) = \alpha(b) = t$, 且 $A \cap B$ 中不存在 $c$ 使得 $\alpha(c) = t$. 由此即使得 $t$ 属于右侧而不属于左侧.

### 3.8

单射: $\alpha(S - A) \cap \alpha(A) = \emptyset$

满射: $alpha(S - A) \cup \alpha(A) = T$

### 3.9

略.

### 3.10

平凡的结论, 证明时留心紧扣定义即可.

对称的结论对于满射的情况也是成立的 (从而对于双射也是成立的): 如果 $f, g$ 分别是 $A \to B$ 与 $B \to C$ 的双射, 那么 $g \circ f$ 也一定是 $A \to C$ 的双射.

### 3.11

一组符合要求的构造如下:

命 $g(n) = 2n$. 对于 $f$, 令 $f(2n) = n$ 即可, 形如 $2n+1$ 的元素的像 $f(2n+1)$ 则可以随便指派. 这就给出了一个构造: $f \circ g = I_S$ 容易验证; $g \circ f \neq I_S$ 则是显然的, 因为 $g$ 的值域不是自然数集 $S$.

如果 $f$ 是双射, 则其右逆必定是其左逆, 亦即这样的构造不存在. 证明如下:

由于 $f \circ g = I_S$, 我们考虑将等式两端各右乘一个 $f$, 即得到 $f \circ g \circ f = f$. (这句话的实际含义是: 我们定义一个复合映射, 即 "先作 $f$ 再作 $g$ 最后作 $f$", 由题设可知它一定完全等于 $f$. )

由于 $f$ 是双射, 我们可以定义 $f$ 的逆映射 $f^{-1}$ . (换句话说, 对任意常数 $a$, 方程 $f(x) = a$ 的解必定存在且唯一, 故可以定义一个 "像 $\to$ 原像" 的映射) . 再对上述等式两端各左乘一个 $f^{-1}$, 即得到 $g \circ f = I_S$. 这样就利用 $f$ 的可逆性完成了将 $f$ "搬动" 到右侧的工作.

在学习了第 5 章群论后, 我们可以用代数结构的观点重新看待这一事实: 在一个代数结构中, 如果存在幺元 (单位元) 1, 元素 $a$ 有左逆且有 $ab = 1$, 那么一定有 $ba = 1$, 即这个元素的左逆 "实际上就是它的逆元".

**3.12**

略.

**3.13**

略.

**3.14**

略.

**3.15**

略.

**3.16**

使用归纳法可以带来很多便捷:

① $n = 2$ 的情况是平凡的;

② 若命题在 $n = k$ 时成立, 即 $(12), (23), (34)...(k-1\ k)$ 能够生成所有的 $k$ 元置换. 则 $n = k+1$ 时:

注意到, 如果 $(12), (23), (34)...(k-1\ k)$ 能生成 $1, 2, 3...k$ 上的所有置换, 那么 $(23), (34), (45)...(k\ k+1)$ 无疑也能生成 $2, 3, 4...k+1$ 上的全部置换.

所以, 任给 $k+1$ 元的置换 $s$, 我们可以先用一个 $1,2,3...k$ 上的置换将前 $k$ 个元素尽可能多地搬动到该在的位置上. 如果 $s(k+1)=k+1$, 那么表示已经完成了; 否则, 此时只有 $k+1$, 以及应该去到第 $k+1$ 号位置的那个可怜的元素 $i$ 还没有就位.

如果 $i \neq 1$, 我们再做一个 $2,3,4...k+1$ 上的置换便可交换它们俩; 否则, 先用对换 (12) 交换 1 和 2 的位置, 然后同上理, 最后再用 (12) 把替身 2 还原回去即可, 此时 1 和 $k+1$ 也就位了.

使用对偶的思想我们可以给出另一种十分直观的证法:

我们知道, 对换 (12) 表示的是交换元素 1 和 2 的位置, 而非交换第 1 个与第 2 个位置上的元素. 但是, 如果采用对偶的思想, 通过 "元素 1 到元素 $n$ 的每个元素所在的位置" 而非 "从第 1 个到第 $n$ 个位置上的每个元素" 来记录一个置换, 那么可以等效地认为, 在这道题里我们能够使用的是所有形如 "交换第 $i$ 个与第 $i+1$ 个位置上的元素" 的对换.

在 C 语言课程里我们已经学过, 通过冒泡排序的算法, 只使用这类对换便足以将一个序列排列到任何事先决定好的顺序. 这就证明了这类对换一起可以生成所有的 $n$ 元置换.

### 3.17

把两边都拆成最小项范式即可.

### 3.18

法一:

$f+g=g$ 说明 $(f,g)$ 只有 $(0,0),(0,1),(1,1)$ 三种可能的取值. 对每个等式逐一代进去每种可能, 验证即可.

法二:

采用逻辑的观点:

$f+g=g$ 说明 $f \leq g$, 即 $f$ 为真时 $g$ 一定为真. 由此我们可以对式子作变换如下:

(1) $f \cdot g+\overline{f}=f+\overline{f}=1$

(2) $\overline{f}+g=(\overline{f}+f)+(g-f)=1+(g-f)=1$

(3)

$f \cdot \overline{g} \leq g \cdot \overline{g}=0$

故有 $f \cdot \overline{g}=0$.

**3.19**

略.

# 4 二元关系

## 笔记

## 题解

### 4.1

(1) 对称;

(2) 对称;

(3) 反自反, 反对称, 传递;

(4) 自反, 传递;

(5) 自反, 对称, 传递.

实际上, 一集合 $A$ 上的相等关系是其上最小的等价关系. 这里 "最小" 一词的含义是: 相等关系是等价关系, 且 $A$ 上的每个等价关系 (看作集合) 都包含相等关系. 读者可以自行尝试验证这一点.

### 4.2

(1) 选一个元素个数足够多的集合, 在相等关系的基础上, 添加 $(a,b)(b,a)(b,c)(c,b)$ 但不添加 $(a,c)$.

(2) $\leq$ 关系.

(3) 空关系, 即空集作为 $Z^2$ 的子集所定义的那个二元关系.

### 4.3

计算题, 略.

### 4.4

证明每一个属于左侧的二元组都属于右侧即可.

有意思的地方在于为什么两侧为什么不一定相等. 读者可以仿照题 3.7 自己试着构造一个反例.

### 4.5

显然 $R'$ 的确是自反的, 故只需要证它是自反且包含 $R$ 的最小关系, 即需要证任何满足此性质的关系 $S$ 都会包含 $R'$.

任取一个自反且包含 $R$ 的关系 $S$. 根据定义, $R \subseteq S$; 又由 $S$ 的自反性, $I_A \subseteq S$. 故有 $R \subseteq S$.

### 4.6

关系成立的条件等价于 $a - b = c - d$, 这样改写之后使得等式的每一端仅与一方的元素有关, 从而可以直接利用 $=$ 是等价关系验证等价关系所需的每一个性质, 证明 $\sim$ 是等价关系.

每个等价类即为: 每个 $k$ 对应的 $x - y = k$ 所成的直线, 其经过的那些自然数点 (每个坐标值都是自然数的点) .

### 4.7

证明等价关系的方法同上.

商集中的每个元素 (是一个集合集) 中的每个元素 (是集合, 即 $A$ 的子集) 的元素个数相等. 从而, 商集

$$
\begin{aligned}
\mathscr{P}(A) = \{ & \{ \emptyset \}, \\
& \{ \{1\}, \{2\}, \{3\}, \{4\} \}, \\
& \{ \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\} \}, \\
& \{ \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\} \}, \\
& \{ \{1,2,3,4\} \} \\
\}
\end{aligned}
$$

**4.8**

自反性, 对称性: 略.

传递性:

设 $xRy, yRz$, 即有 $xy > 0$ 与 $yz > 0$. 则 $xy^2z > 0$. 而 $y^2 > 0$, 故有 $xz > 0$, 即 $xRz$.

可以直观看出 $xRy$ 的语义是 "$x$ 与 $y$ 同号" , 进一步可以验证的确任意两个同号的元素都满足 $R$. 故只有 "正" "负数" 两个等价类. 代表元任选即可 (通常我们会选 1 和-1) .

**4.9**

自反性: 略.

对称性:

设 $xRy$, 即 $\exists z \in Z \ s.t. \ x - y = z$.

我们想要证 $yRx$, 即需证 $\exists z' \in Z \ s.t. \ y - x = z'$. 显然取 $z' = z$, 即得到一个 $z'$ 的构造. 故证.

传递性:

与上类似, 构造方式为 $z' = z_1 + z_2$.

可以看出 R 的语义是 “小数部分相同” . 同上理可知全体代表元可取 $[0, 1)$ (当然你想取 $[1729 - \pi, 1730 - \pi)$ 或者其它什么更奇怪的选法也可以是对的, 只要能让你的读者轻易验证就好) .

### 4.10

称所给关系为 $B_A$, 由 $B_A \subseteq A^2$ 可知它的确是 $A$ 上的二元关系. 故逐一验证三条性质即可.

自反性: $\forall a \in A, a \in X$, 故 $(a, a) \exists B$. 又显然有 $(a, a) \in A^2$, 故 $(a, a) \in B_A$.

反对称性: 使用反证法: 若 $\exists a, b \in A$ 使得 $a \neq b$ 且 $(a, b), (b, a) \in B \cap A^2$, 则 $(a, b), (b, a) \in B$, 与 $B$ 的反对称性矛盾.

传递性: 同上理, 设出反例然后利用 $B$ 的性质推出矛盾即可.

本题实际上验证了: 一个集合 $X$ 上的部分序关系 $R$, 限制在其子集 $Y$ 上得到的局部, 也可以自然地看作一个 $Y$ 上的部分序关系. 实际上这件事对等价关系与完全序关系也都是成立的.

### 4.11

读者如果还记得 “关系” 的形式化定义, 就会知道关系是一种集合 (笛卡尔积的子集) . 而 $xR_1y$ 实际上就是 $(x, y) \in R_1$, 从而不难注意到这里的 $\leq$ 实际上就是两个关系之间的包含关系.

而一族集合上的包含关系无疑是部分序关系, 这一点根据包含的定义容易验证.

**4.12**

略.

**4.13**

略.

**4.14**

所证实际上是 “3 元集合上只有 5 种不同构的部分序”. 不过此时读者似乎还没有学到同构, 所以这里借用了 *Hasse* 图的相同与否来表达, 然而这里的相同/不同实际上指的也是图同构...

① a>b>c

② a>c, b>c

③ a>b, a>c

④ a>b, c

⑤ a, b, c

想要严格地形式化地证明 “不重不漏” 非常麻烦, 不过这题只要求说明那就不证了吧.

**4.15**

部分序的证明略. 唯一需要留意的地方: 反对称的证明是怎么用上 $mn > 0$ 这个条件的.

最大元和极大元显然没有. 极小元为 $-1$ 和 1, 由于有多个极小元可知没有最小元.

### 4.16

我不是很能看得懂这个 “序列” 究竟是怎么定义的... 以下解答仅供参考:

① 若 $|A|$ 有限, 那么这个序列是必定有限的. 如果它必须尽可能长, 那么序列的最后一个集合必须是 $A$ 本身 (否则由于它是 $A$ 的子集, 你总可以在后面添上 $A$ 使序列更长) . 此时这些子集的并集无疑是 $A$ 本身, 从而是极大元;

② 若 $|A|$ 可数无穷, 那么你可以通过取 $|A|$ 的一个列举方式作为序列 $a_i$ , 这样这个集合序列的并也将是 $|A|$ 本身, 从而是极大元; 但你也可以刻意规避掉某些元素 (比如取 $A =^+ Z$, 令 $a_i = 2i$ 或 $a_i = i + 1$) , 使得这个并集里总是缺乏那些元素, 从而被 $A$ 真包含, 即不是极大元;

③ 若 $|A|$ 不可数无穷, 那么显然这个序列的并集无论如何都不能包含 $A$ 中的所有元素, 从而总是被 $A$ 真包含, 不是极大元.

### 4.17

$\Leftarrow$:

反证法: 如果 $\exists M$ 不含极小元, 即 $\forall m \in M, \exists m' \in M \ s.t. \ m' < m$. 我们试图证明 $S$ 中存在一个不终止于有限项的递降序列.

构造方法如下: 任取 $m \in M$ 作为 $a_1$, 则由上述假设 $\exists m' \in M$ (从而 $m' \in S$) 满足 $m' < m$. 故可将 $m'$ 作为 $a_2$.

将这个过程无尽地重复下去, 即可得到一个关于 $a_i$ 的构造.

$\Rightarrow$:

反证法: 若存在这样一个序列, 我们试图证明存在一个不符合性质的 $M$.

命集合 $M = a_i = a_1, a_2, ..., a_n, ...$, 则 $M$ 中的任意元素 $a_i$ 都有比它小的元素 $a_{i+1}$, 从而没有极小元.

### 4.18

设有限集合为 $A$, 可数集合为 $M$.

