课程名称：代数学

第一次作业

中南大學

姓名：　樊昊
学号：242131001

数学与统计学院

第零章

题目 3 . 举例说明, 整数集合 $\mathbb{Z}$ 上存在映射 $f\colon \mathbb{Z}\to\mathbb{Z}$, 使得 f 有左（右）逆但无右（左）逆。

解答.[1] 取 $h\colon k\mapsto 2k$, 则 $g\colon 2k\mapsto k, 2k+1\mapsto 0$ 是 h 的左逆. 因为 h 非满射, 没有右逆. 这里 g 有右逆 h, 但是非单射所以没有左逆. 分别取 $f=g, f=h$ 即可. ■

题目 4 . 试判断自反性、对称性和传递性对下列二元关系是否成立？

(i) 实数系 $\mathbb{R}, x-y$ 为 2π 的整数倍；

(ii) $\mathbb{R}, x\geq y$;

(iii) $\mathbb{R}, x>y$;

(iv) S 是仅含一个元素的集, $x>y$。

解答.[2] 关于 $S=\{*\}$, 此时 $>$ 视作 $S\times S$ 子集应该为空集, 对称性, 传递性成立 (vacuous truth).

表 1: 问题 5

	反身性	对称性	传递性
(i)	✓	✓	✓
(ii)	✓	×	✓
(iii)	×	×	✓
(iv)	×	✓	✓

■

题目 5 . 试判断自反性、对称性和传递性对下列二元关系是否成立？

(i) $\mathbb{R}, |x-y|=1$;

(ii) $\mathbb{R}, |x-y|\leq 1$;

(iii) $\mathbb{R}, x-y=1$;

(iv) $\mathbb{R}, x+y=1$。

解答.[3] 见下表. ■

表 2: 问题 6

	反身性	对称性	传递性
(i)	×	✓	×
(ii)	✓	✓	×
(iii)	×	×	×
(iv)	×	✓	×

题目 11 . 设 X, Y, Z 为任意集合, 又设 $\psi_i : X \to Y, i = 1, 2, \eta : Y \to Z$. 证明：“如果 $\eta\psi_1 = \eta\psi_2$, 则 $\psi_1 = \psi_2$” 对任意 ψ_1, ψ_2 都成立的充要条件是 η 是一个单射。

解答.[4] 充分性: 若 η 是单射, 且 $\eta\psi_1 = \eta\psi_2$, 则任意 $x \in X$ 有 $\eta(\psi_1(x)) = \eta(\psi_2(x))$. 因为单射性, $\psi_1(x) = \psi_2(x)$ 总成立, 即 $\psi_1 = \psi_2$.

必要性: 若 η 不是单射, 则有 $a, b \in Y$ 使得 $\eta(a) = \eta(b)$. 不难构造 $\psi_1(x) = a \neq b = \psi_2(x)$, 且 $\psi_1|_{X\setminus\{x\}} = \psi_2|_{X\setminus\{x\}}$. 则 $\eta\psi_1 = \eta\psi_2$ 但是 $\psi_1 \neq \psi_2$. ■

题目 15 . 应用定理 7, 证明欧拉函数 $\varphi(n)$ 可写成

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

解答.[5] 记 $[r] = \{1, 2, \ldots, r\}$. 由定理 7, 对 $n = p_1^{e_1} \cdots p_r^{e_r}$, 有

$$\begin{aligned}
\frac{\varphi(n)}{n} &= (1 - p_1^{-1}) \cdots (1 - p_r^{-1}) \\
&= \sum_{\ell=0}^{r} \sum_{\sharp\{i | k_i = 1\} = \ell} (-1)^{\ell} p_1^{-k_1} \cdots p_r^{-k_r} \\
&= \sum_{\substack{k_i \in \{0,1\}^r, \\ i \in [r]}} \frac{\mu(p_1^{k_1} \cdots p_r^{k_r})}{p_1^{k_1} \cdots p_r^{k_r}} \\
&= \sum_{\substack{d|n, \\ d\text{无平方因子}}} \frac{\mu(d)}{d} = \sum_{d|n} \frac{\mu(d)}{d}.
\end{aligned}$$

■

题目 18 . 证明：若 $f(n)$ 是一个乘性函数, 则 $h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$ 也是一个乘性函数。

