代数结构 历年期末答案

Eastwind

2018 期末

1

(1)

原方程等价于 $3x-2y=1$, 故有 $3x\equiv 1(\mathrm{mod}2)$, 解得 $x\equiv 1(\mathrm{mod}2)$. 故原方程有解的必要条件是 $x\equiv 1(\mathrm{mod}2)$.

设 $x=2k+1(k\in\mathbb{Z})$, 代回上述方程有 $y=3k+1(k\in\mathbb{Z})$, 显然对于任意 $k\in\mathbb{Z}$, 如此表示的 y 都是整数. 故原方程有解的充分条件是 $x\equiv 1(\mathrm{mod}2)$, 且此时对于每个不同的整数 x, 恰好有一个整数 y 使得 (x,y) 是原方程的解.

综上, 原方程的整数解恰有 $x=2k+1, y=3k+1(k\in\mathbb{Z})$.

(2)

归纳定义:

① 若 $x\in\Sigma$, 则 $x\in\Sigma^+$;

② 若 $x\in\Sigma^+, a\in\Sigma$, 则将 a 添加在字符串 x 左侧得到的新字符串 $ax\in\Sigma^+$;

③ 集合 Σ^+ 中只包含有限次使用①和②得到的那些元素.

Σ^+ 可数, 证明如下:

考虑 Σ^+ 中长为 n 的全体字符串构成的子集, 记为 Σ_n^+. 易证 Σ_n^+ 均为有限集且两两不交, 故 Σ^+ 为可数多个 (非空) 有限集的不交并, 是可数集.

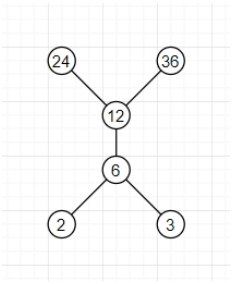
2

由题可知 $8x-12\equiv 0(\mathrm{mod}22)$ 即 $4x\equiv 6(\mathrm{mod}11)$,$x\equiv 1(\mathrm{mod}7)$.

所以有 $28x\equiv 42(\mathrm{mod}77), 11x\equiv 11(\mathrm{mod}77)$. 作差得 $17x\equiv 31(\mathrm{mod}77)$, 解得 $x\equiv 29(\mathrm{mod}77)$.

3

(1)



(2)

极大元, 最大元: 12;

极小元: 2, 3;

有多于一个极小元, 故没有最小元;

最大下界: 无;

最小上界: 12.

4

(1)

$$\begin{array}{ccccc} 1 & \to & 3 & \to & 3 \\ 2 & \to & 2 & \to & 4 \\ 3 & \to & 4 & \to & 1 \\ 4 & \to & 1 & \to & 2 \end{array}$$

所以 $(124)(134) = (13)(24)$.

(2)

① 先证明 $\{(12),(134)\}$ 可以生成任一对换:

$(134)^2=(143)$, 故可以生成 (143).

$(143)(12)(134)=(42),(134)(12)(143)=(32)$, 这样就生成了所有含有 2 的对换.

对于任一对换 (ab), 可以用 $(2a)(2b)(2a)=(ab)$ 生成对换 (ab), 这样就生成了所有对换.

② 再证明全体对换可以生成任一置换:

写出该置换的轮换积表示, 并将其中所有长度超过 2 的轮换分解为若干连锁轮换 $((ab)(bc)(cd)\dots)$ 的积即可.

5

水题.

6

设有群同态 $f:G_1\to G_2$, 其中 G_1 为循环群. 显然只用考虑 G_2 中 f 的值域 $H=f(G_1)$.

先证 H 是群:

封闭性: 任取 H 中元素 b_1,b_2, 则有 $a_1,a_2\in G$ 满足 $f(a_1)=b_1,f(a_2)=b_2$. 从而 $b_1b_2=f(a_1)f(a_2)=f(a_1a_2)$, 其中 $a_1a_2\in G_1$, 故 $b_1b_2\in H$;

结合律: 继承自 G_2;

幺元: 任取 G 中元素 a, 则 $f(a)=f(ae_{G_1})=f(a)f(e_{G_1})$, 由消去律可得 $f(e_{G_1})=e_{G_2}$. 故 $e_{G_2}\in H$;

逆元: 任取 H 中元素 b_1, 则有 $a_1 \in G$ 满足 $f(a) = b$, 则 $f(e_{G_1}) = f(aa') = f(a)f(a') = bf(a')$, 由消去律可得 $f(a') = b'$, 故 $b' \in H$.

再证 H 是循环群, 即 H 可以靠单个元素生成:

取 G_1 一生成元 a, 则 G_1 中任一元素可表示为 a^k ($k \in \mathbb{Z}$). 任取 H 中元素 b_1, 则 b_1 在 G_1 中有至少一个原像 a_1. 设 a_1 可表示为 a^{k_0}, 则 $b_1 = f(a_1) = f(a^{k_0}) = f(a)^{k_0}$, 从而 $f(a)$ 是 H 的生成元.

这就证明了 H 是循环群.

7

(1)

显然这题需要假定 G 是有限群.

先证 G 是交换群:

任取 $a, b \in G$, 则 $aabb = a^2b^2 = e$, 而 $abab = (ab)^2 = e$, 由消去律可得 $ab = ba$.

由于 G 是有限群, 可以任取 G 的一个极小生成组 $A = \{a_1, \ldots, a_m\}$, 则 G 中所有元素可以表示为 a_i 的有限连乘.

由于 G 是交换群, 可以通过交换元素顺序将相同的 a_i 交换到一起乘起来, 所以 G 中任一元素 a 可以表示为 $\prod_{i=1}^{m} a_i^{k_i}$. 又因为所有元素阶为 2, 可知每个 k_i 只能取 1 或 0, 即总共只有 2^m 种不同表示. 最后, 如果存在两个不同表示对应相同的元素, 则说明某个 a_i 可以用其它 a_j 生成, 与 A 是极小生成组矛盾. 从而这 2^m 个表示对应的元素各不相同. 即恰有 2^m 个元素.

(2)

封闭性: 由 $*$ 与 $\oplus$ 的封闭性即得;

结合律, 交换律: 取 A 的一组原子 $A_0 = \{a_1, \ldots, a_m\}$, 我们知道 $A \cong \langle \mathscr{P}(A_0), \subseteq \rangle$, 此时 A 的每个元素 a 对应 $\mathscr{P}(A_0)$ 的一个子集. 此时 $a * b'$

对应交集 $a\cap b^C$ 即补集 $a-b$, 故 $a+b$ 即对应对称差 $a\triangle b$. 而求多个子集的对称差, 意味着求恰好属于这些子集中的奇数个的全体元素构成的集合, 显然与子集排列顺序与运算顺序都无关.