想要证明 $A \cup M$ 可数, 从定义出发的方法是将 $A \cup M$ 中的元素与自然数一一对应 (即所谓 “可列” ) , 我们试图给出一个列举方法:

考虑 $A' = A - M$, 则 $A'$ 仍然是一个有限集 (当然可能是空集) 且 $A' \cap M = \emptyset$. 设 $|A'| = a'$, 则可以将 $A'$ 中的元素与集合 $\{1, 2, ..., a'\}$ 中的元素一一对应.

由于 $M$ 是可数集合, 可以在 $M$ 与自然数集 $N = \{1, 2, ...\}$ 之间建立一一对应, 而后者又可以与自然数集的子集 $\{a' + 1, a' + 2, ...\}$ 一一对应. 将这个两个双射复合即可得到 $M$ 到 $\{a' + 1, a' + 2, ...\}$ 的一个双射.

现在我们分别有 $A' \to \{1, 2, ..., a'\}$ 与 $M \to \{a' + 1, a' + 2, ...\}$ 这两个双射. 由于它们的定义域与值域分别均不交, 可以将它们简单作并得到一个新的映射, 且这个映射依然是双射. 而 $A' \cup M = A \cup M$, 故这个双射就说明了 $A \cup M$ 与 $N$ 的等势.

*p.s.* 其实也可以直接先列举 $A$ 中的所有元素, 再列举 $M$ 中的所有元素, 最后删去重复的元素并将剩下的元素归并好, 由此得到一个列举. 这个方法很直观但不够形式化, 不建议初学者用这种方法写严谨的证明.

思考题: 证明两个可数集合的并是可数集合; 证明任意有限多个可数集合的并是可数集合; 证明可数无穷多个可数集合的并是可数集合.

### 4.19

列举 $N^2$ 的方法很多, 例如按照每个元素 $(m, n)$ 的两数之和从小到大列举, 和相同的所有元素则按随便一个规律 (例如对 $m$ 从小到大) 指派顺序:

$(0,0),(0,1),(1,0),(0,2),(1,1),(2,0),(0,3),...$

**4.20**

两个集合都不与 $N$ 等势, 所以肯定不用去找列举的方法了.

我们先给出如下一个惊为天人的构造:

$f:R\to R^2$, 若 $x\in R$, 写出 $x$ 的十进制表示 $\overline{...x_2x_1x_0.x_{-1}x_{-2}...}$ 并在这个表示的前端添加可列无穷多个 0 (自然地, 如果 $x$ 表示为有限小数, 在后端也添加无穷多个 0) , 由此得到一个两端无限延伸的表示 $x'$ (注意: $x'$ 不是数, 而是一个两端无限延伸的数字序列) .

我们把这个表示每隔一位取出来, 将取出来的数位与留下的数位分别缩并成一个新的小数, 显然它们也各自是一个两端无限延伸的表示, 而这两个表示又可以被翻译回为两个实数. 我们命这两个实数所成的有序对即为 $f(x)$.

(例如, ...0003.1415926535... 被拆分成 ...03.45255... 和 ...00.11963...)

不难理解, 这个不知道怎么想到的构造方法几乎真的把 $R$ 上的元素一一映射到了 $R^2$ 上. 之所以说 "几乎" , 是因为开头我们定义的翻译过程有个小 bug: 这样写出来的表示并不是与实数一一对应的, 而不对应之处便在于万恶的 9999...
. 所以我们需要给这个部分打补丁.

(如果你还不能理解这为什么构成对上述证明的一个反驳, 考虑如下两个实数 $x$ 与 $y$:

$x=4, x'=...0004.0000..., [f(x)]'=(...04.00..., ...00.00...), f(x)=(4,0)$

$y=3.999..., y'=...0003.9999..., [f(y)]'=(...03.99..., ...00.99...), f(y)=(4,1)$

显然有 $x=y$, 但 $f(x)$ $f(y)$. )

不过这个补丁也很容易想到: 我们规定所有的实数都必须使用无限小数表示就好了. 换言之, 即使一个实数存在有限小数表示, 也把它的表示规定成

$...x\__i9999...$ 这种样子. 不难验证: 由此定义出的翻译方法便能衍生出一个的确是双射的 $f$ 了.

*p.s.* 为什么给出的补丁不是 *"对.9999... 这类实数必须使用有限小数表示"?* 这样做能填上漏洞吗? 这部分的思考就留给聪明的读者作为习题了.

*(提示: 考虑 4.0909... 与 5)*

# 5 群论初步

## 笔记

## 题解

### 5.1

尽管书上已经给出过定义, 但我们这里还是再强调一遍这一点: 群的定义是满足封 (封闭性) 结 (结合律) 幺 (幺元的存在性) 逆 (每个元素逆元的存在性) 这 4 条公理的代数系统. 因此, 验证一个代数系统是不是群, 根据定义的做法即是验证其上的运算的确满足这 4 条性质; 要证明一个代数系统不是群, 也就是要指出至少一条被违反了的性质.

这种从定义出发的证明格式是学习群论的第一课.

(1) $\times$

$|1| = |-1| = 1$ 故 $1, -1 \in S$. 但 $|1 + (-1)| = 0$ 故 $1 + (-1) \notin S$, 不满足封闭性.

(2) $\surd$ 且是交换群

我这里写一遍证明格式, 由于这个工作实在是太愚蠢了所以我只做一遍:

封闭性:

$s_1, s_2 \in S, \exists a_1, a_2, b_1, b_2 \in Q$ 满足 $s_1 = a_1 + b_1\sqrt{2}, s_2 = a_2 + b_2\sqrt{2}$

则 $s_1 + s_2 = (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$. 由有理数加法的封闭性 (题目没有给出 $Q$ 的定义, 对读者来说这个估计也不用证) , 可知 $a_1 + a_2, b_1 + b_2 \in Q$.

故 $s_1 + s_2 \in S$.

结合律:

普通乘法具有结合律 (严格来说需要设一组 $s_1, s_2, s_3$ 代进去验证两种计算顺序得到的结果相同, 反正我懒得写了) .

幺元:

$0 \in Q$, 故 $0 = 0 + 0\sqrt{2} \in S$. 而 $\forall s \in S, s + 0 = 0 + s = s \in S$. 故 0 为 $S$ 关于复数加法的幺元.

逆: $\forall s \in S, \exists a, b \in Q$ 满足 $s = a + b\sqrt{2}$. 由有理数的性质, $-a, -b \in Q$, 故 $-s = -a + (-b)\sqrt{2} \in S$. 而 $-s + s = 0$. 故 $-s$ 为 $s$ 在 $S$ 中关于复数加法的逆元.

交:

复数加法具有满足律, 它限制在复数集 $C$ 的子集上当然也满足交换律, 因为这样的限制并不改变两个复数作加法的结果.

证毕.

(3) √ 且是交换群

请自行逐一验证 (其中结合律一条有 $4^3 = 64$ 种组合方式所以要验证 64 次) ; 也可以用线性代数的知识证明: 同阶对角矩阵的乘法其实就是对应位置上的元素的数分别作乘法. 从而易证 5 条性质 (显然这里算上了我们亲爱的交换律) .

(4) √ 且是交换群

封闭性易见;

结合律自己挨个手算一遍 (由于这里的 * 没有具体的语义, 故没有简便方法) ;

幺元: 容易验证是 $\gamma$;

逆元: $\beta$ 的逆元是自身, $\alpha$ 和 $\sigma$ 互为逆元.

交换律: 容易看出乘法表是对称的, 即总有 $a * b = b * a$.

(5)

这种强行定义出来的东西一般性质都不怎么好, 所以先试试能不能证不是群.

然后我们惊喜地发现 $*$ 限制在负数集上就是除法, 而除法当然是不满足结合律的了, 所以任取三个负数就可以证伪结合律.

(如果你试图证伪其它 3 条性质, 会发现都做不到:

封闭性易见;

显然如果 $*$ 有幺元那么只能是 1, 验证一下发现 1 还真是幺元 (因为 1 在左时只取前一种情况, 而 1 在右时无论哪种不会改变 $x$) . 从而易见正数的逆元是其倒数而负数的逆元是其自身. )

### 5.2

(1) 略. 幺元是 0, $a$ 的逆元是 $-\frac{a}{a+1}$.

(2) 可以硬算. 但也可以注意到 $S$ 显然是交换群, 所以可以把 3 换到前面去先和 2 做运算, 节省一点计算量.

$x = -\frac{1}{3}$

### 5.3

要证明交换群, 就是要证明 $\forall a, b \in G, ab = ba$.

已知条件看上去和 $ab$ 这样的形式没有什么关系, 我们得试着把它利用起来, 所以我们考虑以下元素: $(ab)^2 = abab = 1$.

又意识到 $aabb = 1$, 而群中有消去律 (如果你做到这里时还不知道什么是消去律, 对以上两式同时左乘 $a^{-1}$ 右乘 $b^{-1}$ 即可) , 所以有 $ba = ab$.

这正是我们要证的命题.

*p.s.* 有的解答会随手甩一句 "$abab = (ab)^2 = 1 = a^2b^2 = aabb$, 故 $ba = ab$" . 这种做法在初学者看来或许会有点像变魔术, 或者像那种自己这里点点那里碰碰不知道怎么就通关了的解谜游戏. 其实群论的一些萌新级别的证明题确实和解谜游戏很像: 萌新要学会放弃思考 "这个运算的 '含义' 到底是什么", 转而只关注可以使用的证明规则 (即试图理解结构而非内容) , 并尽

可能利用这些规则到达自己所需的命题.

### 5.4

$\Rightarrow$:

显然.

$\Leftarrow$:

同 3 理, 用消去律.

### 5.5

(1)

反证法: 设存在一个元素 $g$ 及其逆元 $g'$, 它们的阶分别为 $i$ 与 $i'$ 而 $i \neq i'$. 不妨设 $i$ 与 $i'$ 中的较小者为 $i$.

考虑 $g^i * g'^i$. 由一个元素与其逆元的可交换性可知它等于 $(gg')^i = 1$. 而又有 $g^i = 1$, 故根据消去律 $g'^i = 1$, 这与 $i$ 作为阶的最小性矛盾.

(2)

两端同乘以 $g^k$, 然后同上理.

### 5.6

设 $ab$ 的阶为 $i$, 即有 $(ab)^i = abab...ab$ ($i$ 个 "$ab$" ) $= 1$.

两式同时左乘 $a^{-1}$, 有 $bab...ab = a^{-1}$. 再同时右乘 $a$, 有 $baba...ba$ ($i$ 个 "$ba$" ) $= 1$.

故 $ba$ 的 $i$ 次幂也为 1, 那么 $i$ 一定是 $ba$ 的幂 $j$ 的倍数. 但根据对称性, 又有 $j$ 是 $i$ 的倍数. 由于 $i$ 与 $j$ 都是正整数, 显然有 $i = j$.

### 5.7

题目有一个不容易利用起来的条件 "$a$ 是唯一的二阶元" . 所以我们可以考虑反证法: 即假设 $\exists x$ 使得 $ax \neq xa$, 试图证明还有 $a$ 以外的二阶元.

$ax \neq xa$, 即是 $x^{-1}ax \neq a$.

而 $(x^{-1}ax)^2$=$x^{-1}axx^{-1}ax = x^{-1}aax = x^{-1}x = 1$, 故其要么是二阶元, 要么是一阶元即幺元自己.

由前提知没有 $a$ 以外的二阶元. 故 $x^{-1}ax = 1$ 即 $ax = x$, 从而 $a = 1$. 这与 $a$ 是二阶元矛盾.

### 5.8

回想起 5.(1): "任意元素与其逆元同阶" , 我们可以将每个元素和它的逆元两两配对, 由此无法配对的元素只能是 1 或 2 阶元, 因为它们都以自己为逆元.

而 1 阶元只有一个, 每一对又恰为群贡献两个元素, 为保证 $|G|$ 为偶数, 必定有奇数个 2 阶元, 那么自然也就至少有一个.

### 5.9

已经知道 $H$ 是 $G$ 的子集, 那么只需证 $H$ 本身是群. 这回我们得换个顺序:

结合律: 从 $G$ 中继承;

幺元: 任取一个 $h \in H$, 有 $h * h^{-1} = 1_G \in H$. 显然 $G$ 中的幺元到了 $H$ 中还是幺元 (实际上这个位子也只能给 $G$ 中的幺元) , 故 $H$ 有幺元.

逆元: $\forall h \in H, 1 * h^{-1} = h_G^{-1} \in H$. 由于 $1_H$ 就是 $1_G$, $G$ 中每个元素的逆元到了 $H$ 中也是该元素的逆元 (并且对应的位子也只能给它) .

封闭性: $\forall h_1, h_2 \in H$, 由逆元一条知 $h_2^{-1} \in H$. 故有 $h_1 * (h_2^{-1})^{-1} = h_1 * h_2 \in H$.

