代数结构笔记 & 题解

Eastwind

目录

1 集合 **3**
笔记 3
题解 4

2 数论初步 **11**
笔记 11
题解 12

3 映射 **26**
笔记 26
题解 27

4 二元关系 **34**
笔记 34
题解 35

5 群论初步 **44**
笔记 44
题解 45

6 商群 **55**
笔记 55
题解 56

7 环和域 **64**
笔记 64
题解 65

8 格与布尔代数 **79**

1 集合

笔记

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.

2 数论初步

笔记

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.

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_{i}9999... 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 γ;

逆元: β 的逆元是自身, α 和 σ 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

⇒:

显然.

⇐:

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 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 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 $gH \subseteq gH_1 = H_1g$, 同理 $gH \subseteq H_2g$. 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_1H_2:

子群:

封: 任取 h_1h_2, 由 H_1 正规性知存在 $h \in H_1$ 使得 $h_1h_2 = h_2h$. 故有 $h_{11}h_{21}h_{12}h_{22} = h_{11}h_{13}h_{21}h_{22} = h_1h_2 \in H_1H_2$;

幺: $1 \in H_1$ 且 $1 \in H_2$, 故 $1 = 1 * 1 \in H_1H_2$. 由 1 是 G 的幺元可知它也是 G 任意子集的幺元;

逆: 任取 h_1h_2, 其在 G 中的逆为 $h_2'h_1' \in H_2H_1$, 而由任一 H_i 正规性可知这 H_1H_2 中的元素.

正规性: 任取 $a \in G$, 考虑 aH_1H_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 的地位完全对等, 我们不妨设这个倒霉蛋是 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:

$(f(g+h))(x) = f(g(x)+h(x))$, 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 $i_1 i_2 \in I_1 I_2$. 由 I_1 的乘法吸收性知 $i_1 i_2 \in I_1$, 同理它 $\in I_2$. 故 $i_1 i_2 \in I_1 \cap I_2$.

再证理想:

$\cap, +$ 的情况略. 我们只证 $I_1 \cdot I_2$:

减封:

任取 $i_1 i_2, i_3 i_4 \in I_1 I_2$, 需证 $i_1 i_2 - i_3 i_4 \in I_1 I_2$.

引入一个 $i_1 i_4$ 以解决问题:

有 $i_1 i_2 - i_1 i_4 = i_1(i_2 - i_4) \in I_1 I_2$, 亦有 $i_1 i_4 - i_3 i_4 = (i_1 - i_3) i_4 \in I_1 I_2$, 故二者之和也 $\in I_1 I_2$.

乘吸:

任取 $i_1 i_2 \in I_1 I_2, r \in R$, 考虑 $r i_1 i_2 = (r i_1) i_2$. 由 I_1 的吸收性质左部为 I_1 的元素, 从而整体是 $I_1 I_2$ 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) .