幺元, 逆元: 同上理, 对称差运算的幺元为空集 $\emptyset$

这就证明了 $\langle\mathscr{P}(A_0),\triangle\rangle$ 是交换群, 从而 $\langle A,+\rangle$ 是交换群.

(3)

任取子集 $a\in\mathscr{P}(A_0)$, 其与自身取对称差为 $a\triangle a=\emptyset$, 即证 $\langle A,+\rangle$ 所有元素阶为 2.

由 (1)(2) 结论即得.

8

任取 $a\in R$, 有 $2a=(a+a)=(a+a)^2=4a^2=4a$, 由加法消去律得 $a+a=0$.

任取 $a,b\in R$, 有 $a^2+b^2=a+b=(a+b)^2=a^2+ab+ba+b^2$, 由加法消去律得 $ab+ba=0$, 结合 $ab+ab=0$ 得 $ab=ba$, 即 R 是交换环. 故所有左零因子都是右零因子 (反之亦然) , 即只需证有左零因子.

我们知道 $a^2-a=(a-1)a=0$, 由于 $|R|\geq 3$, 可以取到一个 0 和 1 以外的元素 a, 则 $a,a-1\neq 0$, 从而 $a-1$ 是左零因子, 进而也就是零因子.

2019 期末

1

① 记数列 $a_n = 2^n - n$. 2 在 mod3 同余乘法下阶为 2, 故第一项所属的 mod3 同余类每 2 项循环一次; 显然第二项所属的 mod3 同余类每 3 项循环一次, 可知这个数列本身所属的 mod3 同余类至多每 6 项循环一次. 枚举检验可知 $n \equiv 4$ 或 $5(\mathrm{mod}6)$.

同理, ②意味着 $n \equiv 7$ 或 13 或 14 或 $16(\mathrm{mod}20)$, ③意味着 $n \equiv 1(\mathrm{mod}2)$. 所以可以求 n 在 mod60 下的同余类. 验证可得 $n \equiv 47(\mathrm{mod}60)$.

所以最小的正整数 n 为 47.

2

根据中国剩余定理, 由于 a, b 互素, 命题等价于 $a^m + b^n \equiv 1(\mathrm{mod}a)$ 且 $a^m + b^n \equiv 1(\mathrm{mod}b)$. 后者又等价于 $b^n \equiv 1(\mathrm{mod}a)$ 且 $a^m \equiv (\mathrm{mod}b)$. 显然取 $m = \phi(b), n = \phi(a)$ 即可.

3

(1)

$$
\begin{array}{ccccc}
1 & \to & 4 & \to & 1 \\
2 & \to & 3 & \to & 3 \\
3 & \to & 2 & \to & 4 \\
4 & \to & 1 & \to & 2
\end{array}
$$

(2)

所给置换表示为轮换积为 $(146)(253)$. 我们知道 n-轮换的阶为 n, 且不交置换的乘法满足交换律. 故原式 $=[(146)(253)]^3=(146)^3(253)^3=I$.

4

(1)

水题.

(2)

等价类共有 2 个: 正奇数集, 正偶数集.

5

(1)

R_1: 不自反性, 反对称性;

R_2: 自反性, 对称性, 传递性;

(2)

$R_1\circ R_2$: 略.

$R_1^+=A^2$. 因为 $(a,b),(b,c),(c,d),(d,a)$ 构成了所有元素上的有向圈, 任意两个元素的有序组 (x,y) 都可以通过它们根据传递性生成;

R_2^+ 就是 R_2 自身, 因为 R_2 已经满足传递性.

6

(1)

封闭性: 任取 $h_1k_1, h_2k_2 \in HK$, 则 $(h_1k_1) * (h_2k_2) = (h_1(k_1h_2))k_2 = (h_1(h_2k_1))k_2 = (h_1h_2)(k_1k_2) \in HK$;

结合律: 从 S 中继承;

幺元: 取 H, K 中单位元 e, 则 $e = e * e \in HK$. 任取 $hk \in HK$, 则 $e * (hk) = (e * h)k = hk, (hk) * e = h(k * e) = hk$, 从而 e 是 HK 中运算 $*$ 的幺元;

逆元: 任取 $hk \in HK$, 记 h 在 $\langle H, * \rangle$ 中逆元为 h_H^{-1}, k 在 $\langle K, * \rangle$ 中逆元为 k_K^{-1}, 有 $h_H^{-1}k_K^{-1} \in HK$. 则 $(hk)(h_H^{-1}k_K^{-1}) = (h(kh_H^{-1}))k_K^{-1} = (h(h_H^{-1}k))k_K^{-1} = (hh_H^{-1})(kk_K^{-1}) = e * e = e$, 同理可以检验 $(h_H^{-1}k_K^{-1})(hk) = e$. 从而 hk 的逆元是 $h_H^{-1}k_K^{-1}$.

(2)

任取 $h \in H$, 则 $h = he \in HK$, 也就意味着 $H \subseteq HK$. 又 H 对于 $*$ 构成群, 故 H 是 HK 的子群.

考虑 H 的所有右陪集 (包括自身) , 我们断言每个右陪集中恰有一个元素属于 K.

先证每个右陪集中含有元素属于 K: 对 H 的任一右陪集, 任取其中一个元素 h_1k_1, 则这个右陪集可以表示为 Hk_1, 从而至少含有 k_1 这个 K 中的元素.

再证每个右陪集中不能有多于一个属于 K 的元素: 如果 k_1, k_2 属于 H 的同一个右陪集, 则这个右陪集可以表示为 Hk_1, 从而存在 h 满足 $hk_1 = k_2$ 即 $h = k_2k_1^{-1}$. 右侧是一个 K 中的元素, 且由于 $k_1 \neq k_2$ 故不是 e, 这与 H, K 除了幺元不交矛盾.

由此我们知道, H 的每个右陪集恰有一个 K 中的元素, 这说明 H 的每个右陪集恰好是每个 Hk, 其中 $k \in H$. 现在只需证明 $\forall k \in K, Hk = kH$, 而这可以根据 h 与 k 乘法的交换律得到.

这就证明了 H 是正规子群, K 的情况完全对称.

(3)

我们断言 $f : K \to G/H, f(k) = Hk$ 是二者间的同构映射. 证明如下:

根据 (2) 我们已经知道商群 G/H 中的元素恰好是所有的 Hk, 故 f 首先是一个双射. 任取两个陪集 Hk_1, Hk_2, 则有 $Hk_1 * Hk_2 = H(k_1H)k_2 = H(Hk_1)k_2 = (HH)(k_1k_2) = H(k_1k_2)$. 这就证明了 f 是一个同态映射. 综上 f 是同构映射.