解答.[6] 对于互素的 n_1, n_2, 有

$$\begin{aligned} h(n_1n_2) &= \sum_{d|n_1n_2} \mu\Big(\frac{n_1n_2}{d}\Big) f(d) = \sum_{\substack{d_1|n_1,\\ d_2|n_2}} \mu\Big(\frac{n_1}{d_1}\frac{n_2}{d_2}\Big) f(d_1d_2) \\ &= \sum_{d_1|n_1} \mu\Big(\frac{n_1}{d_1}\Big) f(d_1) \sum_{d_2|n_2} \mu\Big(\frac{n_2}{d_2}\Big) f(d_2) \\ &= h(n_1)h(n_2). \end{aligned}$$

■

题目 21 . 证明

$$\sum_{\substack{1\le r\le n\\ (r,n)=1}} r = \frac{1}{2} n\varphi(n).$$

解答.[7] 左边即对落在 $[1, n]$ 的一组 mod n 剩余类求和, 故

$$\sum_{\substack{1\le r\le n\\ (r,n)=1}} r = \sum_{\substack{1\le r\le n\\ (r,n)=1}} n - r = \sum_{\substack{1\le r\le n\\ (r,n)=1}} \frac{r + (n-r)}{2} = \frac{1}{2} n\varphi(n).$$

■

群论

第一章

题目 5 . 在 S_3 中找出两个元素 x, y , 适合

$$(xy)^2 \neq x^2y^2.$$

解答.[8] 只要 $xy \neq yx$ 即可. 取 $x = (12)$, $y = (13)$. 则

$$xy = (132) \neq yx = (123).$$

■

题目 8 . 证明：群 G 为一交换群当且仅当映射 $x \mapsto x^{-1}$ 是一同构映射。

解答.[9] 记 $i\colon x \mapsto x^{-1}$. i 是双射. 熟知 $(xy)^{-1} = y^{-1}x^{-1}$. 所以 i 是同构当且仅当 $y^{-1}x^{-1} = x^{-1}y^{-1}, \forall x, y$; 当且仅当 $xy = yx, \forall x, y$. ■

题目 13 . 设群 G 的阶为一偶数, 证明 G 中必有一个元素 $a \neq e$ 适合 $a^2 = e$。

解答.[10] 在集合 G 上定义关系: $g \sim h \iff gh = e$. 则 $\sim$ 是等价关系. 并且, 每个等价类一定是一个元或者两个元. 注意 $[e] = \{e\}$,

$$\sharp G = \sum_{[g]\in G/\sim} \sharp[g] = 1 + \underbrace{\sum_{\substack{[g]\in G/\sim \\ [g]\neq[e]}} \sharp[g]}_{\text{是奇数}},$$

所以求和项有奇数, 即某等价类为一个元, 也即 $a^2 = e$. ■

题目 16 . 在群 $SL_2(\mathbb{Q})$ 中, 证明元素

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

的阶为 4, 元素

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

的阶为 3, 而 AB 为无限阶元素.

解答.[11] 直接计算

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ A^3 = -A \neq I,\ A^4 = I.$$

于是阶为 4.

$$B^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix},\ B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

于是阶为 3.

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ (AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},\ \forall n \geq 1.$$

于是 AB 为无限阶元素. ■

第二章

题目 21 . 证明任一非交换的 6 阶群同构于 S_3。

解答.[12] 设 G 为非交换 6 阶群. 由 Sylow 第三定理,

$$N_3 := \text{Sylow 3-子群的个数} \equiv 1 \pmod 3,$$

且 $N_3 \mid 2$, 可见 $N_3 = 1$. 所以有唯一一个 Sylow-3 群 P_3, 且是正规子群. 现在, 除去子群 P_3, 还有 3 个元素, 均不是 3 阶元, 又不是单位元; Langrange 定理保证阶数只能从 $1, 2, 3, 6$ 取; 如果有 6 阶元, 那么群应是循环群, 和非交换的假设矛盾.