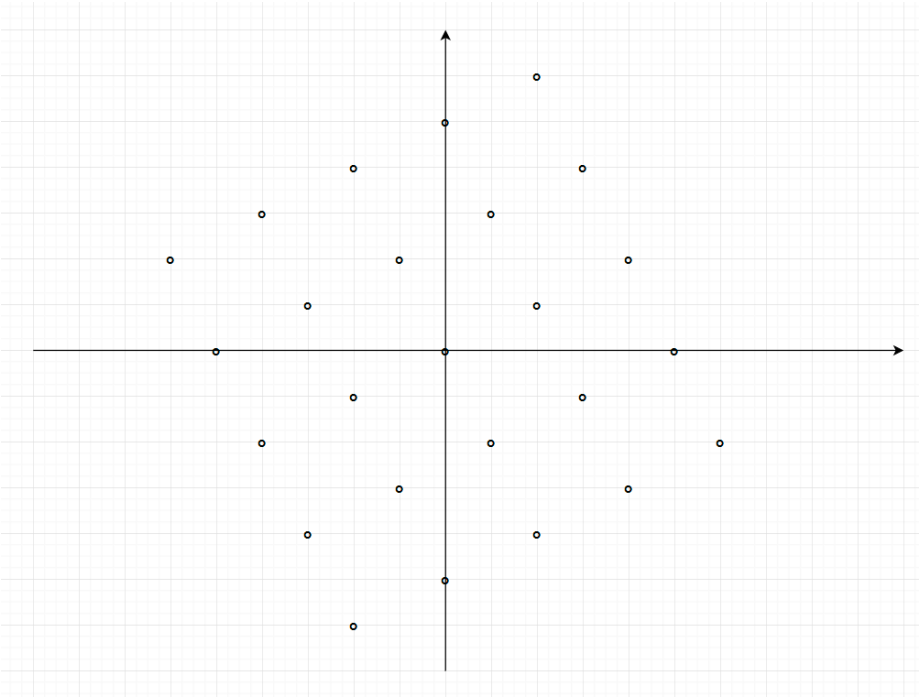
问题出在哪里呢? 实际上, 在我们从 $2x+y\cong 0(\mathrm{mod}5), 2y-x\cong 0(\mathrm{mod}5)$ 得到 $5x\cong 0(\mathrm{mod}5), 5y\cong 0(\mathrm{mod}5)$ 的过程中, 存在着信息的丢失. 这里作为条件的两个同余方程是不独立的 (恰恰相反, 它们完全等价, 从而只要其中任意一个就能提供另外一个提供的全部信息) . 用线性方程组的话说, 这样的方程组是 “不满秩” 的. 在第 2 章里我们学过如何求解解确定的一次同余方程组. 但 “不满秩” 同余方程组的处理方式, 以及我们能从中得到的尽可能精确的信息, 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:

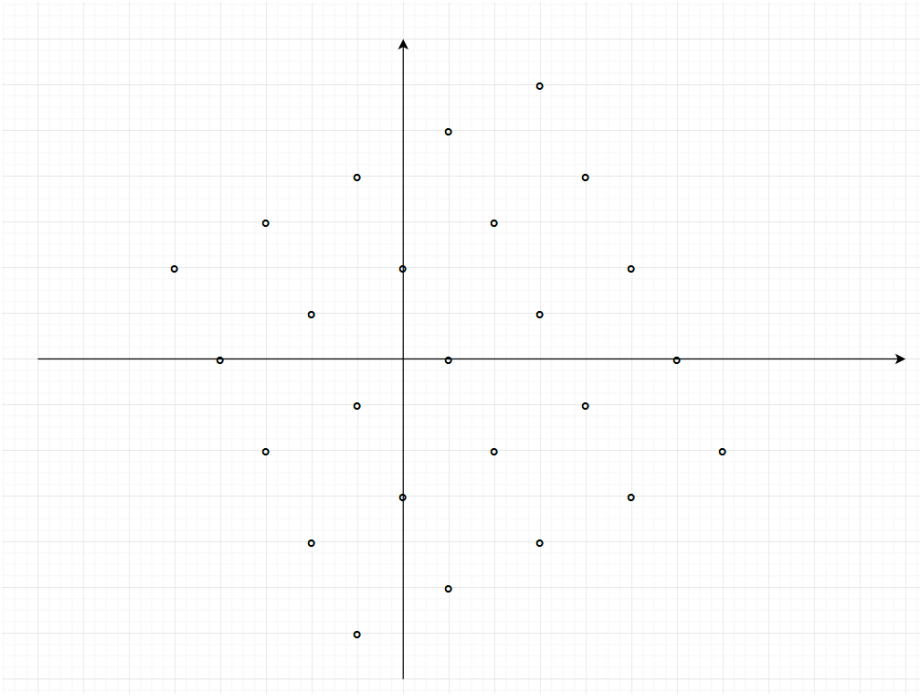


虽然这张简陋的图没有告诉我们 I 中的点应该满足什么具体的式子, 但我们至少对它们的分布有了一些几何的直观认识. 如果你基于此求出它们的性质, 所得的结果应该与①代数法相同. 但它的真正作用在于研究商群的元素:

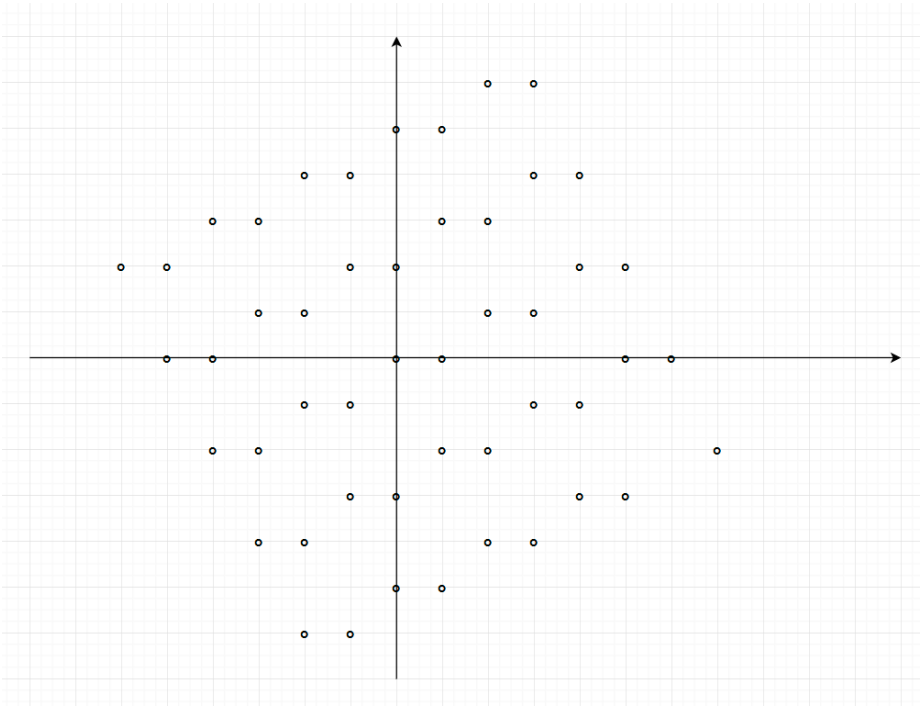
首先考虑一个问题: 商群中应该有多少个元素? 我们可以如此直观地想象: 由于新网格中所有距离被延长只 $\sqrt{5}$ 倍, 说明新网格的点的线密度应该是旧网格的 $\frac{1}{\sqrt{5}}$, 从而面密度是 $\frac{1}{5}$, 也就是说新网格的点的数量是旧网格的 $\frac{1}{5}$ (这样讨论两个无限集的数量非常不严谨, 你直观地理解就好) . 由于每个等价类 (陪集) 的元素数量应当相同 (这句话的严谨性也一样扯淡) , 可以想到应该有 5 个等价类.

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:

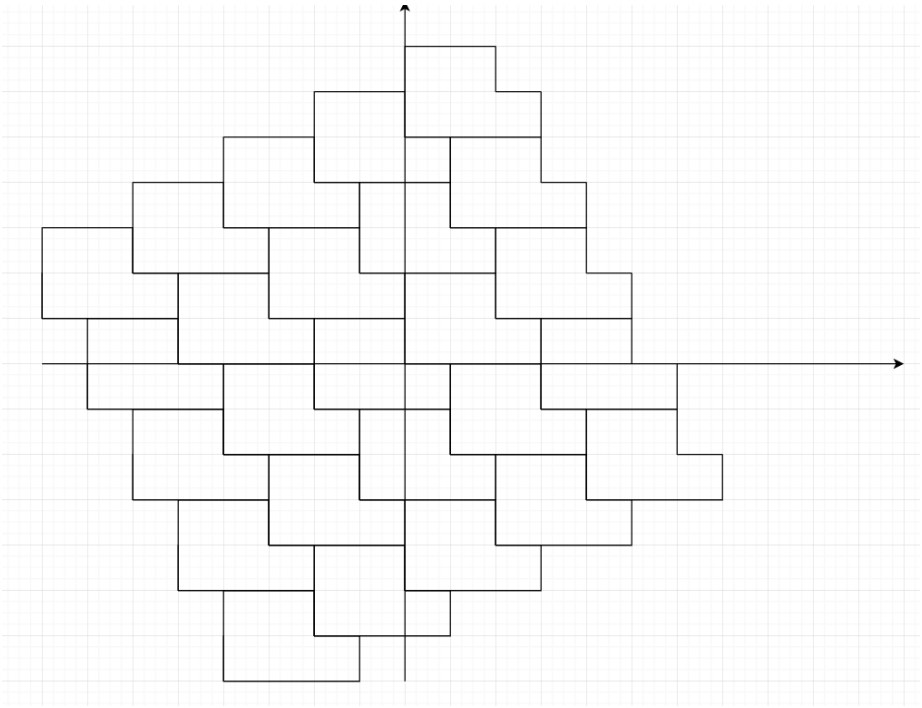


这看上去就是单纯把 y 轴往左移了 1 格. 所以我们把两个等价类同时放进来看:

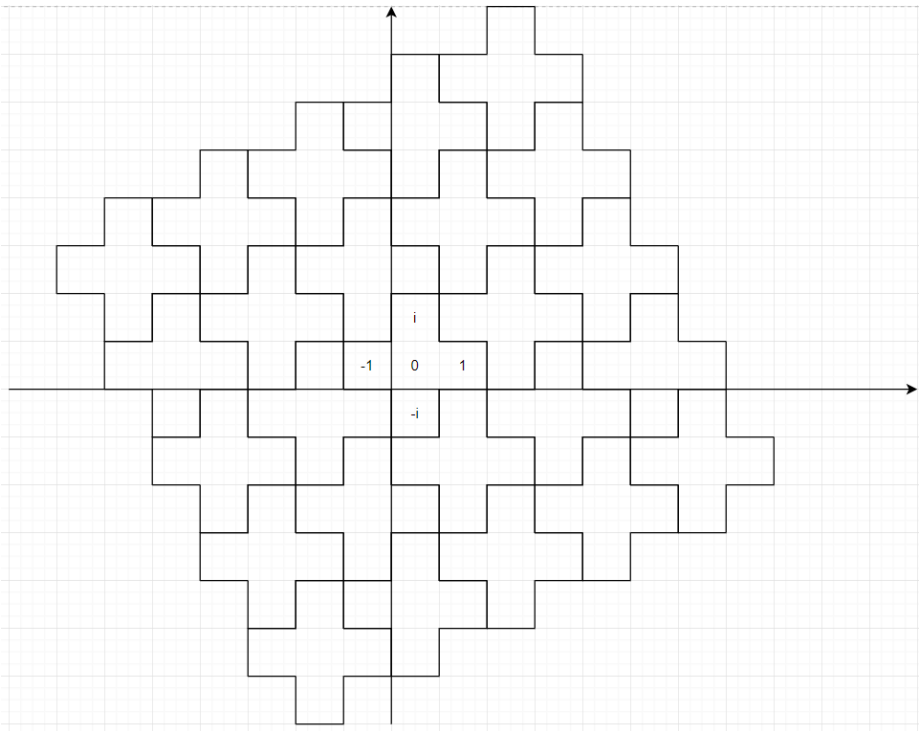


这样一看就直观多了! 可以看到, [1] 中的元素没有与 [0] 中的重合, 从而它的确是一个新的等价类. 如果我们选对了接下来 3 个等价类, I 和它的 4 个副本将会铺满整个复平面上的所有整点, 不重也不漏. 换言之, 我们需要找到一块恰由 5 个单位正方形拼成的 “瓷砖” , 使得它通过 “右移 2 格上移 1 格” 与 “上移 2 格左移 1 格” 这两个操作可以循环地密铺整个复平面.

$(0,0)$ 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 $\{[[x,y],[z,w]]|x,y,z,w\in\{0,1\}\ \}$.

8 格与布尔代数