7

先证 H 是子群:

封闭性: 任取 $h_1, h_2 \in H$, 需要证明 h_1h_2 也是与 G 中所有元素可交换的元素. 任取 $a \in G$, 则 $a(h_1h_2) = (ah_1)h_2 = (h_1a)h_2 = h_1(ah_2) = h_1(h_2a) = (h_1)(h_2)a$, 即 h_1h_2 与 a 可交换. 由 a 任意性可知 $h_1h_2 \in H$;

结合律: 从 G 中继承;

幺元: 取 G 中幺元 e, 则任取 $a \in G$, 有 $ae = ea = a$ 即 e 与任意元素可交换, 故 $e \in H$;

逆元: 任取 $h \in H$, 需要证明 h^{-1} 也是与 G 中所有元素可交换的元素. 任取 $a \in G$, 则 $h^{-1}a = (h^{-1}a)(hh^{-1}) = (h^{-1}(ah))h^{-1} = (h^{-1}(ha))h^{-1} = ((h^{-1}h)a)h^{-1} = ah^{-1}$, 即 h^{-1} 与 a 可交换.

再证 H 的正规性:

任取 $a \in G$, 则 $aH = ah|h \in H = ha|h \in H = Ha$.

这就证明了 H 是 G 的正规子群.

8

加封: 由自然加法和自然减法在 $\mathbb{R}$ 上的封闭性可得;

加结: 任取 $x, y, z \in \mathbb{R}$, 有 $(x \oplus y) \oplus z = (x + y - 1) \oplus z = x + y + z - 2 = x \oplus (y + z - 1) = x \oplus (y \oplus z)$;

加幺: 断言 $1 \in \mathbb{R}$ 是 $\oplus$ 的单位元. 任取 $x \in \mathbb{R}$, 有 $1 \oplus x = 1 + x - 1 = x, x \oplus 1 = x + 1 - 1 = x$;

加逆: 任取 $x \in \mathbb{R}$, 断言 $2 - x$ 是 x 关于 $\oplus$ 的逆元. 因为有 $x \oplus (2 - x) = x + 2 - x - 1 = 1, (2 - x) \oplus x = 2 - x + x - 1 = 1$;

加交: 显然;

乘封: 由自然加法, 自然减法和自然乘法在 $\mathbb{R}$ 上的封闭性可得;

乘结: 任取 $x, y, z \in \mathbb{R}$, 有 $(x \otimes y) \otimes z = (x + y - xy) \otimes z = x + y + z - xy - xz - yz + xyz = x \otimes (y + z - yz) = x \otimes (y \otimes z)$;

乘幺: 断言 $0 \in \mathbb{R}$ 是 $\oplus$ 的单位元. 任取 $x \in \mathbb{R}$, 有 $0 \otimes x = 0 + x - 0x = x, x \otimes 0 = x + 0 - 0x = x$.

分配: 任取 $x, y, z \in \mathbb{R}$, 有 $x \otimes (y \oplus z) = x \otimes (y + z - 1) = x + y + z - 1 - xy - xz + x = (x + y - xy) + (x + z - xz) - 1 = x \otimes y \oplus x \otimes z$, 这就证明了左分配率. 又因为 $\otimes$ 显然满足交换律, 故右分配律可以直接通过 $(x \oplus y) \otimes z = z \otimes (x \oplus y) = z \otimes x \oplus z \otimes y = x \otimes z \oplus y \otimes z$ 得到.

9

题目没有断言 S 在自然加法与自然乘法下成环, 所以最好验证一下这一点. 由于这个过程实在太繁琐所以在此略去.

先证明 Ψ 保运算从而是环同态 这件事情对 $\Psi(f(x)) = f(x_0)$ 来说是平凡的:

任取 $f(x), g(x) \in \mathbb{Q}[x]$, 有 $\Psi(f + g) = (f + g)(\sqrt{\Delta}) = f(\sqrt{\Delta}) + g(\sqrt{\Delta}) = \Psi(f) + \Psi(g)$; $\Psi(fg) = (fg)(\sqrt{\Delta}) = f(\sqrt{\Delta}) + g(\sqrt{\Delta}) = \Psi(f) + \Psi(g)$.

再证明 Ψ 是满射:

任取 $a+b\sqrt{\Delta}\in S$, 则可取 $f(x)=a+bx\in\mathbb{Q}x$, 显然有 $\Psi(f)=a+b\sqrt{\Delta}$. 这就证明了 S 中每个元素都有原像.

求 KerΨ:

显然 S 的加法单位元为 $0=0+0\sqrt{\Delta}$, 现在要寻找使得 $\Psi(f)=f(\sqrt{\Delta})=0$ 的那些 f. 由于 f 是多项式, $f(\sqrt{\Delta})=0$ 说明 f 含有因式 $x-\sqrt{\Delta}$. 然而, 我们知道 f 的每一项系数均为有理数, 但 $\sqrt{\Delta}$ 却可能是无理数. 下面我们分两种情况讨论:

① Δ 是完全平方数, 从而 $\sqrt{\Delta}$ 是整数:

f 含有因式 $x-\sqrt{\Delta}$*

2020 期末

这份卷子佚失了.

2020 小测

1

$r(R) = \{(a,a),(a,b),(b,b),(c,c),(c,d),(d,d)\} = R \cup \{(c,c),(d,d)\}$

$s(R) = \{(a,a),(a,b),(b,a),(b,b),(c,d),(d,c)\} = R \cup \{(b,a),(d,c)\}$

$t(R) = R$

2

等价关系的证明略. 注意任意集合 A 上的一个等价关系 $\langle A, R\rangle$ 限制在 A 的一个子集 B 上 (得到 $\langle B, R \cap B^2\rangle$) 依然是等价关系.

$$
\begin{aligned}
A/R = \{&\{1,6,11,16\}\\
&\{2,7,12,17\}\\
&\{3,8,13,18\}\\
&\{4,9,14,19\}\\
&\{5,10,15,20\}\\
\}&
\end{aligned}
$$

3,4,5

It is trivial.

6

记集合 $\{1,2,3,4\}$ 为 A. 定义相等关系 $I_A = \{(a,a)|a \in A\}$.

(a)

为了破坏传递性, 考虑加入一对形如 $(a,b),(b,c)$ 的元组而不加入 (b,c), 又为了保证对称性还要加入所有对称的元组. 最后为了保证自反性再并上 I_A.

一个例子为 $R = I_A \cup \{(1,2),(2,1),(2,3),(3,2)\}$

(b)

为了保证对称性, 只要出现形如 (a,b) 的元组也一定会出现 (b,a), 从而根据传递性又会出现 (a,a) 和 (b,b). 所以为了破坏自反性, 必须要留至少一个元素 c 使得元组 (c,c) 不出现.

一个例子为 $R = \{(a,a),(a,b),(b,a),(b,b)\}$.

当然, 或许你已经发现了, 直接取 $R = \emptyset \subseteq A$ 也是一个例子.

(c)

破坏传递性的方法与 (a) 类似, 为了保证反对称性在加入 (a,b) 后不加入 (b,a) 即可.