*p.s. 需要换顺序的原因很容易看出. 这回要问的思考题是: $H$ "非空" 这个条件有什么作用? 当然, 我们知道从内容上讲, 根据定义, 空集不成群; 但这里要问的是: 上面的论述构成了一个看上去还算有模有样的证明. 如果把 "非空" 这个条件撤掉, 从形式上讲, 上述证明的哪一步会受到损害?*

*(书上好像没讲空集为什么不成群. 那这里也一并问了吧: 空集 (并配备了一个运算 *, 由于空集中没有元素, 这个运算实际上不需要定义/可以随便定义) 应该被认为是群吗? 如果不是, 它违反了哪一条公理? )*

**5.10**

结合律: 继承;

幺元: 显然;

封闭性: $a, b \in H, c \in G, c(ab) = (ca)b = (ac)b = a(cb) = a(bc) = (ab)c$, 故 $ab$ 是 $G$ 中的可交换元, 即 $ab \in H$;

逆: $\forall a \in H, c \in G, a^{-1}aca^{-1} = ca^{-1}$, 但如果你把 $a$ 换到右边去, 化简后留下来的 $a^{-1}$ 就是左边那个, 即 $a^{-1}aca^{-1} = a^{-1}c$. 故 $a^{-1}c = ca^{-1}$, 即 $a^{-1}$ 也是可交换元, 根据定义有 $a^{-1} \in H$.

**5.11**

$\cap$: 是, 利用交集的定义证明封闭性, 以及幺元和各逆元的存在性即可.

$\cup$: 不总成立. 例如考虑 $G = (Z_2)^2, H = (0,0), (0,1), K = (0,0), (1,0)$.

实际上, 如果你观察上面那个反例构成反例的缘由, 或者你试图证明一下成立然后看看自己在哪里卡壳了, 你会意识到在非平凡的情况下 (即除非 $H \subseteq K$ 或 $K \subseteq H$), 这个命题总是不成立的: 你可以任取 $H, K$ 各自独有的一个元素 $h, k$, 将它们作运算 $hk$. 利用群的性质可证无论 $hk$ 属于 $H$ 与 $K$ 中的哪一个, 都会违背 "独有" 这件事, 从而矛盾. 故结果只能落在 $H \cup K$ 之外.

**5.12**

除了两个平凡子群 $\{1\}$ 和 $K_4$ 本身, 还有 $\{1, a\}, \{1, b\}$ 和 $\{1, c\}$.

**5.13**

验证即可. 略.

**5.14**

(1) $\times$

虽然这里不要求, 但如果要证明一个群 $G$ 不是循环群, 从定义出发需要证明 $G$ 中任何一个元素 $g$ 都不能单凭自己生成 $G$ 的全体. 这里反例可以取 $h = \frac{g}{2}$ (如果 $g$ 是 0 就更显然了) .

(2) $\surd$

6 与-6.

(3) $\surd$

6 与 $\frac{1}{6}$.

**5.15**

略.

**5.16**

如果 $G$ 有 3 个及以上的元素, 那么生成元的逆 $g^{-1}$ 必然与 $g$ 不同, 但它又有着与 $g$ 相同的阶, 故可取彼而代之矣.

**5.17**

可以断言 $i$ 从 1 到 $n$ 取值时, $g^i$ 作为 $G$ 中的元素两两不同. 否则, 即有 $g^j = g^k$, 其中 $j, k \in \{1, 2, ..., n\}$ 且 $j \neq k$, 不妨设 $k > j$. 则 $g^{k-j} = 1$, 从而 $g$ 的阶 $n$ 是 $k - j$ 的因子. 但 $0 < k - j < n$, 矛盾.

而 $G$ 中一共就只有 $n$ 个不同的元素, 这就意味着 $g$ 可以生成整个 $G$.

**5.18**

$G$ 的 $d$ 阶子群中元素的阶应为 $d$ 的因子, 由数论知识可知 $d$ 是 $n$ 的因子时, 全体 $\mathrm{mod}n$ 同余类即 $G$ 中的元素中能做到这一点的恰有 $d$ 个. 所以 $G$ 中如果存在 $d$ 阶子群, 那么只能恰好由这 $d$ 个元素组成.

容易验证这 $d$ 个元素关于 $\mathrm{mod}n$ 同余加法同构于 $Z_d$.

**5.19**

除了两个平凡的, 还有 $\{I, (12)\}, \{I, (13)\}, \{I, (23)\}, \{I, (123), (132)\}$ 这 4 个.

**5.20**

懒得写.

**5.21**

反证法: 假设 $S$ 的子群 $T$ 中存在奇置换且其数目与偶置换不同.

由于每个 $n$ 元置换都可以表示成 $\{1, 2, ..., n\}$ 上的对换的乘积, 且该置换本身的奇偶性与这种表示用到的对换数量的奇偶性相同, 容易证明置换乘法也满足所谓的 “奇偶得奇, 奇奇得偶” .

所以, 任取一个奇置换, 它分别乘上所有奇置换 (当然包括它自身) 得到的必定都是偶置换, 由封闭性这些偶置换都在 $T$ 中. 故偶置换的数目不低于奇置换.

但是反过来如法炮制一次也成立, 从而奇置换不少于偶置换, 即两者只能数目相等, thus lead to contradiction.

**5.22**

$f : Z \to 2Z, f(a) = 2a$

容易验证这便是一个同构映射 (是双射且保运算) .

*补充题: $Z$ 与 $2Z$ 之间的所有同构映射有哪些?*

**5.23**

自反性: 即需证对任意群 $G$, 有 $G \cong G$. 取 f 为恒等映射即可.

对称性: 对于两个同构的群 $G_1, G_2$ 及其间的同构映射 $f : G_1 \to G_2$, 由于 $f$ 是双射, 故存在逆映射 $f^{-1}$, 可以验证此即为 $G_2 \to G_1$ 的同构映射.

传递性: 对于群 $G_1, G_2, G_3$ 及其间的两个同构映射 $f : G_1 \to G_2$ 与 $g : G_2 \to G_3$, 取映射 $h = g \circ f$ 即可. 由 $f$ 与 $g$ 均是双射, 可证 $h$ 也是双射. 可以验证 $h$ 便是 $G_1 \to G_3$ 的同构映射.

**5.24**

‘

**5.25**

首先易证引理 1: 无限循环群 $G \cong Z$ 中除了幺元 0 $(e)$ 以外任意元素的阶都是无限的.

然后可以证明引理 2: 循环群 $G$ 的子群 $H$ 依然是循环群.

故任取 $G$ 的子群 $H$, 根据引理 2, 其如果不是无限循环群, 那么只能是有限循环群. 而其如果不是 0 , 那么任取非零元素 $a$, 其阶 $i$ 必定是正整数. 但这个阶在 $G$ 中也成立, 与引理 1 矛盾.

**5.26**

封闭性: 略.

结合律: $a \cdot (b \cdot c) = a \cdot (c * b) = (c * b) * a = c * (b * a) = c * (a \cdot b) = (a \cdot b) \cdot c$;

幺元: 容易验证 $\langle G, * \rangle$ 的逆 $I_{\langle G,* \rangle}$ 即为 $\langle G, \cdot \rangle$ 的幺;

逆元: 同上理, 容易验证一个元素在 $\langle G, * \rangle$ 中的逆即为其在 $\langle G, \cdot \rangle$ 中的逆.

# 6 商群

## 笔记

## 题解

### 6.1

$\forall h \in H, ah = ha \in Ha$. 故 $aH \in Ha$.

反之亦然, 可知 $aH = Ha$.

这实际上证明了: 交换群的子群一定也是正规子群. 换言之, 如果有时我们想构造非正规子群的例子, 必须去非交换群中寻找.

### 6.2

证明 $n$ 个命题两两等价的常用途径是逐一证明 $p_1 \to p_2, p_2 \to p_3, ..., p_{n-1} \to p_n, p_n \to p_1$, 由此说明这些命题中的任意两个可以互相推出. 但建议学习者先从自己的直观出发, 先考虑那些彼此之间容易看出关联的命题.

‘

### 6.3

懒得写.

### 6.4

由题知 $H$ 的陪集只有一个 (且这个陪集既是左陪集也是右陪集, 从而 H 是正规子群) , 即 $H$ 在 $G$ 中的补集 $G\backslash H = \{x \in G | x \notin H\}$.

若 $a \in H$, 命题自然成立; 若 $a \notin H$ 即 $a \in G\backslash H$, 如果此时有 $a^2 \in G\backslash H$, 则 $aH$ 与 $a^2H$ 都是陪集 $G\backslash H$. 但由题 6.2 中 (2) 与 (5) 的等价性可知这意味

着 $a = a^{-1}a^2 \in a^{-1}aH = H$. 矛盾.

追问:

自己试着证一下就能发现反例的构造方法:

若有 $a \in H$, 显然成立. 若 $a \notin H$, 则 $aH$ 是 $H$ 的一个左陪集, 不妨称另一个左陪集为 $bH$.

我们先考虑 $a^2$, 显然不能有 $a^2 \in aH$, 否则同上理 $a$ 属于 $H$. 如果想要证明题给的断言, 接下来我们本应试图证明 $a^2 \in bH$ 即 $a^2 \in H$, 但实际上这是不总成立的. 考虑以下反例:

取 $G = S_3, H = I, (12)$, 显然满足题给的性质. 考虑 $a = (23)$, 则 $a^2 = I \in H$.

### 6.5

直接从群的元素个数出发, 写 "设群 $G$ 的阶为 $n$" 是错误的. 因为 $G$ 不一定是有限群.

由于 $H \cap K$ 是群, 则它也分别是 $H$ 和 $K$ 的子群. 考虑积集 (不一定是群) $HK = \{hk | h \in H, k \in K\}$, 它是 $K$ 的一系列左陪集 $a_iK$ 的不交并, 其中 $a_i \in H$. 与此同时, $H$ 也是其子群 $H \cap K$ 的一系列左陪集 $b_j(H \cap K)$ 的不交并, 其中 $b_j \in H$.

考虑 $HK/K$ 的商集中的元素: $H$ 的两元素 $h_1, h_2$ 属于同一个左陪集 $a_iK$, 当且仅当 $h_1K = h_2K$ 即 $h_1h_2^{-1} \in K$, 后者又等价于 $h_1h_2^{-1} \in H \cap K$; 类似地, 考虑 $H/(H \cap K)$ 的商集中的元素: $H$ 的两元素 $h_1, h_2$ 属于同一个左陪集 $b_j(H \cap K)$, 当且仅当 $h_1h_2^{-1} \in H \cap K$.

这就说明这两个商结构对 $H$ 所作的划分完全相同, 从而划分出的陪集数量也相同, 即有 $[HK : K] = [H : H \cap K]$ (这种写法实际上有些瑕疵, 因为 $HK$ 不一定是群) . 而 $HK \subseteq G$, 所以 $n = [G : K] \geq [HK : K] = [H : H \cap K]$.

从而有 $[G:H\cap K]=[G:H][H:H\cap K]\leq m\cdot n$.

### 6.6

反证法: 若 $G$ 有两个不同的 $q$ 阶子群 $A$ 与 $B$.

则 $A\cap B$ 亦为 $G$ 的子群, 同时又是 $A$ 的子群, 故其阶只能是 $q$ 或 1. 但若 $|A\cap B|=q$, 则其等于 $A$, 即得 $A=B$, 矛盾.

故只能是 $|A\cap B|=1$, 即 $A\cap B=e$, 这是两个除 $e$ 外不交的子群. 那么它们的乘积 $AB=ab|a\in A,b\in B$ 应有 $q^2$ 个不同的元素 (如果存在非平凡的 $a_1b_1=a_2b_2$, 则有 $(a_1)^{-1}a_2=b_1(b_2)^{-1}$, 两端非幺元且分别属于 $A$ 与 $B$, 矛盾) , 而这些元素都是 $G$ 中的元素, 从而 $|G|=pq\geq q^2$. 矛盾.

*p.s.* 实际上, 根据近世代数知识, 可以确定这样的群一定是 $pq$ 阶循环群 $Z_{pq}$.

### 6.7

由题给条件我们知道成立陪集的相等关系 $aH=bH,cH=dH$. 由于 $H$ 是正规子群, , 同一个元素乘出的左陪集与右陪集总是相同, 实际上也就有 $aH=Ha=bH=Hb,cH=Hc=dH=Hd$.

我们考虑子集 $aH=bH$ 以及 $Hc=Hd$, 既然是相同的子集, 我们可以通过相乘得到 $aHHc=bHHd$. 又 $H$ 是群, 其中的两元素相乘依然在 $H$ 中, 所以 $HH=H$, 即上式可以得到 $aHc=bHd$. 再次根据 $H$ 的正规性分别交换 $H$ 与 $c,d$ 得到 $acH=bdH$. 这就说明了 $ac\sim bd$.

*p.s.* 请读者注意这里每次作集合乘积的具体含义.

### 6.8

要看懂 $H$ 即为 $m$ 的整数倍所构成的集合, 然后这题就很平凡了:

$G/H = \{[0], [1]...[m-1]\}$, 其中 $[m]$ 为 $m$ 所在的等价类/陪集.

单位元为 $[0]$.

### 6.9

反证法: 若 $H$ 不是正规子群, 则存在 $a \in G$ $s.t.$ $aH \neq Ha$ 即 $aHa' \neq H$.

可以验证 $aHa'$ 也是 $G$ 的一个子群 (验证留给读者作为习题) , 且其阶数与 $H$ 相同, 矛盾.