取一个三阶元 g , 一个二阶元 h; 则 $\langle g\rangle \cap \langle h\rangle = \{e\}$ 且 $\langle g, h\rangle = G$. 由于 $\langle g\rangle$ 是指数 2 的子群, 是正规的, 也就是说 $G = \langle g\rangle \rtimes \langle h\rangle$, 有共轭作用 $\langle h\rangle \curvearrowright \langle g\rangle$, 且这个不是平凡的作用 (作用平凡即 $hgh^{-1} = g$, 换言之 $\langle g\rangle, \langle h\rangle$ 交换, 此时 G 由他们生成从而交换). 非平凡的群作用对应一个非平凡的同态 $\langle h\rangle \to \mathrm{Aut}(\langle g\rangle)$, 而 $\mathrm{Aut}(\langle g\rangle) \cong \mathbb{Z}/\langle 2\rangle$, 所以这共轭作用只能是

$$hgh^{-1} = g^2, hg^2h^{-1} = g.$$

综上所述,

$$G = \langle g, h \mid g^3 = h^2 = e, hgh^{-1} = g^2, hg^2h^{-1} = g\rangle;$$

欲求的同构由

$$G \to S_3 \colon g \mapsto (123),\ h \mapsto (12)$$

给出. ■

题目 22 . 定出全部互不相构的 15 阶群。

解答.[13] 由 Sylow 第三定理,

$$N_5 \coloneqq \text{Sylow 5-子群的个数} \equiv 1 \pmod 5,$$

且 $N_5 \mid 3$, 可见 $N_5 = 1$. 所以有且仅有一个 5 阶正规子群 H. 同理有且仅有一个 3 阶正规子群 K. 两个正规子群交为 $\{e\}$: $H \cap K$ 中元素阶数整除 $3, 5$ 于是为 1. 计数

$$|HK| = \frac{|H||K|}{|H \cap K|} = 15 \implies G = HK$$

由内直积的刻画, 这就是 $G = H \times K$; 换言之, $G \cong \mathbb{Z}/\langle 3\rangle \times \mathbb{Z}/\langle 5\rangle \cong \mathbb{Z}/\langle 15\rangle$(中国剩余定理).

综上所述, 同构意义下, 15 阶群只有 $\mathbb{Z}/\langle 15\rangle$. ■

题目 23 . 设 p, q 为不同的素数, 证明不存在阶为 pq 的单群。

解答.[14] 不妨设 $p < q$. 由 Sylow 第三定理, $N_q \equiv 1 \pmod q$. 且 $N_q \mid p$ 所以 $N_q = 1$, 此时 Sylow q-子群即正规子群. ■

题目 24 . 设 p, q 为不同的素数, 证明 p^2q 阶群必包含一个正规西罗子群。

补充

题目 1 . k 是奇数，证明 $2k$ 阶群必有一个 k 阶子群.

尝试. 一定有 Sylow 2-子群 (同构于 $\mathbb{Z}/\langle 2\rangle$), 设某个 Sylow 2-子群的生成元为 g. 设 G 在正则表示 ρ 下有 $G \lesssim S_n$, 此时 $\rho(G) \cap A_n$ 是 $\rho(G)$ 的正规子群, 对应的 $\rho^{-1}(A_n)$ 是 G 的正规子群

题目 3 . 设 G 是有限群，p 是 $|G|$ 的最小素因子。又设 $H \leq G$ 且 $|G : H| = p$，则 $H \lhd G$。

更多习题

题目 5 . Prove that all the groups of order p^2 is commutative. Here p is a prime number.

解答.[18] Let G be a group of order p^2. Then it has a nontrivial center, whose order is p^2 or p. If $= p^2$ the $G = Z(G)$. If $|Z(G)| = p$ then it is isomorphic to $\mathbb{Z}/\langle p\rangle$, let $Z(G) = \langle g\rangle$. What's more, $|G \setminus Z(G)| = p^2 - p$ elements are not in center and take $h \in G \setminus Z(G)$, which generates a subgroup H of order p. Now,

$$|Z(G)H| = \frac{|Z(G)| \times |H|}{|Z(G) \bigcap H|} = p^2 \implies Z(G)H = G.$$

Thus, $G = Z(G) \rtimes H$, and this semi-direct product is trivial, since $g \in Z(G)$ ensures $hgh^{-1} = g$. Now, $G \cong (\mathbb{Z}/\langle p\rangle)^2$ is commutative. Therefore, it is impossible that $|Z(G)| = p$.