一个例子为 $R = I_A \cup \{(1,2),(2,3)\}$.

(d)

任意在 A 上定义一个等价关系即可. 可以直接取 $R = I_A$ 或 $R = A^2$.

(e)

任意在 A 上定义一个偏序关系即可. 可以直接取 $R = I_A$ 或 $R = (a,b)|a \leq b$.

2021 期末

1

(1)

联立前两个方程得到 $x \equiv 11(\mathrm{mod}30)$.

再联立第三个方程得到 $x \equiv 11(\mathrm{mod}210)$.

最后联立第四个方程得到 $x \equiv 2111(\mathrm{mod}2310)$.

(2)

7800 的素因子分解为 $7800 = 2^3 \times 3 \times 5^2 \times 13$

故 $\phi(7800) = \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times 1213 \times 7800 = 1920$

2

R 的传递闭包就是 A^2. 显然 $(1,2),(2,3),(3,4),(4,1)$ 在 A 上构成了一条涉及所有点的有向圈. 因此对任意两个元素 $a, b \in A$, 可以通过它们根据传递性生成 (a,b).

$R^2 = \{(1,1),(1,3),(2,2),(2,4),(3,1),(4,2)\}$.

3

(1)

等价类的证明: 要证的只有传递性. 考虑 $a,b,c \in \mathbb{R}*$ 满足 $ab, bc > 0$, 则 $ab^2c > 0$, 又因为 $b^2 > 0$, 故 $ac > 0$.

等价类有两个, 分别为正数集 $\mathbb{R}^+$ 和负数集 $\mathbb{R}^-$.

(2)

不是. 对于 $0 \in \mathbb{R}$, $0^2 = 0 \not> 0$, 这就违反了自反性.

4

略.

5

必要性 $\Rightarrow$:

由于 H 非空, 可以任取 $a, b \in H$. 由于 H 是子群, 存在单位元 $e_H \in H$ 满足 $ae_H = a$, 根据 G 上的消去律得到 $e_H = e$. 这证明了 H 中的单位元就是 G 中的原单位元.

再由于 H 是子群, 存在 a 的逆元 a_H^{-1} 满足 $aa_H^{-1} = e_H = e$, 根据 G 上的消去律得到 $a_H^{-1} = a^{-1}$. 由 A 的任意性, 这证明了 H 中每个元素的逆元就是其在 G 中的原逆元.

依然由于 H 是子群, 根据 H 的封闭性有 $a_H^{-1}b \in H$ 即 $a^{-1}b \in H$.

充分性 $\Leftarrow$:

我们验证 H 满足群定义中的四条性质:

① 结合律: 直接从 G 中继承;

② 幺元: 由于 H 非空, 可以任取 $a \in H$, 则 $a^{-1}a = e \in H$. 由于 e 在 G 中是单位元, 故 $\forall h \in H$ 有 $eh = he = h$, 即 e 是 H 中的单位元;

③ 逆元: 任取 $a \in H$, 则 $a^{-1}e = a^{-1} \in H$. 由于 a^{-1} 在 G 中是 a 的逆元, 故 $aa^{-1} = a^{-1}a = e$ 为 H 中单位元. 这样就证明了 a^{-1} 在 H 中也是 a 的逆元;

⓪ 封闭性: 任取 $h_1, h_2 \in H$, 由③有 $h_1^{-1} \in H$, 故 $h_1 h_2 = (h_1^{-1})^{-1} h_2 \in H$.

请思考为什么在这里我们改变了验证四条性质的顺序. 如果从封闭性开始验证, 是否能够完成证明?

6

我们分 b 的阶是否有限来讨论.

① 如果 b 的阶有限, 即存在最小的正整数 n, 使得 $b^n = e_G$:

由于 f 是同构映射, 所以是同态映射. 故有 $(f(b))^n = f(b^n) = f(e_G) = e_{G'}$. 这说明 $f(b)$ 也有有限阶 m, 且有 $m|b$.

又由于 f 还是双射, 可以定义其逆 f^{-1}, 后者也是一个同构映射. 故有 $b^m = (f^{-1}(f(b)))^m = f^{-1}((f(b))^m) = f^{-1}(e_H) = e_G$. 这说明 $n|m$.

由于 m, n 都是正整数, 只能是 $m = n$.

7

确定最大元 0 与最小元 1, 由于集合 A 含有至少 3 个元素, 可以选出一个 $0, 1$ 之外的元素 a 满足 $0 < a < 1$.

接下来我们证明引理: 在线性序 $\langle A, R\rangle$ 中, 任意两个元素 a, b 的最小上界为 $max\{a, b\}$, 最大下界为 $min\{a, b\}$ (由于 A 中任意两个元素都可比, 这些记号都是良好定义的) .

(证明非常简单故在此略去, 可参考习题解答 8.1 题.)

现在假设 a 有补元 b, 但根据引理 $a * b$ 与 $a \oplus b$ 中至少有一者为 a, 两者不可能分别为 1 和 0. 矛盾.

8

⇒:

$I + \mathrm{Ker}f \subseteq R$ 根据封闭性是平凡的, 需要证明的仅有 $R \subseteq I + \mathrm{Ker}f$.

任取 R 中元素 r, 则可以确定 R' 中元素 $r' = f(r)$. 由于 $f(I) = R'$, 可以在 I 中找到 (至少一个) 元素 i 满足 $f(i) = r'$.

由于环关于加法构成一个群, 在 R 中可以确定 $r - i$, 接下来只需证明 $r - i \in \mathrm{Ker}f$. 考虑 $f(i) + f(r - i) = f(r) = r'$, 而左式又等于 $r' + f(r - i)$, 说明 $f(r - i) = 0_{R'}$, 即 $r - i \in \mathrm{Ker}f$.

⇐:

$f(I) \subseteq R'$ 是必然的, 需要证明的仅有 $R' \subseteq f(I)$.

任取 $r' \in R'$, 我们需要找到 $i \in I$ 满足 $f(i) = r'$. 任取 r' 在 R 中的一个原像 r, 则 r 可以表示为 $i + s$, 其中 $i \in I$, $s \in \mathrm{Ker}f$. 则 $r' = f(i) + f(s) = f(i) + 0_{R'} = f(i)$. 这就证明了上一步确定下来的 i 即为所求.

2022 期末

1

注意到 $(21, 39, 117) = 3$, 故原方程等价于 $7x \equiv 13(\mathrm{mod}39)$.

由于 $13|13$ 且 $13|39$, 而 $(7, 13) = 1$, 这说明 x 一定是 13 的倍数. 记 $x' = \frac{x}{13}$, 则原方程等价于 $7x' \equiv 1(\mathrm{mod}3)$.

显然解为 $x' \equiv 1(\mathrm{mod}3)$, 故原方程解为 $x \equiv 13(\mathrm{mod}39)$.