### 6.10

$H_1 \cap H_2$ 是子群的证明见前.

正规性:

命 $H = H_1 \cap H_2$. 任取 $g \in G$ 考虑 $gH$, 则有 $gH \subseteq gH_1 = H_1 g$, 同理 $gH \subseteq H_2 g$. 故 $gH \subseteq Hg$. 由元素个数易知 (或者你把上面的过程反过来操作一遍) $gH = Hg$, 故证.

$H_1 H_2$:

子群:

封: 任取 $h_1 h_2$, 由 $H_1$ 正规性知存在 $h \in H_1$ 使得 $h_1 h_2 = h_2 h$. 故有 $h_{11} h_{21} h_{12} h_{22} = h_{11} h_{13} h_{21} h_{22} = h_1 h_2 \in H_1 H_2$;

幺: $1 \in H_1$ 且 $1 \in H_2$, 故 $1 = 1 * 1 \in H_1 H_2$. 由 1 是 $G$ 的幺元可知它也是 $G$ 任意子集的幺元;

逆: 任取 $h_1 h_2$, 其在 $G$ 中的逆为 $h_2' h_1' \in H_2 H_1$, 而由任一 $H_i$ 正规性可知这 $H_1 H_2$ 中的元素.

正规性: 任取 $a \in G$, 考虑 $aH_1 H_2$. 由两个 $H_i$ 的正规性交换两次顺序即可.

### 6.11

由其与 $G$ 的关系易证 $H_1N$ 是群, 而它又是 $H_2N$ 的子集, 故是子群.

又 $H_1N$ 是 $G$ 的正规子群 (上一题的结论) , 故任取 $x \in H_2N \subseteq G$, 有 $xH_1N = H_1Nx$. 从而 $H_1N$ 也是 $H_2N$ 的正规子群.

### 6.13

首先把符号翻译成自己能看懂的人话: $f$ 是一个将 $Z$ 中所有元素映射到 $0, 1$ 上的函数, $G$ 则是所有这样的 $f$ 组成的集合.

交换群:

封: 任取 $f_1, f_2 \in G$, $f_1 + f_2$ 在每一个 $z$ 上的取值都是 $Z_2$ 上的元素, 故这也是一个 $Z \to Z_2$ 的函数;

结: 平凡;

幺: $f_0 = 0$ (请注意: 这里的 $f_0$ 不是 $Z$ 或 $Z_2$ 中的元素, 而是一个 "把所有整数都映射到 0" 的函数 $f : f(a) = 0$, 即所谓零函数) 为幺元;

逆: 任取 $f$, 定义 $f' : Z \to Z_2, f'(a) = -f(a)$, 则 $f'$ 为其逆 (虽然下面我们会看到 $-f$ 其实就是 $f$, 但还是请注意 $-1$ 作为 $Z_2$ 的一个元素在 $Z_2$ 上 "做乘法" 的意义究竟是什么) ;

交: 废话.

阶为 2: 任取 $f$ 考虑 $2f$ 即 $f + f$. 在任一处 $z$ 上 $f$ 的取值无论是 0 还是 1, 这个元素自加后都将在 $Z_2$ 中得到 0, 即 $2f$ 是零函数, 亦即 $G$ 中的幺元. 故证.

*p.s.* 我忘记我要补充什么了, 等我回想起来了再说.

### 6.14

判断一个映射是否是同态映射, 实际上就是看这个映射是否保持了原结构. 而在代数结构中, "结构" 即是每一种运算的每一个结果.

(1) √: $xy = z \Rightarrow |x||y| = |xy| = |z|$

(2) ×: $xy = z \Rightarrow 2x \cdot 2y = 4z \neq 2z$

其余小题过程略.

(3) √

(4) √

(5) ×

(6) √

### 6.15

(如果我没理解错的话, $(Q)_n$ 意为 $n$ 阶有理数方阵集合. )

同态断言的语义其实就是 "det 的乘积等于乘积的 det" , 这是我们在线性代数课程中已经知道的. Ker 即为 det= 1 的所有矩阵.

### 6.16

同态: $f(a)f(b) = a^k b^k = (ab)^k = f(ab)$. 这里起关键作用的是交换律.

$f(G)$ 好像没有什么简洁的表示... 难道就说成 "$G$ 中所有形如 $a^k$ 的元素" ? Ker$f$ 为 $G$ 中所有满足 $a^k = 1$ 的 $a$, 或者说所有 "阶为 $k$ 的因数" 的元素.

### 6.17

数学上没什么难度. 要注意 $m$ 和 $n$ 都是确定的数, 左右两侧都是关于 $k$ 的命题. 基于这一点把题意翻译成人话就好了.

### 6.18

考虑商集 $G/H$, 则其元素个数为 $m$, 而 $xH$ 为其中的元素. $x^m \in H$ 等价于 $(xH)^m = H$, 故所证即为 "元素的阶是群的元素个数的因数", 而这是我们已经知道的.

### 6.19

由题意, $\forall a, b \in G$, 都有 $abH = baH, abK = baK$. 故 $ab(H \cap K) = abH \cap abK = baH \cap baK = ba(H \cap K)$.

### 6.20

(1)

先证子群:

封: 有限个换位子乘积与有限个换位子乘积相乘, 显然还是有限个换位子乘积;

结: 略;

幺: $1' * 1' * 1 * 1 = 1 \in G'$ 是 $G'$ 的幺元;

逆:

先考虑单个换位子: $\forall a, b \in G$, $a'b'ab$ 的逆是 $b'a'ba$, 而后者显然也是一个换位子, 从而 $\in G'$.

如果 $x \in G$ 是多个换位子的成绩, 则这些换位子每一个的逆也在 $G'$ 中, 从而其反向求积也在 $G'$ 中. 这个反向积即是 $x$ 的逆.

再证正规性:

$\forall x \in G$, $xG'$ 中的元素可表示为 $xa'b'abc'd'cd....$ 我们下面讨论只有一个换位子的情况, 多个换位子的情况基本一样.

对于每个 $xa'b'ab \in xG'$, 我们要证明 $\exists c, d \in G$ 使得 $c'd'cdx \in xG'$. 这里的 $c$ 与 $d$ 我们可以随意构造, 关键目的是在代入与消去后让两式形式相同.

注意到两式 $x$ 的位置不同, 我们很自然地认为 $c$ 应该具有 $xa...$ 的形式, 而 $d$ 应该形如 $...bx'$. 而为了使右侧中段不出现多余的 $x$ 或 $x'$, 我们可以试着让 $c$ 形如 $xa...x'$ 而 $d$ 形如 $x...bx'$, 这样的相邻的 $c$ 和 $d$ 在内侧带来的 $x$ 与 $x'$ 一定会成对消去. 此时我们发现, $c = xax', d = xbx'$ 恰好是我们想要的构造. 故得证.

(2)

即要证 $\forall a, b \in G, aG'bG' = bG'aG'$. 由于 $G'$ 是正规子群, 我们可以将等式两端各自的第 2,3 项交换位置, 并且可以通过 $G'G' = G'$ 消去一个 $G'$. 故待证命题化为 $abG' = baG'$.

$a'b'ab \in G'$, 故 $ab \in baG'$. 故 $ab, ba$ 在同一个陪集中.

(3)

由于 $G'$ 是所有换位子及其有限乘积构成的集合, 我们可以试着只证明所有的换位子均在 $N$ 中, 从而证明 $N$ 含有 $G'$ 的全部元素.

由于 $abN = baN$, 可知 $a'b'abN = N$, 从而 $a'b'ab \in N$. 故证.

*p.s. 第 (3) 问实际上说明了: 如此定义的正规子群 $G'$ 是*最小的*能够使得 $G/N$ 为交换群的正规子群 $N$. 换言之, 任何做到这一点的正规子群 $N$ 都至少包含 $G'$.*

# 7 环和域

## 笔记

## 题解

### 7.1

和第 5 章的习题相同, 在证明一个代数系统是环时, 最回归定义的证法是证明它满足所有关于环的公理; 证明一个代数系统不是环, 也就是要指出至少一条被违背了的公理. 这个过程尽管琐碎, 但确实每个初学者不可跳过的一步.

(1) √

*(在这里我还是把每条性质都验证过去, 但每次验证中我会省略一些太平凡而繁琐的细节. 如果你正在参加你这门课的期末考试, 不要学我. )*

加封: 由自然加法在 $Z$ 上的封闭性易得;

加结: 由自然加法的结合律易得;

加幺: $(0,0)$;

加逆: $(a,b)$ 的逆为 $(-a,-b)$;

加交: 由自然加法的交换律易得;

乘封: 由自然乘法在 Z 上的封闭性易得;

乘结: 由自然乘法的结合律易得;

乘幺: $(1,1)$;

分配: 无论是左分配律还是右分配律 *(请注意: 在验证环时总是需要分别验证这两者! 无论你的方法是代入式子还是由乘法的交换律省去一些步骤)*, 都由自然乘法对自然加法的分配率易得.

(2) ×

如果你看完了 (1) 小问的解答, 应该能够意识到问题出在 $(1,1) \notin R$.

(3) ×

*(这种人为刻意定义的奇怪玩意大概率性质不好 $*2$)*

问题出在分配率: $(-1+2)\cdot 1 = |-1+2| \times 1 = 1 \times 1 = 1$.

但 $(-1)\cdot 1 + 2\cdot 1 = |-1| \times 1 + 2 \times 1 = 1 + 2 = 3$.

**7.2**

(1) 只有 1 和-1;

(2) 除了 0 以外的所有有理数;

(3) [1] 和 [3];

(4) [1] 和 [5].

*p.s.* 如果你有一些敏锐的洞察力, 应该能够观察出环 $Z_n$ 的可逆元似乎总是 $n$ 的缩系元素所在的那些同余类–实际上也容易证明的确如此.

**7.3**

如果 $R$ 是循环群, 那么你可以找到一个元素仅通过加法 $+$ 生成 $R$ 中的所有元素, 不妨命之为 $e$ (你不能直接将它命名为 1, 因为 "1" 这个符号在环的语境下有先在的含义–尽管在循环群的情况下 1 总是生成元之一, 你不妨试着证明这一点) .

任取 $a, b \in R, \exists i, j$ 使得 $a$ 为 $i$ 个 1 相加, $b$ 为 $j$ 个 1 相加 (由于乘号已经被占用过了, 这个式子难以用符号表示) . 我们要证明 $a \cdot b = b \cdot a$, 那么我们可以把 $a$ 和 $b$ 都表示成一大堆 1 的加和, 然后凭借分配率把括号拆开, 最后可见左右两式都是 $ij$ 个 1 相加.

**7.4**

(1)

(环中并没有天生的对 “2” 的定义. 这里的 “$2a$” 应该是朴素地指 $a+a$. )

由题设, $a+a=a^2+a^2$ (请注意为什么可以在这里使用 ‘2’ : 在环中, “i 次幂” 很自然地表示 $i$ 个自身做乘法, 与一般语境下保持一致; 但 “乘以 a” 却未必表示 $a$ 个自身相加, 尤其是当 $a$ 没有自然数的含义的时候) ; 但同样由题设, $a+a=(a+a)^2=a^2+a^2+a^2+a^2$.

由消去律得 $a^2+a^2=0$, 从而 $a+a=0$.

(2)

即要证明 $ab=ba$.

由 (1) 的结论我们有 $ab+ab=0$, 所以不妨试着证明 $ab+ba=0$.

如果你对平方差公式很敏感, 并且没有习惯于交换律 (在抽象代数中, 这是个坏习惯) , 可以立即联想到 $(a+b)(a+b)=a^2+ab+ba+b^2$. 由题设, 左侧, 以及右侧的首尾两项都是 0, 故二三两项之和也是 0. 此即所求证.

**7.5**

(1) 不是整环:

$(0,1)(1,0)=(0,0)$

(2) 是整环但不是域:

由于这里的乘法是朴素乘法, 显然非零元素相乘不会得到 0. 而 $\sqrt{2}$ 的逆为 $\frac{1}{\sqrt{2}}=\frac{\sqrt{2}}{2}$, 不在 $R$ 中.

(3) 是整环也是域. 整环理由同上, 只需证明域独有的两条公理:

乘逆: $a+b\sqrt{3}$ 的逆为 $\frac{1}{a+b\sqrt{3}}=\frac{(b\sqrt{3}-a)}{(3b^2-a^2)}$, 后者不存在当且仅当 $a=b=0$, 而这对应 $R$ 的零元. 由有理数的四则运算封闭性知该元素在 $R$ 中;

乘交: 由朴素乘法的...

### 7.6

(1)

*(这里 $-a$ 的定义应该是 $a$ 的加法逆元. )*

不妨命 $a$ 的乘法逆元为 $b$, 我们很自然地想到 $-a$ 的逆大概会是 $-b$, 所以试着证明 $(-a)(-b) = 0$.

请注意: 在这里你不能直接说 “根据负负得正, $(-a)(-b) = ab = 0$...” , 因为所谓 “负负得正” 是来自朴素乘法的概念, 在抽象代数的语境下我们不一定拥有所有关于数的公理, 这里负号的意义也未必与负数有什么关系. 我们只能从抽象代数的公理出发进行证明.