2

(1)

m 的缩系在 $\mathrm{mod}m$ 同余乘法下构成群 (记作 $\mathbb{Z}_n^*$) , 且 a 在 m 的缩系中故在 $\mathbb{Z}_n^*$ 中.

显然 $\mathbb{Z}_n^*$ 的单位元为 1. 由于这是一个有限群, a 有有限阶 n, 即 $a^n \equiv 1(\mathrm{mod}\, m)$. 又由于 $0 \notin \mathbb{Z}_n^*$, 故 $|\mathbb{Z}_n^*| \leq m-1$, 从而 a 的阶 n 至多为 $m-1$. n 即为所求.

(2)

教材 2.6.1 的原内容.

充分性: 由 $d_0|h$, 设 $h = kd_0$ 其中 $k \in \mathbb{N}$. 则 $a^h \equiv (a_0^d)^k \equiv 1^k \equiv 1(\mathrm{mod}m)$.

必要性:

若存在 h 满足 $a^h \equiv 1(\mathrm{mod}m)$, 则根据带余除法可以确定唯一的 $k, b \in \mathbb{N}$ 满足 $h = kd_0 + b$ 且 $0 < b < d_0$.

考虑 a^b, 有 $a^b \cdot a^{kd_0} \equiv a^h \equiv 1(\mathrm{mod}m)$, 又有 $a^{kd_0} \equiv (a_0^d)^k \equiv 1(\mathrm{mod}m)$. 根据群的消去律, 可知 $a^b \equiv 1(\mathrm{mod}m)$, 这与 d_0 的最小性矛盾.

3

(1) $(12345)(23) = (45123)(32) = (4512)$

(2)

第一问为教材习题 *5.19.*

左陪集: $\{I, (23)\}, \{(12), (123)\}, \{(13), (132)\}$

右陪集: $\{I, (23)\}, \{(12), (132)\}, \{(13), (123)\}$

4

略.

5

验证是平凡的.

6

显然这里默认了 g 的阶有限, 以及 $|G/H|$ 有限.

设 g 的阶为 m, $|G/H| = n$. 则由题有 $g^m = e$.

考虑 g 所在的陪集 gH. 由于 G/H 是一个良定义的群, 我们可以讨论 gH 作为元素在其中的阶 m'. 由于 $g^m = e \in H$, 故必然有 $(gH)^m = H$, 从而 $m'|m$.

另一方面, 由 Lagrange 定理, 阶 $m'|n$. 根据 $(m, n) = 1$ 可知 $m' = 1$, 即 gH G/H 中的单位元 H, 从而 $g \in H$.

7

这题的表述有问题. 我猜测题目的原意是 "存在 $G \to G'$ 的满同态映射的充要条件是 $n|m$" .

$n = 1$ 的情况是显然的, 此时 $n|m$ 与 f 是满同态都平凡地成立: 下面我们只考虑 $n \geq 2$ 的情况:

必要性 $\to$:

我们知道同态映射 f 一定有 $f(e_G) = e_{G'}$. 考虑 G 的一个生成元 a, 则 a 的阶是 m, 且有 $(f(a))^m = f(a^m) = f(e_G) = e_{G'}$.

我们知道像集 $f(G)$ 必定是一个群, 而这个群中的所有元素都可以用 $f(a)$ 生成 (任一元素的原像在 G 中可以用 a 生成, 然后根据同态保运算即得) . 由于 f 是满射, 即 $f(G) = H$, 所以 $f(a)$ 是 H 的生成元, 且其阶是 m 的因子, 即 $m|n$.

充分性 $\leftarrow$:

任取 G, G' 各自的生成元 a, a'. 则 G 中每个元素可以唯一表示为 a^k, 其中 $0 \leq k < m$. 定义映射 $f : G \to G', f(a^k) = f(a)^k$. 容易验证这的确是一个环同态 考试时请自己严格验证一遍, 所以只需要证明 f 是满射.

由于 a' 是 G' 的生成元, 因此 $\{a'^n | n \in \mathbb{N}\}$ 包含了整个 G', 也就意味着 $f(G) = G'$ 从而是满射.

p.s. 关于必要性的证明: 请时刻注意区分 $f(G)$ 和 H, 以及某个元素 "是 $f(G)$ 的生成元/是 H 的生成元" 这样的说法. 有的时候我们讨论一个映射时会默认其值域指的是所有能够被取到的元素, 即所谓 "所有的映射都是满射". 但在谈论两个具体的集合间的映射时请注意区分这一点.

8

首先证明 $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$:

(寻找同构映射和验证都是显然的, 这里略去.)

(1)

$\mathbb{Z}_n[x]$ 中元素形如 $f(x)=\sum_{i=0}^{n}\overline{a_i}x^i$, 其中 $\overline{a_i}$ 为 a_i 所在的同余类, $0\le a_i<n$.

定义映射 $f:\mathbb{Z}_n[x]\to\mathbb{Z}[x]/(n):f(\sum_{i=0}^{n}a_ix^i)=\overline{\sum_{i=0}^{n}a_ix^i}$, 即 $\sum_{i=0}^{n}a_ix^i$ 所在的同余类. 我们断言 f 是一个同构映射, 下面来证明这一点:

分别验证 f 具有双射和保运算的性质. 保运算直接代入验证即可, 没有技术含量; 关于双射的部分: 注意为证明是满射, 可以改为证明 $\mathbb{Z}[x]$ 中每个多项式所在的等价类都有原像, 因为 $\mathbb{Z}[x]/(n)$ 中的每个元素都是某个等价类. 这样就不必死板地证明 "每个元素都有原像".

(2)

这里的 $\mathbb{Z}[i]$ 指的应该是将 i 代入所有多项式的结果, 即所有形如 $ai+b(a,b\in\mathbb{Z})$ 的复数 (高斯整数) 构成的环. 我不确定这个记号在我们的是否规范.

不过, 对于环 R 中的任何一个元素 x_0, 其多项式环 $R[x]$ 中的所有多项式 $f(x)$ 代入 x_0 后得到的元素构成环, 这件事是必然的. (可以自行验证. 实际上它是 $R[x]$ 在 $\phi(f)=f(x_0)$ 下的同态像.)

我们已经知道 $\mathbb{Z}/2\mathbb{Z}\cong\mathbb{Z}_2$. 所以需要验证 $\mathbb{Z}[i]/(1+i)$ 恰有两个元素, 且它们的运算关系与 $\mathbb{Z}_2$ 中的相同.

考虑 $\mathbb{Z}[i]$ 上的等价关系: $a+bi\sim c+di$ 当且仅当 $\exists z\in\mathbb{Z}[i]\ s.t.\ (a+bi)-(c+di)=(1+i)z$. 我们来研究 $\mathbb{Z}[i]$ 在这个等价关系下有哪些等价类.

首先, 对于任意虚整数 $a+bi(b\neq 0)$, 显然其与实整数 $a-b$ 等价. 这说明可以选取每个等价类的代表元使得每个代表元都是实整数.