不过, 如果你在小学时自己证明过 $(-1)^2 = 1$, 大概很容易想到这里应该采取的处理: 取一个 $a(-b)$ 这样的元素作为中间元素. 主要凭借分配率, 我们有:

$ab + a(-b) = a(b + (-b)) = a * 0 = 0$

$(-a)(-b) + a(-b) = ((-a) + a)(-b) = 0(-b) = 0$

然后由加法的消去律即得.

(2)

如果 $a$ 是零因子, 意味着 $\exists c \neq 0 \ s.t. \ ac = 0$. 考虑 $bac$. 先做左侧的乘法得到 $bac = 1c = c \neq 0$; 但先做右侧得到 $bac = b0 = 0$. 矛盾.

*补充题: 如果你还没有自己证过, 请根据负数的定义证明 “负负得正”, 注意你实际上只需要证明 $(-1) \times (= 1) = 1$.*

*负数乘法的运算规则不是人为定义出来的, 而是自然推导出来的.*

**7.7**

由于 $ab$ 是零因子, $\exists c, d \neq 0\ s.t.\ abc = dab = 0$.

先看 $abc$, 考虑将其表示成 $a(bc)$. 由于 $ab$ 是零因子, 显然它不能是 0, 进而 $a$ 和 $b$ 分别也不是 0. 这意味着要么 $bc = 0$; 要么 $a$ 是左零因子且 $bc$ 是右零因子. 其中前者又意味着 $b$ 是左零因子且 $c$ 是右零因子. 换言之, 我们得到: $a$ 是左零因子或 $b$ 是左零因子.

$dab$ 同理, 我们可以得到: $a$ 是右零因子或 $b$ 是右零因子. 但这并不足以说明 $a$ 或 $b$ 是零因子, 因为 "$a$ 仅是左零因子且 $b$ 仅是右零因子" 这种状态同样满足上面两条性质, 而 $a, b$ 中没有任何一者是零因子.

此时我们惊喜地发现交换群这个条件还没有用上. 根据交换律我们可以得到 $acb = bca = 0$. 采取和上面类似的处理, 我们还可以得到 "$a$ 是左零因子或 $b$ 是右零因子" 与 "$a$ 是右零因子或 $b$ 是左零因子" 这两个命题. 如果你会用一点形式命题逻辑, 已经可以从这些条件推出 "$a$ 是零因子或 $b$ 是零因子" . 不过这里的情况很简单, 直接从直觉出发推理也不难:

为满足第一个命题, 需要 $a$ 与 $b$ 之一是左零因子. 由于目前 $a$ 与 $b$ 的地位完全对称, 不妨设它是 $a$. 此时第一, 三个命题已经被满足, 为使第二个命题成立, 要么 $a$ 是右零因子 (这意味着 $a$ 是零因子), 要么 $b$ 是右零因子. 而在后一种情况下我们还需要凑齐第四个命题: 要么 $a$ 是右零因子, 要么 $b$ 是左零因子. 无论哪种情况, $a, b$ 中都至少有一个零因子.

**7.8**

*($E$ 上的加法显然为两个映射在每个元素上的像对应相加; 乘法我猜测定义为 $(f \cdot g)(x) = f(g(x))$. )*

$E_H$ 显然是 $E$ 的子集, 故只需证明它是环:

加封: 由于 $f, g \in E_H$, 故 $f(x), g(x) \in H$. 由于 $H$ 是群, $f(x) + g(x) \in H$, 故 $f + g \in E_H$; *(可以看到, 在这里起关键作用的是 $H$ 的封闭性. 相应地, 如果 $H$ 是一个任意的子集, $E_H$ 很可能没有这么好的性质. )*

加结: 继承;

加幺: $f_0(x) = 0_G$ ($G$ 中加法的幺元) 显然是一个自同态, 而它是 $f$ 加法的幺元;

加逆: $f(x)$ 的逆即为 $f' : G \to G, f'(x) = -f(x)$; *(显然, $-f \in E_H$ 成立的根源也在于 $H$ 的逆)*

加交: 略;

乘封: 同上;

乘结: 映射的复合显然满足结合律;

乘幺: $I(x) = x$ ($G$ 上的恒等映射) 显然也是一个自同态, 而它是映射复合的幺元;

分配:

*(注意在环中乘法不一定有交换律, 因此分配率实际上意味着两条性质: 左分配律 f(g+h)=fg+fh, 以及右分配律 (f+g)h=fh+gh. 验证一个代数结构中分配率成立时必须分别验证两者.)*

根据定义, $(f(g + h))(x) = f(g(x) + h(x))$, 由于 $f$ 是同态从而保运算, 右侧 $= f(g(x)) + f(h(x))$.

而 $(fg + fh)(x) = f(g(x)) + f(h(x))$, 二者相等, 左分配律得证.

相比之下右分配律的证明是平凡的, 略.

**7.9**

命该环为 $R$, 其两个子环为 $R_1, R_2$, 交为 $R_3$:

加封: $\forall x, y \in R_1, R_2$, 有 $x + y \in R_1$ 且 $x + y \in R_2$, 故 $x + y \in R_3$;

加结: 从 $R$ 中继承;

加幺: $0 \in R_1$ 且 $0 \in R_2$, 故 $0 \in R_1 \cap R_2 = R_3$;

加逆: $\forall x \in R_1, R_2$, 有 $-x \in R_1$ 且 $-x \in R_2$, 故 $-x \in R_3$;

加交: 继承;

乘封: 同上;

乘结: 继承;

乘幺: 同上;

分配 (无论是左还是右) : 继承.

### 7.10

证明环同态:

没什么含金量, 自己做.

Ker$f$:

$Z$ 的零元是 0, 故 Ker 中的元素是形如 $(0, b)$ 的那些元素.

### 7.11

*这种题的一般适用做法是: 先确定群 $G$ 的所有子群, 再逐一检查每一个子群是否符合成环所需要的性质.*

$Z_6$ 的子群有: $\{0\}, \{0, 3\}, \{0, 2, 4\}, \{0, 1, 2, 3, 4, 5\}$, 而这些子群很幸运 (其实并不是巧合) 地都是环.

### 7.12

先证最后的结论:

任取 $i_1i_2 \in I_1I_2$. 由 $I_1$ 的乘法吸收性知 $i_1i_2 \in I_1$, 同理它 $\in I_2$. 故 $i_1i_2 \in I_1 \cap I_2$.

再证理想:

$\cap, +$ 的情况略. 我们只证 $I_1 \cdot I_2$:

减封:

任取 $i_1i_2, i_3i_4 \in I_1I_2$, 需证 $i_1i_2 - i_3i_4 \in I_1I_2$.

引入一个 $i_1i_4$ 以解决问题:

有 $i_1i_2 - i_1i_4 = i_1(i_2 - i_4) \in I_1I_2$, 亦有 $i_1i_4 - i_3i_4 = (i_1 - i_3)i_4 \in I_1I_2$, 故二者之和也 $\in I_1I_2$.

乘吸:

任取 $i_1i_2 \in I_1I_2, r \in R$, 考虑 $ri_1i_2 = (ri_1)i_2$. 由 $I_1$ 的吸收性质左部为 $I_1$ 的元素, 从而整体是 $I_1I_2$ 的元素. 由此左乘吸收性得证. 右乘同理.

### 7.13

理想:

减封: 任取 $i_1, i_2 \in I$, 显然 $i_1 - i_2 \in I$;

乘吸: 任取 $i = [[0, 2x], [0, 0]] \in I, r = [[a, b], [0, c]] \in R$, 则 $ir = [[0, 2cx], [0, 0]]$. 由整数乘法的封闭性, $cx \in Z$, 故 $ir \in I$. $ri$ 同理.

元素:

$r_1 - r_2 \in I$ 实际上在 $R$ 的矩阵中建立了这样一种等价关系: $a_1 = a_2$ 且 $b_1 - b_2$ 为偶数且 $c_1 = c_2$. 因此, 任何不满足这种等价关系的矩阵都将带来一个新的等价类. 换言之, 除了 $b$ 处的元素取值只有两种情况 (通常我们选取为 0 和 1) , $a$ 和 $c$ 中的任何一个发生改变都会产生一个新的等价类. 故有:

$R/I = \{[[a, 0], [0, c]], [[a, 1], [0, c]] | a, c \in Z\}$

**7.14**

I=(2+i) 中的元素实际上是所有具有形式 (a+bi)(2+i) 的整复数. 下面我们用两种方法来考虑哪些整复数具有这样的形式:

① 代数法

根据 $x+yi=(a+bi)(2+i)$ 得到 $x=2a-b, y=2b+a$.

故可知 $2x=4a-2b, 2x+y=5a\cong 0(\mathrm{mod}5)$. 同理可得 $2y-x\cong 0(\mathrm{mod}5)$

在这里, 很多初学者的直观想法是仿照解二元一次方程组的方法, 从这两个方程出发解出 $x$ 与 $y$ 所属的同余类来. 然而由此求出的解却是 $5x\cong 0(\mathrm{mod}5)$ $5y\cong 0(\mathrm{mod}5)$ 两个平凡的式子. 这难道说明所有的 $x+yi$ 都满足前文所述的性质? 但我们可以轻易地举出反例: 1 不能表示为 $(a+bi)(2+i)$ 的形式 (如果你列方程求出 $a$ 和 $b$, 会发现它们不是整数) .

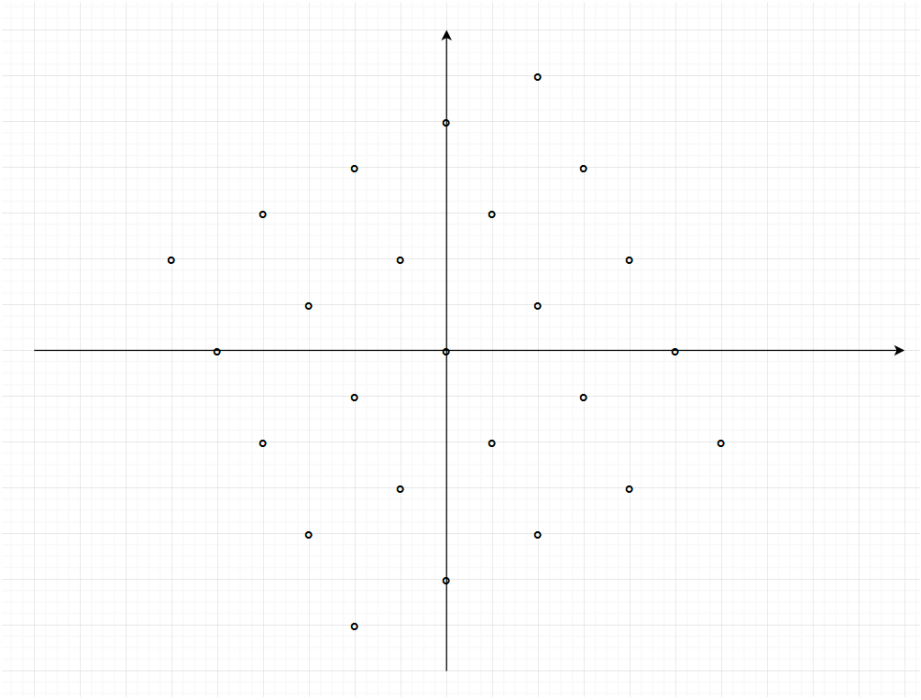
问题出在哪里呢? 实际上, 在我们从 $2x+y\cong 0(\mathrm{mod}5), 2y-x\cong 0(\mathrm{mod}5)$ 得到 $5x\cong 0(\mathrm{mod}5), 5y\cong 0(\mathrm{mod}5)$ 的过程中, 存在着信息的丢失. 这里作为条件的两个同余方程是不独立的 (恰恰相反, 它们完全等价, 从而只要其中任意一个就能提供另外一个提供的全部信息) . 用线性方程组的话说, 这样的方程组是 “不满秩” 的. 在第 2 章里我们学过如何求解解确定的一次同余方程组. 但 “不满秩” 同余方程组的处理方式, 以及我们能从中得到的尽可能精确的信息, 却与方程组的情况大不相同. 具体到这个问题, 我们只能确定 $2x+y\cong 0(\mathrm{mod}5)$ 这一点; 但 x 与 y 本身, 却可以取遍任何一种模 5 等价类甚至是任意一个整数.

② 几何直观

尽管代数法确切地告诉了我们 $I$ 中的元素有怎样的性质, 但我们还是很难想象它们在 $Z[i]$ 中处于怎样的位置, 而这会为后面研究商群元素带来不便. 所以我们换一种严谨性略有欠缺, 但理解起来直观的方法:

读者或许还记得一个关于复数乘法的性质: 对一复数乘以另一个复数, 等价于复平面上对应的点 (或者向量) 幅角相加, 模长倍增 (倍数等于第二个复数的模长) . 如果我们把 $Z[i]$ 中所有元素画在复平面上, 会得到一个无限延伸的网格 (就像一个无限路的围棋棋盘) . 把这个网格中的所有点乘以 $2+i$,

也就等于将所有点模长乘以 $\sqrt{5}$, 旋转一定角度 (我懒得算了) , 得到一个如下的新网格:

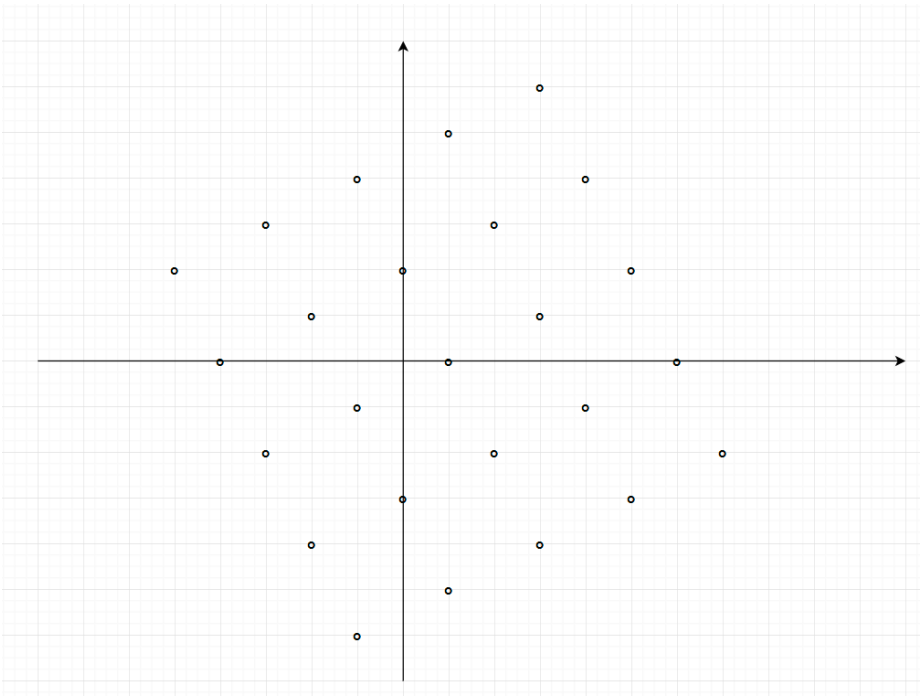


虽然这张简陋的图没有告诉我们 $I$ 中的点应该满足什么具体的式子, 但我们至少对它们的分布有了一些几何的直观认识. 如果你基于此求出它们的性质, 所得的结果应该与①代数法相同. 但它的真正作用在于研究商群的元素:

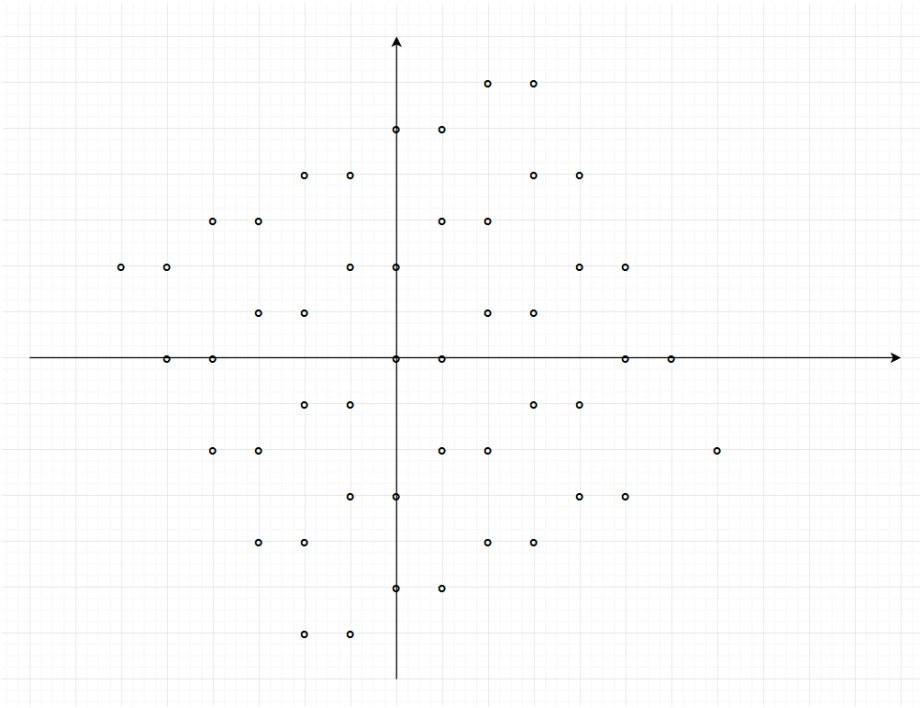
首先考虑一个问题: 商群中应该有多少个元素? 我们可以如此直观地想象: 由于新网格中所有距离被延长只 $\sqrt{5}$ 倍, 说明新网格的点的线密度应该是旧网格的 $\frac{1}{\sqrt{5}}$, 从而面密度是 $\frac{1}{5}$, 也就是说新网格的点的数量是旧网格的 $\frac{1}{5}$ (这样讨论两个无限集的数量非常不严谨, 你直观地理解就好) . 由于每个等价类 (陪集) 的元素数量应当相同 (这句话的严谨性也一样扯淡) , 可以想到应该有 5 个等价类.

为了写出这 5 个定价类, 我们只需要写出 5 个代表元 $a$ 就好 ($a$ 所属的等价类可以表示为 $[a] = a + I = \{(2 + i)z + a | z \in Z[i]\}$) . 你可以不停地随便选整复数作为 $a$, 然后检查它是否与已经被选出的元素等价, 如果等价就把它扔掉, 直到找到 5 个互不等价的元素为止. 但我们还有不那么愚蠢的方法:

我们取一个显然不属于 $I$ 的元素, 试试看它所属的等价类是什么样的. 以 1 为例, $1+I$ 对应的网格如下:

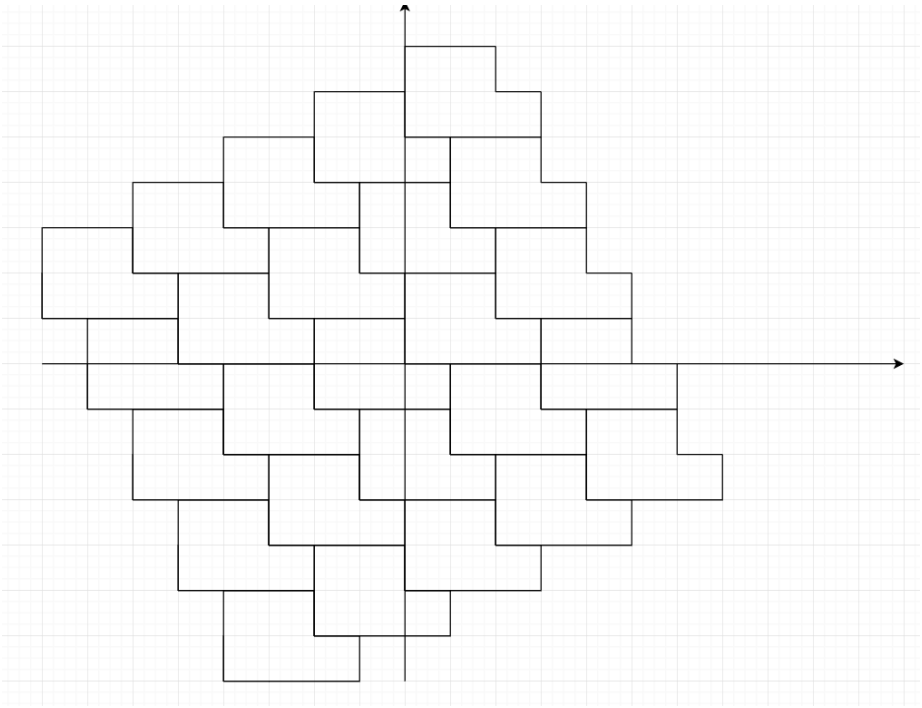


这看上去就是单纯把 y 轴往左移了 1 格. 所以我们把两个等价类同时放进来看:

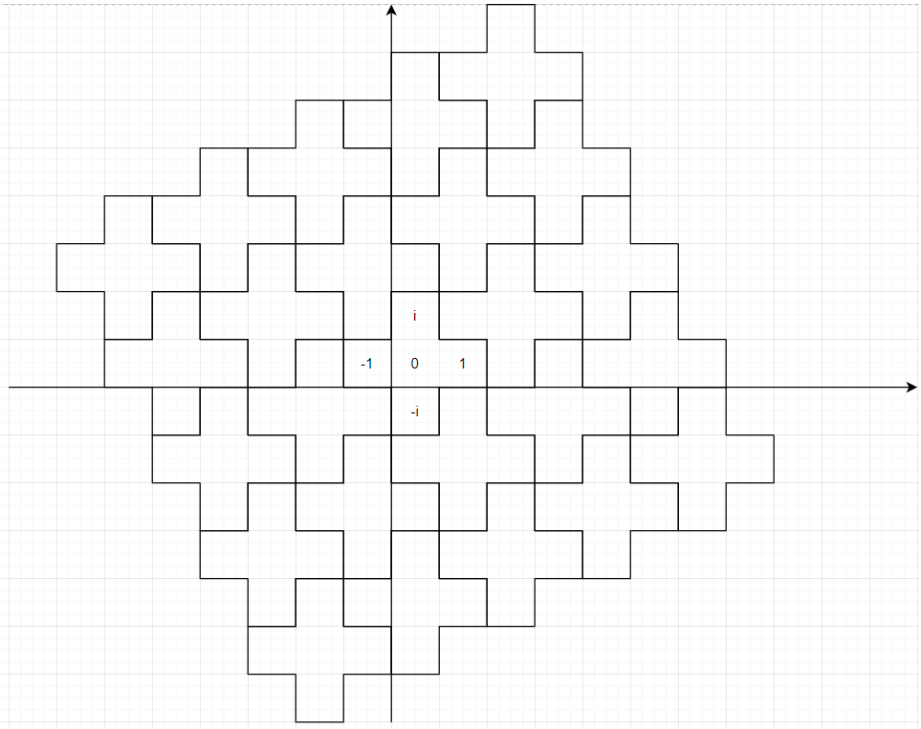


这样一看就直观多了! 可以看到, [1] 中的元素没有与 [0] 中的重合, 从而它的确是一个新的等价类. 如果我们选对了接下来 3 个等价类, $I$ 和它的 4 个副本将会铺满整个复平面上的所有整点, 不重也不漏. 换言之, 我们需要找到一块恰由 5 个单位正方形拼成的 “瓷砖” , 使得它通过 “右移 2 格上移 1 格” 与 “上移 2 格左移 1 格” 这两个操作可以循环地密铺整个复平面.

$(0,0)$ 到 $(2,1)$ 所成矩形中除去其中 $(2,1)$ 这一者恰好剩下 5 个元素, 我们据此猜测这 5 个元素所成的 “瓷砖” 可以密铺整个平面. 幸运的是, 它的确可以:



所以我们可以得出, $Z[i]/(2+i)$ 的一个表示是 $\{[0],[1],[2],[i],[1+i]\}$. 不过话说回来, 我个人更喜欢另一种更 “漂亮” 的密铺方法:




它对应的表示是 $\{[0],[1],[i],[-1],[-i]\}$.

### 7.15

这题比 *14* 简单多了，不知道为什么放在这里... 理想的证明过程略.

$R/I$ 的全部元素为 $\{\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} | a_{ij} \in \{0,1\} \}$.

### 7.16

注意这题旧纸质书的版本有笔误：“一次多项式环”应为“多项式环”. 实际上容易发现一个域上的所有一次多项式不构成环，因为这个集合违反了乘法封闭性：可以找到两个一次多项式的积是二次多项式.

这里 $(2,x)$ 表示用 $2$ 和 $x$ 两个元素所能生成的所有多项式.

$\forall f(x)\in(2,x)$, 存在多项式 $f_1(x),f_2(x)\in Q[x]$ $s.t.$ $f(x)=x\cdot f_1(x)+2\cdot f_2(x)$.

对于其中的第一项, $x\cdot f_1(x)=2\cdot\frac{xf_1(x)}{2}$, 后者是将 $xf_1(x)$ 的每一项的系数 $a_i$ 除以 2 得到的多项式, 由于 $Q$ 是一个域, $\frac{a_i}{2}$ 也是有理数, 从而该式也是一个 $Q$ 上的多项式.

因此 $f(x)$ 可以表示为 $2\cdot(\frac{xf_1(x)}{2}+f_2(x))$, 是一个可以由 2 生成的多项式. 这就证明了 $(2,x)\subseteq(2)$. 而 $(2)\subseteq(2,x)$ 是显然的 (只用 2 生成的多项式当然也可以由 2 和 $x$ 一同生成, 只需让 $f_1(x)=0$ 即可) , 这就证明了 $(2,x)=(2)$, 从而是主理想.