其次, 由于 $2=(1+i)(1-i)$, 因此当两个实整数的差是 2 的整数倍, 则它们两个等价. 这说明等价类至多有两根: 0 所在的等价类与 1 所在的等价类.

最后我们证明 $0\not\sim 1$. 假定存在 z 满足 $1-0=(1+i)z$, 解得 $z=\frac{1}{2}-\frac{1}{2}i$, 不是复整数.

综上, $\mathbb{Z}[i]/(1+i)$ 恰有两个元素. 我们知道二元环只有一种同构类, 因此 $\mathbb{Z}[i]/(1+i)$ 和 $\mathbb{Z}_2$ 也就是 $\mathbb{Z}/2\mathbb{Z}$ 同构. (当然这里也可以代入同构映射验证

保运算.)

9

我们先说明一点: 要证明题给命题, 只需证明两个理想的情况, 即 $I_1+I_2I_3=R$. 我们已经知道理想的积依然是理想 (参考习题 7.12) , 因此可以将 I_2I_3 视作一个新的理想 I_2', 从而有 $I_1+I_2'=I_1+I_4=R$, 因此也就有 $I_1+I_2'I_4=R$ 即 $I_1+I_2I_3I_4=R$. 类似地, 可以用归纳法推广到任意 $n\in\mathbb{N}^+$.

接下来我们来证明 $I_1+I_2I_3=R$.

$I_1+I_2I_3\subseteq R$ 是必然的, 我们只需要证明反方向的包含关系. 任取 $r\in R$, 根据 $I_1+I_2=I_1+I_3=R$, 我们可以确定 $i_{11}\in I_1, i_2\in I_2$ 满足 $i_{11}+i_2=r$, 以及 $i_{12}\in I_1, i_3\in I_3$ 满足 $i_{12}+i_3=1_R$, 即 R 中的乘法单位元.

则有 $r=r\cdot 1_I=(i_{11}+i_2)(i_{12}+i_3)=(i_{11}i_{12}+i_{11}i_3+i_{12}i_2)+i_2i_3$. 由于理想满足乘法吸收性, 所以 $i_{11}i_{12}, i_{11}i_3, i_{12}i_2\in I_1$; 又由于理想满足加法封闭性, 所以右式的第一项属于 I_1, 而第二项属于 I_2I_3, 这就证明了 r 可以表示为 $I_1+I_2I_3$ 中的形式. 由 r 的任意性也就证明了 $R\subseteq I_1+I_2I_3$.

2023 期末

1

联立前两个方程解得 $x \equiv 31(\mathrm{mod}35)$.

再联立第三个方程解得 $x \equiv 31(\mathrm{mod}385)$.

2

由于 $(m,n)=1$, 只需证 $m^{\phi(n)}+n^{\phi(m)} \equiv 1(\mathrm{mod}m)$ 和 $m^{\phi(n)}+n^{\phi(m)} \equiv 1(\mathrm{mod}n)$ 分别成立. 显然它们分别等价于 $n^{\phi(m)} \equiv 1(\mathrm{mod}m)$ 和 $m^{\phi(n)} \equiv 1(\mathrm{mod}n)$.

考虑 m 的缩系在 $\mathrm{mod}m$ 同余乘法下构成的群 $\mathbb{Z}_m^*$ 以及 n 所在的等价类作为元素. 由于 $|\mathbb{Z}_m^*|=\phi(m)$, 根据 Lagrange 定理, n 的阶为 $\phi(m)$ 的因子, 从而 $n^{\phi(m)}$ 为这个群中的单位元 1. 这样就证明了 $n^{\phi(m)} \equiv 1(\mathrm{mod}m)$. 根据对称性另一个式子完全同理.

3

略.

4

教材习题 4.6 原题.

5

教材习题 5.8 原题.

(1)

对任一阶大于 2 的元素 a, 可以证明其逆元 a' 与 a 阶相同 *(证明在此略去, 请读者尝试自行完成)* 故也大于 2. 又 a 的阶大于 2 故 $a \neq a'$.

这说明阶大于 2 的元素总是成对出现. 由于 G 是有限群故其中阶大于 2 的元素数量有限, 从而是偶数.

(2)

由于 $|G|$ 为偶数, 故 G 中阶为 1 和 2 的元素数量之和也为偶数. 而 1 阶元只有 1 个, 即单位元 e, 从而 2 阶元有奇数个, 也就至少有一个.

6

充分性 $\Leftarrow$:

平凡群 $\mathbb{Z}_1 = \{e\}$ 自然没有非平凡子群. 对于素数阶循环群: 我们知道如果 G 是有限群, 则其子群 $H \subseteq G$ 的元素个数必为 $|G|$ 的因子. 从而素数阶循环群 $\mathbb{Z}_p$ 的子群 H 的元素个数只可能是 1 或 p, 而前者只能同构于平凡群 $\mathbb{Z}_1$, 后者只能是 $\mathbb{Z}_p$ 本身.

必要性 $\Rightarrow$:

我们分两种情况讨论: 假如 G 的最小生成组有多于一个元素 (即需要多于一个元素生成) , 则任取一个非单位元 $a \in G$, 其生成的子群 $[a]$ 含有非单位元 a 故不是平凡群 $\{e\}$, 又 a 不能独自生成整个 G 故 $[a]$ 不是 G 本身. 这样就证明了 G 有平凡子群, 矛盾.

假如 G 的最小生成组至多有一个元素, 则 G 必然是循环群.

如果 G 是无限循环群, 则其只能同构于 $\mathbb{Z}$, 而 $2\mathbb{Z} = \{2k | k \in \mathbb{Z}\}$ 便是其一个非平凡子群, 舍去; 如果 G 是有限循环群, 设其为 n 阶循环群. 如果 n 有非

平凡因子 m, 则生成元 a 对应的 a^m 生成的子群 $[a^m]$ 便是其一个非平凡子群.

这样就推翻了除了平凡群和素数阶循环群之外的任何可能性. 故证.

7

考虑商群 G/H 中 x 所在的等价类 $\overline{x}$ 的阶. 由于 $|G/H| = [G : H] = m$, $\overline{x}$ 的阶必为 m 的因子, 从而 $\overline{x}^m$ 为单位元 H.

x^m 所在的等价类即为 $\overline{x}^m$, 故 $x^m \in H$.

8

(1)

先验证 $Z(G)$ 是子群, 即 $Z(G)$ 在原乘法下构成群:

⓪ 封闭性: 任取 $a, b \in Z(G)$, 则 $\forall g \in G$, 有 $abg = agb = gab$, 从而 ab 也与任何元素可交换. 这就证明了 $ab \in G$, 由 a, b 任意性即得 $Z(G)$ 封闭性;

① 结合律: 直接从 G 中继承;

② 幺元: e 当然是与任何元素可交换的;

③ 逆元: 任取 $a \in Z(G)$, 我们欲证明 $a' \in Z(G)$. $\forall g \in G$, 则 $a'ga = a'ag = g$, 又 $ga'a = g$, 根据消去律可得 $a'g = ga'$. 这就证明了 $a' \in Z(G)$.

再证 $Z(G)$ 的正规性: $\forall g \in G$, 有 $gZ(G) = \{ga | a \in Z(G)\} = \{ag | a \in Z(G)\} = Z(G)g$, 从而 $Z(G)$ 的每个元素的左右陪集对应相等. 故证.

(2)

这是一句废话.

(3)

这是近世代数中一个相当有趣的结论: 如果一个群 G 商掉其“中心”后得到循环群, 那么这个循环群必然是平凡群即群 G 就是其中心, 也就意味着 G 就是交换群.

任取 G 的两个元素 b, c. 我们可以试图证明 b, c 可交换来证明 G 是交换群. 考虑 b, c 在 $G/Z(G)$ 中对应的所属的等价类 $bZ(G), cZ(G))$.

考虑 $G/Z(G)$ 的一个生成元, 记其为 $aZ(G)$, 则 $\exists m, n \in \mathbb{Z}$ 满足 $bZ(G) = (aZ(G))^m, cZ(G) = (aZ(G))^n$.

在 (1) 中我们已经知道 $Z(G)$ 是正规子群, 从而对任意两个元素 s, t, 有 $sZ(G)tZ(G) = st(Z(G))^2 = stZ(G)$ (后一个等号是因为 $Z(G)$ 满足封闭性和幺元的存在性) . 基于这一点, 我们可以归纳地证明 $(aZ(G))^m = a^mZ(G)$. 从而 $bZ(G) = a^mZ(G), cZ(G) = a^nZ(G)$.

这意味着 $b \in a^m(G), c \in a^nZ(G)$. 从而我们可以写出如此表示 $b = a^ms, c = a^nt$, 其中 $s, t \in Z(G)$ 即与任意元素可交换. 则有 $bc = a^msa^nt = a^{m+n}st$, 以及 $cb = a^nta^ms = a^{m+n}ts = a^{m+n}st$, 从而 $bc = cb$.

由 b, c 的任意性可知 G 中任意两个元素可交换, 从而 G 是交换群.

9

这是一道非常典型的“不需要任何洞见, 但考察对基本概念的定义的记忆及其嵌套的使用”的验证题. 因此我在此略去它的解答, 请认为自己在处理复杂符号嵌套上不熟练的同学, 自行从定义出发写一遍这道题的完整过程. 这对考前复习来说是一次很好的锻炼. *(另一个原因是我实在懒得写了.)*

2024

1

$$2 \times 2 \equiv 4(\mathrm{mod}13)$$
$$4 \times 2 \equiv 8(\mathrm{mod}13)$$
$$8 \times 2 \equiv 3(\mathrm{mod}13)$$
$$3 \times 2 \equiv 6(\mathrm{mod}13)$$
$$6 \times 2 \equiv 12(\mathrm{mod}13)$$
$$12 \times 2 \equiv 11(\mathrm{mod}13)$$
$$11 \times 2 \equiv 9(\mathrm{mod}13)$$
$$9 \times 2 \equiv 5(\mathrm{mod}13)$$
$$5 \times 2 \equiv 10(\mathrm{mod}13)$$
$$10 \times 2 \equiv 7(\mathrm{mod}13)$$
$$7 \times 2 \equiv 1(\mathrm{mod}13)$$

由上可知 2 关于 mod13 同余乘法的阶为 12, 从而 2 能够生成 mod13 的整个缩系, 是 13 的一个原根.

方程 $4x^9 \equiv 7(\mathrm{mod}13)$ 等价于 $x^9 \equiv 5(\mathrm{mod}13)$. 设 $x \equiv 2^k \equiv (\mathrm{mod}13)$, 则 $2^{9k} \equiv (\mathrm{mod}13)$ 即 $9k \equiv 9(\mathrm{mod}12)$.

后者解得 $k \equiv 1(\mathrm{mod}4)$ 即 $k \equiv 1$ 或 5 或 $9(\mathrm{mod}12)$, 从而 $x \equiv 2$ 或 6 或 $5(\mathrm{mod}13)$.

2

(1)

不具有自反性, 因为不含有 $(1, 1)$;

具有反自反性, 因为对任意元素 $a \in A$, 都不含有 (a, a);

不具有对称性, 因为有 $(1, 2)$ 而没有 $(2, 1)$;

不具有反对称性, 因为同时有 $(3, 4)$ 和 $(3, 4)$;

不具有传递性, 因为有 $(1, 2), (2, 3)$ 但没有 $(1, 3)$.

(2)

自反闭包: $R \cup I_A$;

传递闭包: $\{(1,2),(1,3),(1,4),(1,5),(2,3),(2,4),(2,5),(3,3),(3,4),(4,3),(4,4)\}$;

$R^2 = \{(1,3),(1,5),(2,4),(3,3),(4,4)\}$

p.s. 注意这里 R^2 指的是关系的复合而非 R 作为集合的笛卡尔积的二次幂.

3

(1)

由 $d \geq 1$, 有

$$\begin{aligned} a \equiv b(\mathrm{mod} m) &\Leftrightarrow \exists k \in \mathbb{Z}\ s.t.\ a - b = mk \\ &\Leftrightarrow \exists k \in \mathbb{Z}\ s.t.\ da - db = dmk \\ &\Leftrightarrow da \equiv db(\mathrm{mod} dm) \end{aligned}$$

故证.

(2)

根据中国剩余定理, 由于 m, n 互素, 命题等价于 $m^{\phi}(n) + n^{\phi}(m) \equiv 1(\mathrm{mod}\ m)$ 且 $m^{\phi}(n) + n^{\phi}(m) \equiv 1(\mathrm{mod} n)$. 后者又等价于 $m^{\phi}(n) \equiv 1(\mathrm{mod} n)$ 且 $n^{\phi}(m) \equiv (\mathrm{mod} m)$.

由 Eular 定理即得.