*p.s. 我不太理解这题想干什么: 显然任一域 $F$ 的多项式环 $F[x]$ 中, 任一零次多项式 $a\neq0$ 都可以生成整个 $F[x]$, 这是因为将任一多项式 $f(x)$ 除以 $a$ 后得到的多项式依然在 $F[x]$ 中. 具体到这道题, 2 可以生成整个 $F[x]$, 那么 2 和 $x$ 一起当然也可以, 即 $(2,x)$ 实际上就是 $Q[x]$. 问题是平凡的.*

### 7.17

我们逐一验证环定义所要求的每条性质: 由于 $\langle F[x],+,\cdot\rangle$ 中加法的结构不变, 因此我们不必再验证只涉及加法的那些性质.

乘封: 设 $f(x)=\sum_{i=0}^{n_f}a_ix^i, g(x)=\sum_{i=0}^{n_g}b_ix^i$, 则可以据此计算出 $f(g(x))$ *(这个式子完整写出来会很恶心所以我这里略过)* . 它的每项系数无非是 $F$ 中的两个元素相乘, 再将一些这样的乘积相加, 依然是 $F$ 中的元素, 因此它也依然是 $F$ 上的多项式. 成立;

乘结: 映射复合显然满足结合律;

乘幺: 恒同映射 $I_F(x)=x$ 无论在左边还是在右边都是映射复合的幺元;

分配: 考虑左分配律, 即 $f(g+h)=f(g)+f(h)$ 是否总是成立. 这实际上接近于要求 $f(x)$ 是线性的, 因此可以先考虑在非线性的多项式寻找反例. 实际上也很容易找到: 取零次多项式 $f(x)\equiv1$, 则无论 $g(x),h(x)$ 为何, 总有 $f((g+h)(x))=1$ 而 $f(g(x))+f(h(x))=1+1=2$. 从而左分配律不成立.

读者可以自行验证右分配律是否成立.

由此, $\langle F[x], +, \cdot \rangle$ 不是环, 因为它不满足左分配率.

*p.s.* 个人认为这题的题干不太严谨: 教材中并没有在多项式环的语境下定义过 $f(g(x))$. 由于在多项式环中多项式仅仅被定义为一个元素序列 (而非一般所说的多项式), 并不该直接按映射复合来理解这个符号.

### 7.18

计算题略.

### 7.19

充分性:

记奇数 $n = 2k + 1$, 则容易验证 $\sum_{i=0}^{n} x^i = (1 + x) \sum_{i=0}^{k} x^{2i}$, 后者也是一个 $Z_2$ 上的多项式.

必要性:

使用反证法: 充分性的部分给我们以启发: 对于偶数 $n = 2k$, 我们可以先考虑该多项式除常数项 1 以外的部分, 它满足 $\sum_{i=1}^{n} x^i = (1 + x) \sum ($ $1 + x)i = 1^k x^{2i-1}$, 即以 $1 + x$ 为因式. 如果整个式子也有因子 $1 + x$, 则必须有 $1 + x|1$.

设 $1 = (1 + x)f(x)$, 其中 $f(x) \in \mathbb{Z}_2[x]$ 显然不为 0, 故可以设其为 $n$ 次多项式 ($n \geq 0$), 首项系数为 $a_n \neq 0$. 则 $(1+x)f(x)$ 中 $n+1$ 次系数为 $1 \cdot a_n = a_n$ 不为 0, 其至少是 $n + 1$ 次多项式, 不可能等于零次多项式 1. 故原式 $\sum_{i=0}^{n} x^i$ 不以 $1 + x$ 为因式.

**7.20**

考虑任一 $\mathbb{Z} \to \mathbb{Z}$ 的环同态 $f$.

由于环同态映射保幺元, 必有 $f(1) = 1$. 再任取整数 $a \in \mathbb{Z}$:

① 若 $a$ 为正整数: 由于 $\mathbb{Z}$ 作为群时 1 是生成元, $Z$ 中正整数 $a$ 都可以表示为 $a$ 个 1 相加 *(注意这里两处 $a$ 含义的不同)*. 则可以将 $f(a)$ 中的 $a$ 如此表示. 又由 $f$ 是环同态, $f(a)$ 是 $a$ 个 $f(1)$ 相加, 也就是 $a$.

② 若 $a$ 为负整数: 则 $a$ 的加逆 $-a$ 是正整数, 满足 $f(a) = a$. 又由 $f$ 是环同态, $f(0) = f(-a + a) = f(-a) + f(a) = f(-a) + a = 0$. 故 $f(-a) = -a$.

③ 若 $a = 0$: $f(0) = 0$ 是环同态所蕴含的.

综上, $\mathbb{Z} \to \mathbb{Z}$ 只有一个环同态, 就是恒同映射 $I_{\mathbb{Z}}$. 其 Ker 为 $\{0\}$.

**7.21**

考虑任一 $\mathbb{Z}_2 \to \mathbb{Z}$ 的环同态 $f$.

由于 $f$ 是环同态, $\mathbb{Z}_2$ 中 $0_{\mathbb{Z}_2}$ 为零元, $1_{\mathbb{Z}_2}$ 为幺元, 故只能有 $f(0_{\mathbb{Z}_2}) = 0, f(1_{\mathbb{Z}_2}) = 1$. 但此时 $f(1_{\mathbb{Z}_2} + 1_{\mathbb{Z}_2}) = f(0_{\mathbb{Z}_2}) = 0$, 但 $f(1_{\mathbb{Z}_2}) + f(1_{\mathbb{Z}_2}) = 1 + 1 = 2$, 与 $f$ 是环同态矛盾.

故不存在 $\mathbb{Z}_2 \to \mathbb{Z}$ 的环同态.

**7.22**

难点完全在于读懂题意. 一步步根据定义弄清每一个对象后验证就好.

**7.23**

环同态的验证是平凡的. 注意这一命题在数论语言下的含义: 已知 $r|m$, 如果两个数在 mod$m$ 的意义下等价, 那么它们当然也在 mod$r$ 的意义下等价, 这种等价自然是保运算的.

根据定义, $\mathrm{Ker}f = \{\overline{a}|f(\overline{a}) = [0]\}$. 我们知道 $f(\overline{a}) = [a]$, 因此这一条件等价于 $[a] = [0]$, 即 $a \equiv 0(\mathrm{mod})r$. 记 $m = kr$, 则 $\{0, 1, \ldots, m-1\}$ 中被 $r$ 整除的恰有 $0, r, \ldots, (m-1)r$, 那么 $\mathrm{Ker}f$ 便恰好含有这些元素所在的等价类 $\overline{0}, \overline{r}, \ldots, \overline{(m-1)r}$. 注意: 这些等价类之并恰好就是所有被 $r$ 整除的整数, 也就是 $\mathbb{Z} \to \mathbb{Z}_r$ 的唯一群同态的核!

考虑商群 $Z_m/\mathrm{Ker}f$ 中的元素, 记其零元为 $\overline{\mathbf{0}} = \{\overline{0}, \overline{r}, \ldots, \overline{(m-1)r}\}$, 每个元素 $\overline{\mathbf{a}}$ 形如 $\{\overline{a}, \overline{r+a}, \ldots, \overline{(m-1)r+a}\}$, 其中 $a \in \{0, 1, \ldots, r-1\}$. 根据数论知识容易验证, 任取两个同余类 $\overline{k_1 r + a}, \overline{k_2 r + b}$, 其和为同余类 $\overline{(k_1+k_2)r + a + b}$, 属于等价类 $\overline{\mathbf{a+b}}$; 其乘积为同余类 $(k_1 k_2 r + k_1 b + k_2 a)r + ab$, 属于等价类 $\overline{\mathbf{ab}}$. 从而这个环同构于 $\mathbb{Z}_r$.

**7.24**

环同态的验证是平凡的, 只需注意到多项式乘法中对结果常数项有贡献的仅有两个多项式的常数项即可. 为说明是满同态, 只需为每个 $a \in R$ 找到一个原像, 可以直接选取 $f(x) = a$.

$\mathrm{Ker}\phi = \{f(x)|\phi(f(x)) = 0\}$, 故 $\mathrm{Ker}\phi$ 中的元素恰为所有常数项为 0 的多项式. 商环 $\mathbb{R}[x]/\mathrm{Ker}\phi$ 中, 每个等价类都是常数项为一个特定实数 $a$ 的全体多项式构成的集合, 不妨选取 $a$ 为其代表元, 则容易注意到其作为环同构于 $\mathbb{R}$ 本身 (验证是平凡的) .

**7.25**

(1)

分别验证两端的集合互相包含即可.

$I + \mathrm{Ker}\phi \subseteq \phi^{-1}(\phi(I))$:

任取 $a \in I + \mathrm{Ker}\phi$, 其可以表示为 $a = i + a_0$, 其中 $i \in I, a_0 \in \mathrm{Ker}\phi$. 由 $\phi$ 是环同态, 则 $\phi(a) = \phi(i + a_0) = \phi(a) + \phi(a_0) = \phi(a) + 0_{R_2} = \phi(a) \in \phi(I)$. 这就证明了 $a$ 在 $\phi(I)$ 的原像中.

$\phi^{-1}(\phi(I)) \subseteq I + \mathrm{Ker}\phi$:

任取 $a \in R_1$ 满足 $a \in \phi^{-1}(\phi(I))$, 则 $\phi(a) \in \phi(I)$, 即存在某个 $a_0 \in I$ 使得 $\phi(a) = \phi(a_0)$. 由于环对其加法构成交换群, 可以构造元素 $b \in R_1$ 使得 $a = a_0 + b$. 则有 $\phi(a) = \phi(a_0) + \phi(b) = \phi(a_0)$, 故 $\phi(b) = 0$ 即 $b \in \mathrm{Ker}\phi$. 这就证明了 $a \in I + \mathrm{Ker}\phi$.

(2)

$\Rightarrow$:

由条件有 $\phi^{-1}(\phi(I)) = \phi^{-1}(R_2) = R_1$.

又由 (1), 有 $\phi^{-1}(\phi(I)) = I + \mathrm{Ker}\phi$. 故证 $I + \mathrm{Ker}\phi = R_1$.

$\Leftarrow$:

由 (1), $\phi^{-1}(\phi(I)) = I + \mathrm{Ker}\phi = R_1$.

又由 $\phi$ 是满同态, $\phi(I) = \phi(\phi^{-1}(\phi(I))) = \phi(R_1) = R_2$.

*p.s.* 可以发现本题的证明过程里没有用到 $I$ 作为理想的任何性质. 实际上也的确如此: 这一命题对 $R$ 的任何子集 $A$ 都成立.

**7.26**

显然 $(n) = (-n)$, 所以下面我们只研究 $n \geq 0$ 的情况.

充分性:

① 若 $n = 0$, 则 $(n) = \{0\}$, $ab \in (0)$ 即 $ab = 0$, 当然蕴含 $a = 0$ 或 $b = 0$.

② 若 $n$ 为素数 $p$, 则 $ab \in (p)$ 即 $p|ab$. 根据数论知识有 $p|a$ 或 $p|b$.

必要性:

只需说明任取合数 $n$, 存在 $a, b$ 满足 $ab \in (n)$ 但 $a, b \notin (n)$. 由 $n$ 是合数, 可以表示为 $n = st$, 其中 $1 < s, t < n$. 取 $a = s, b = t$ 即可.

**7.27**

充分性:

反证法: 假定还有比 $(x, n)$ 更大的非平凡理想 $I \subset \mathbb{Z}[x]$.*

必要性:

若 $n$ 不为素数, 设 $n = ab$, 其中 $1 < a, b < n$*

# 8 格与布尔代数

## 笔记

## 题解

### 8.1

任取 $a, b \in R_1 = [0, 1]$, 则 $a, b$ 可比, 不妨设 $a \leq b$. 断言 $a, b$ 的最大下界是 $a$, 最小上界是 $b$.

显然 $a$ 是 $a, b$ 的下界. 假设还有更大的下界 $c$, 则 $c > a$, 不是 $a, b$ 的下界, 矛盾. 这就证明了 $a$ 是最大下界. 同理可证 $b$ 是最小上界.

故 $a * b = min\{a, b\}, a \oplus b = max\{a, b\}$.

### 8.2

(1) 根据定义这是显然的.

(2)

8.1 的过程中我们实际上得出了更强的结论: 如果在一个偏序结构中 $a \leq b$, 则 $a, b$ 的最大上界的最小下界分别就是 $a$ 和 $b$. 显然这的确是上/下界, 并且可以轻易地反正不存在比它更大/小的上下界. 这个结论并不依赖于偏序结构整体是否是全序集.

由此即证题给命题.

### 8.3

$a * c$ 是 $a, c$ 的最大下界, 从而有 $a * c \leq a \leq b$ 与 $a * c \leq c \leq d$ 成立, 因此它也是 $b, d$ 的下界, 自然小于 $b, d$ 的最大下界.

**8.4**

(1)

同 8.2, 我们已经证明了: $a \leq b$ 时 $a, b$ 的最大上界的最小下界分别是 $a$ 和 $b$. 故此时等式两端都是 $b$.

(2)

同理, $LHS = a \oplus b = b = b * c = RHS$.