4

(1)

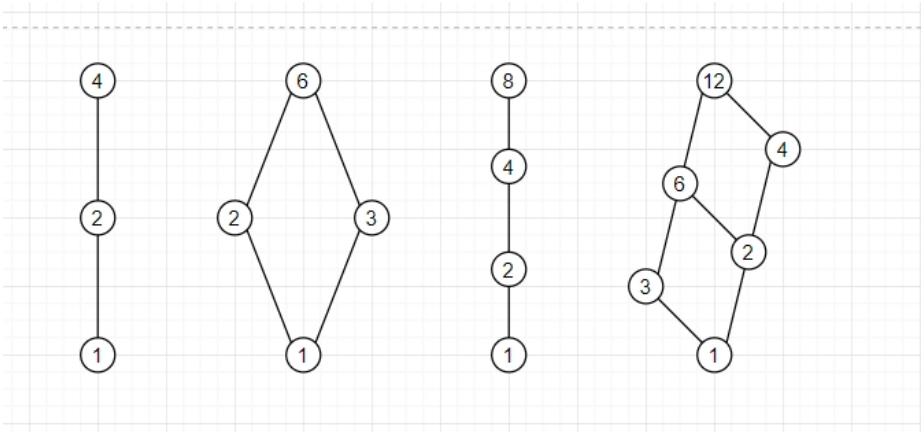
我们断言在 S_n 中, 任意两个元素 a, b 的最小上界和最大下界分别是 $[a, b]$ 和 (a, b). 下面来证明这一点:

先证明 $[a, b]$ 和 (a, b) 如果在 S_n 中, 则一定分别是最小上界和最大下界: 如果 $[a, b]$ 在 S_n 中, 而 $\{a, b\}$ 存在不比 $[a, b]$ 大的上界 c, 则有 $a|c, b|c$ 以及 $[a, b] \not| c$, 这与 $[a, b]$ 作为 a 和 b 的最小公倍数定义矛盾, 故 $[a, b]$ 是最小上界; 同理, 若 (a, b) 在 S_n 中, 则一定是最大下界.

再证明 $[a, b]$ 和 (a, b) 的确都在 S_n 中: 由 $a, b \in S_n$ 有 $a|n, b|n$, 根据 $[a, b]$ 作为最小公倍数的定义则有 $[a, b]|n$, 从而 $[a, b] \in S_n$; 至于 (a, b), 由 $(a, b)|a|n$ 即得 $(a, b) \in S_n$.

这样我们就证明了 S_n 中任意两个元素都存在最小上界和最大下界, 从而证明了 S_n 是格.

(2)



(3)

S_n 为线性序当且仅当其中任意两个元素 a, b 可比. 我们断言其充要条件是 $n = 1$ 或 $n = p^k$(p 为素数 ,$k \in \mathbb{N}^+$). 下面证明这一点:

必要性: 采用反证法. 若 n 有至少两个不同的素因子 a, b, 则 $a, b \in S_n$ 不可比, S_n 不是线性序;

充分性: 若 $n = 1$, S_n 中只有一个元素, 显然是线性序; 若 $n = p^k$, 则 S_n 中任意两个元素形如 $a = p^i, b = p^j (0 \leq i, j \leq k)$. 易见 $a|b \Leftrightarrow i \leq j$, 由于 i, j 在整数的小于关系下一定是可比的, 从而 a, b 在整除关系下是可比的. 从而 S_n 是线性序.

5.

(1)

单位元 e 满足对任意 $B \in \mathscr{P}(A)$ 即 $B \subseteq A$, 有 $e \oplus B = (e \setminus B) \cup (B \setminus e) = B$.

如果 e 中有 B 中没有的元素 $a \in e \setminus B$, 则 $a \in e \oplus B$ 而 $a \notin B$, 矛盾; 如果 e 中有 B 中有的元素 $b \in e \cap B$, 则 $b \notin B \setminus e$ 从而 $b \notin e \oplus B$, 同样矛盾.

这说明 e 中不应有任何元素即 $e = \emptyset$.

任取 $B \in \mathscr{P}(A)$ 即 $B \subseteq A$, 考虑子集 $C \subseteq A$ 使得 $B \oplus C = \emptyset$, 则应有 $C \cap B = B$ 以及 $C \cap B^c = \emptyset$, 从而有 $C = B$, 即每个元素的逆元都是它自身.

(2)

由消去律, $X = \{1, 3\}^{-1} \oplus \{3, 4, 5\} = \{1, 3\} \oplus \{3, 4, 5\} = \{1, 4, 5\}$.

(3)

(1) 中证明了任意元素的逆为自身从而阶为 2, 故 B 的生成子群 $\langle B \rangle$ 同构于 $\mathbb{Z}_2$, 即 $\langle B \rangle = \{B, \emptyset\}$.

6.

证明理想需证明 A 满足减法封闭性与乘法吸收性. 任取方阵 $M, N \in A, P \in \mathbb{Z}_{2\times 2}$, 则 M, N 均为偶数方阵从而其差为偶数方阵, MP 与 PM 的每个元素均为偶数从而也是偶数方阵.

$|R/A| = 16$.

7.

由于 Ker$f$ 是 G_1 的子群且满足 $\forall a \in G$ 有 $a\text{Ker} = \text{Ker}a$, 从而 Ker$f$ 是 H 的子群且是 H 的正规子群.

从而 H 是 Ker 的一系列陪集的不交并即 $H = \bigcup\limits_{i\in I} a_i\text{Ker}$. 任取 G_1 中的元素 b, 则有:

$$\begin{aligned}
bH &= \bigcup_{i\in I} ba_i\text{Ker} \\
&= \bigcup_{i\in I} ba_i\text{KerKer} \\
&= \bigcup_{i\in I} b\text{Ker}a_i\text{Ker} \\
&= \bigcup_{i\in I} a_i\text{Ker}b\text{Ker} \\
&= \bigcup_{i\in I} a_i\text{KerKer}b \\
&= \bigcup_{i\in I} a_i\text{Ker}b \\
&= Hb
\end{aligned}$$

这就证明了 H 是 G_1 的正规子群, 其中第三行到第四行的等号来自于 G_2 是交换群.

8.

由 Lagrange 定理, G 中元素的阶都应该是 $|G|$ 的因子, 从而奇数阶群 G 中不应有 2 阶元. 这意味着 G 中元素除了单位元逆 e 外每个 a 都可以和自己

的逆元 a' 一一配对, 而每一个这样的配对乘积都是 e, 连乘并再乘上 e 后结果也是 e.

9.

法①:

反证法: 假设 f 不是同构, 则 f 不单即 $\mathrm{Ker}f \neq \{e\}$.

从而对于全体 $n \in \mathbb{N}$, $f^{-n}\mathrm{Ker}$ 是 G 的两两不同的子群, 与 G 只有有限多个子群矛盾.

法②:

我们直接证明 G 是有限群.

先证明 G 中任意元素 a 有限阶, 否则 $\langle a\rangle \cong \mathbb{Z}$, 则全体每个 $n \in \mathbb{N}$, $n\langle a\rangle\mathbb{Z}$ 是 G 的两两不同的子群, 矛盾;

又有 $G = \bigcup\limits_{a\in G} \langle a\rangle$. 右侧中每个集合都是有限集. 同时每个集合都是 G 的子群, 从而至多有有限多个不同的. 则 G 是有限个有限集的并集, 从而是有限群.

由 G 是有限群, 且 f 是 G 上的满射, 从而必定是 G 上的双射, 从而是 G 的自同构.