**8.5**

(1)

左式是 $a * b$ 和 $c * d$ 的最小上界, 现需证右式大于等于左式, 等价于证明右式是 $a * b$ 与 $c * d$ 的一个公共上界, 即它同时大于等于 $a * b$ 与 $c * d$.

显然 $a \oplus c \geq a, b \oplus d \geq b$, 根据 8.3 可知 $(a \oplus c) * (b \oplus d) \geq a * b$. $c * d$ 的情况完全同理.

(2)

同 (1), 只需证明右式大于等于 $a * b, b * c$ 和 $c * a$. 以 $a * b$ 为例, 显然有 $a * b = a * b * a$, 其中每一项都小于等于 $(a \oplus b) * (b \oplus c) * (c \oplus a)$ 的对应位置中的项. 则根据 8.3 有 $a * b = a * b * a \leq (a \oplus b) * (b \oplus c) * (c \oplus a)$.

对于另外两者, 也可以类似地补一个在右式的剩下一项中涉及的元素, 在不改变自身的前提下证明小于等于右式.

**8.6**

题给命题实际上意味着 "任给两个可比元素 $a, b$, 一个格限制在 $a$ 和 $b$ 之间依然是格."

由于偏序关系限制在一个子集上依然是偏序关系, 我们只需要证明 $\langle B, \leq \rangle$ 中任意两个元素 $c, d$ 的最大下界与最小上界依然唯一.

考虑 $c, d$ 在原集合 $A$ 中的最大下界 $c*d$ 与最小上界 $c \oplus d$. 由于 $a \leq c, d \leq b$, 所以 $a, b$ 分别是 $\{c, d\}$ 在 $A$ 中的一个上界和一个下界, 因此 $a \leq c * d \leq c \oplus d \leq b$. 这就证明了 $c * d$ 和 $c \oplus d$ 也都在 $B$ 中, 从而在 $B$ 中它们依然分别是 $\{a, b\}$ 的上界和下界.

然后只需证明这两个界的最大/小性. 以 $a * b$ 为例, 假如在 $B$ 中有元素 $x$ 是 $\{a, b\}$ 的下界, 且 $x \not\leq a * b$, 则这件事在 $A$ 中也成立, 所以 $a * b$ 在 $A$ 中也不会是 $\{a, b\}$ 的最大下界, 矛盾. 这就证明了 $a * b$ 在 $B$ 中依然是 $\{a, b\}$ 的最大下界. $a \oplus b$ 的情况同理.

**8.7**

任取 $A$ 中元素 $a$, 则有 $0 \leq a \leq 1$. 如果 $0 = 1$, 则只能有 $a = 0 = 1$. 由 $a$ 任意性可知 $A$ 中只有一个元素 0.

**8.8**

略.

**8.9**

由 $a * a = a \oplus a = a$, 再结合 8.7 即可.

### 8.10

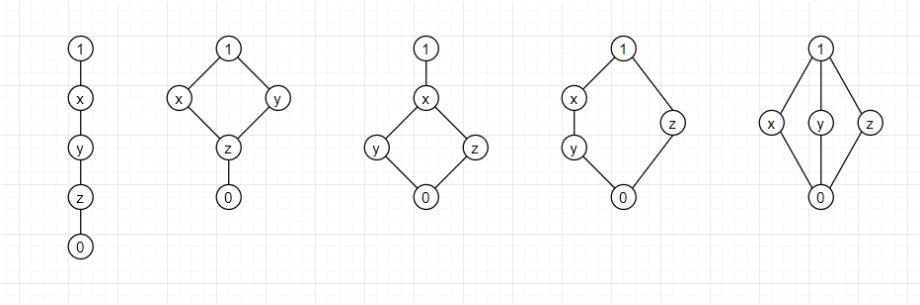
任取一个既不是 0 也不是 1 的元素 $a$. 对于任意一个元素 $b$, 由于 $A$ 是线性序集, $b$ 与 $a$ 一定可比. 若 $a \leq b$, 则 $a*b = a \neq 0$; 若 $b \leq a$, 则 $a \oplus b = a \neq 1$. 从而 $a$ 一定没有补元, $A$ 不是补格.

### 8.11

我们知道有限格必定是完全格, 而完全格必定是有界格, 故集合 $A$ 的元素中一定可以定义最大元 1 和最小元 0. 因此, 只要确定了另外三个元素的偏序结构, 整个格的结构就被完全确定.

严格地说, 这是因为定义一个偏序关系可以看作等价于给出其集合中每个有序二元组 $(a, b)$ 的比较结果 (大于等于/不大于等于). 现在我们已经知道了 0 和 1 与每个元素的比较结果, 只需要给出剩余三个元素内部的比较结果就确定了这个五元偏序关系.

在 4.14 中我们已经分类过所有不同构的 5 种三元偏序关系, 与之对应的 5 种五元有界偏序关系的 Hasse 图分别为:




利用 Hasse 图容易验证, 这 5 种五元有界偏序关系都是格, 只需要检查它们是否是分配格.

第 1 个格是线性序, 当然是分配格; 在第 4 个格中, 左侧的元素以右侧的两个元素为其补元, 补元不唯一, 故这个格不是分配格; 同理, 第 5 个格也不是分配格.

在第 2 个格中, 如果所取的 $a, b, c$ 形成线性的可比关系, 则当然满足分配律; 如果所取的 $a, b, c$ 并不构成线性序, 则一定是因为选到了两个不可比的元素 $x$ 和 $y$. 可以验证无论第三个元素如何选取, 以及三者的位置如何, 代入后都满足分配率. 故第 2 个格也是分配格. 第 3 个格的情况同理.

故五元分配格有图示的第 1,2,3 个五元格这三种.

*p.s.* 读者可以尝试对比此题的结论与定理 *8.14*.

### 8.12

必要性:

根据分配率, 可以写出:

$$\begin{aligned} LHS &= [(a \oplus (b * c)) * (b \oplus (b * c))] \oplus (c * a) \\ &= [((a \oplus b) * (a \oplus c) * b] \oplus (c * a) \\ &= [b * (a \oplus c)] \oplus (c * a) \\ &= (b \oplus (c * a)) * ((a \oplus c) \oplus (c * a)) \\ &= (b \oplus c) * (b \oplus a) * (a \oplus c) = RHS \end{aligned}$$

*p.s.* 整个过程无非是根据分配率不断打开括号. 这个过程看似很巧合, 但实际上有通俗得多的理解方式: 根据分配率, 左式完全展开的结果无非是在每个括号中取一项作 $\oplus$, 并将所有这样产生的项 (根据计数中的乘法原理易知共 *8* 项, 当然其中会有若干相同的) $*$ 起来. 会产生的项有 $a \oplus b, b \oplus c, c \oplus a$ 以及 $a \oplus b \oplus c$. 其中最后一项大于等于前几项, 故在求下界的过程中它不会产生任何贡献, 可以直接消去. 因此所有项的最大公共下界无疑就是 $(a \oplus b) * (b \oplus c) * (c \oplus a)$.

充分性:

我们观察如上展开过程, 可以看到整个展开中只使用了分配率中的 $(a * b) \oplus c = (a \oplus c) * (b \oplus c)$ 这一条. 如果现在没有分配格的条件, 则如上展开中的所有等号 $=$ 变为小于等于号 $\leq$.

现在条件告诉我们左右两式相等, 则每一处不等号都应该取等. 根据最后两行可知有 $b \oplus (a * c) = (b \oplus a) * (b \oplus c)$ 成立. 由 $a, b, c$ 选取的任意性, 我们实际上证明了 $A$ 中任一有序三元组 $(a, b, c)$ 满足这一点, 从而分配率得证.

**8.13**

(1)

根据定义有 $b * b' = 0$. 由于 $a \leq b$, $a$ 所有下界都比 $b$ 小 (从而是 $b$ 的下界) . 因此 $a$ 与 $b'$ 的最大下界也一定是 $b$ 与 $b'$ 的公共下界, 应当小于等于 $b * b' = 0$, 从而只能是 0.

(2)

与 (1) 同理.

**8.14**

$\langle \mathscr{P}(B), \subseteq \rangle$ 是格, 以及 $S \subseteq \mathscr{P}(B)$ 都是自然的. 需要证明的只是 $S$ 中任意两个元素的最大下界和最小上界存在.

任取 $S$ 中含有的子集 $B_1, B_2$, 我们知道 $B_1, B_2$ 在 $\mathscr{P}(B)$ 中的最大下界和最小上界即为 $B_1 \cap B_2$ 和 $B_1 \cup B_2$, 所以可以考虑证明 $B_1 \cap B_2$ 和 $B_1 \cup B_2$ 都在 $S$ 中.

由于 $B_1, B_2 \in S$, 可知存在 $A$ 的子集 $A_1, A_2$ 满足 $f(A_1) = B_1, f(A_2) = B_2$. 容易证明有 $f(A_1 \cap A_2) = B_1 \cap B_2$ 与 $f(A_1 \cup A_2) = B_1 \cup B_2$. 这就证明了 $B_1 \cap B_2, B_1 \cup B_2 \in S$, 也就给出了 $S$ 中任意两个元素的最大下界与最小上界.

**8.15**

首先验证 $f$ 的像在 $B$ 中. 任取 $A$ 中元素 $c$, 则 $a \oplus c, b \geq a$, 即 $a$ 是 $a \oplus c$ 与 $b$ 的公共下界, 故知 $(a \oplus c) * b \geq a$. 又显然有 $(a \oplus c) * b \leq b$, 从而 $(a \oplus c) * b \in B$.

然后验证 $f$ 保持运算结果. 任取 $A$ 中两个元素 $c, d$:

$$\begin{aligned} f(c * d) &= ((c * d) \oplus a) * b \\ &= (c \oplus a) * (d \oplus a) * b \\ &= [(c \oplus a) * b] * [(d \oplus a) * b] \\ &= f(c) * f(d) \end{aligned}$$

$$\begin{aligned} f(c \oplus d) &= (c \oplus d \oplus a) * b \\ &= ((c \oplus a) \oplus (d \oplus a)) * b \\ &= [(c \oplus a) * b] \oplus [(d \oplus a) * b] \\ &= f(c) \oplus f(d) \end{aligned}$$

故证 $f$ 是同构映射.

**8.16**

*

**8.17**

(1)

$a \oplus (a' * b) = (a \oplus a') * (a \oplus b) = 1 * (a \oplus b) = a \oplus b.$

(2)

与 (1) 同理.

**8.18**

由 $x \leq y$, 有 $x * y = x$. 对两端取补, 则有 $(x * y)' = x'$. 又 $(x * y)' = x' \oplus y'$, 故 $x'$ 是 $x'$ 与 $y'$ 的公共上界, 故有 $x' \geq y'$.

**8.19**

可以直接验证新的代数结构 $A_1 \times A_2$ 满足布尔代数定义中的若干性质. 但因为布尔代数与布尔格之间存在对应关系, 也可以直接证明 $A_1 \times A_2$ 作为格是有补分配格.

分配律的证明直接继承 $A_1$ 与 $A_2$ 内部的分配率即可. 对于有补性, 可以直接验证每个元素 $(a_1, a_2)$ 的补是 $(a_1', a_2')$.

**8.20**

这道题用的符号说实话不太好. $\mathscr{P}(A \cup B)$ 是一个集合的幂集, 其上的包含关系是确定的; 但 $\mathscr{P}(A) \times \mathscr{P}(B)$ 是两个幂集的笛卡尔积, 其中的每个元素都是有序二元组, 二元组中的元素分别是 $A$ 和 $B$ 的子集, 而我们并没有定义过两个有序组之间的包含关系 $\subseteq$. 当然这个定义实际上也很容易想到: 每个分量上分别满足包含关系.

符号看似互相嵌套非常纷繁, 但只需注意翻译每层符号的含义就不难找到思路. 考虑两个布尔代数的结构: $\mathscr{P}(A \cup B)$ 是一个集合的幂集上的包含关系, 其结构我们是熟知的. 对于 $\mathscr{P}(A) \times \mathscr{P}(B)$, 其中每个元素是 $A, B$ 各一个子集 $A_1, B_1$ 所成的有序组. 如何在两者间建立对应关系呢?

我们想到 $A, B$ 不交. 这意味着任取 $A \cup B$ 中的一个元素 $c$, 我们可以确定它来自 $A$ 与 $B$ 中的恰好一个, 否则 $A$ 与 $B$ 应有共同元素即交集非空. 进一步地, 任取 $A \cup B$ 的一个子集 $C_1$, 则其中的每个元素要么来自 $A$, 要么来自 $B$, 从而可以根据这一标准将 $C_1$ 划分为 $A_1 = C_1 \cap A$ 与 $B_1 = C_1 \cap B$. 容易验证这个划分是不重不漏的, 因此每个子集 $C_1$ 对应唯一一个子集二元组 $(A_1, B_1)$.

由于这个双射非常自然, 我们当然会考虑它是否就是同构映射. 验证也十分简单, 联想到一个布尔代数总是对应着一个布尔格, 只需验证这两个布尔格作为偏序关系同构即可, 即只需验证保持包含关系. 而这是自然的.