Above all, all the groups of order p^2 is Abelian. ■

题目 8 . Let M be a finite abelian group $\neq 0$. Can M be made into a left $\mathbb{Q}$-module?

解答.[19] It can't be made into a left $\mathbb{Q}$-module. Else, for $0 \neq g \in M$, for $n \in \mathbb{Z}_{>0}$ we have $\frac{1}{n}g \in M$. It turns out that $\operatorname{ord}(\frac{1}{n}g) = n \operatorname{ord}(g)$ and $\operatorname{ord}(\frac{1}{n}g) > |M|$ for large n, which is impossible due to Langrange's Theorem. ■

题目 10 . Determine $\operatorname{End}(\mathbb{Q}, +, 0)$.

解答.[20] 作为环同构于 $\mathbb{Q}$:

$$\operatorname{End}(\mathbb{Q}, +, 0) \to \mathbb{Q},\ f \mapsto f(1). \tag{1}$$

这显然是满射, 下证明是单射. 设 $f(1) = g(1)$, 则 $\forall m \in \mathbb{Z}, \forall n \geq 1$,

$$f(1) = n \cdot f\Big(\frac{1}{n}\Big) = n \cdot g\Big(\frac{1}{n}\Big) = g(1);$$
$$f\Big(\frac{m}{n}\Big) = mf\Big(\frac{1}{n}\Big) = mg\Big(\frac{1}{n}\Big) = g\Big(\frac{m}{n}\Big).$$

所以 $f = g$, (1) 是单射. 而同态性质: 加法层面是直接根据定义得到的, 乘法层面

$$f\Big(\frac{m}{n}\Big) = \frac{m}{n}f(1) \implies (f \circ g)(1) = f(g(1)) = f(1)g(1).$$

■

题目 11 . Show that any subgroup of index two is normal. Hence prove that A_n is normal in S_n. 第 1 章第 12 题

解答.[21] Let G be a group and $H \leq G$ is of index two. Then for $g \in G$, either $gH = H$ or $G = H \sqcup gH$.

- If $gH = H$, then $(gH)^{-1} = Hg^{-1} = H^{-1} = H$ and hence $gHg^{-1} = g(Hg^{-1}) = gH = H$.
- If $G = H \sqcup gH$, then $g \notin H$ and hence $Hg \neq H$; so $G = H \sqcup Hg$. Compare and it follows $gH = Hg$.

Above all, H is normal.

For A_n, it is known that $|A_n| = n!/2 = |S_n|/2$ that is of index two and thus is normal. ■

题目 12 . Verify that the intersection of any set of normal subgroups of a group is a normal subgroup. Show that if H and K are normal subgroups, then HK is a normal subgroup.

解答.[22] Let $\{G_i\}_{i\in I}$ be a family of normal subgroups of G and $\{\pi_i \colon G \twoheadrightarrow G/G_i\}$ be the natural projections. Then

$$\pi \colon G \to \prod_{i\in I} G/G_i,\ g \mapsto (\pi_i(g))_{i\in I}$$

is a group hommorphism, whose kernel is $\ker \pi = \bigcap_{i\in I} G_i$, which must be a normal subgroup.

Let H, K be normal subgroups of G.

- It is a subgroup. Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$, we have

$$(h_1k_1)^{-1}h_2k_2 = k_1^{-1}h_1^{-1}h_2k_2 = \underbrace{(k_1^{-1}h_1^{-1}h_2k_1)}_{\in H}k_1^{-1}k_2 \in HK.$$

- It is normal. Let $g \in G$, $ghkg^{-1} = (ghg^{-1})(gkg^{-1}) \in HK$ and hence HK is normal.

■

题目 15 . Show that if $a^m = b^m$ and $a^n = b^n$, for m and n relatively prime positive integers, and a and b in a commutative domain, then $a = b$.

解答.[23] By Bézout's Theorem, there are $u, v \in \mathbb{Z}$ s.t. $um + vn = 1$. Therefore

$$a = a^{um+vn} = (a^m)^u \cdot (a^n)^v = (b^m)^u \cdot (b^n)^v = b^{um+vn} = b.$$

■

题目 16 . Determine the sign of the permutation

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

解答.[24] The permutation σ is strictly decreasing, so

$$\mathrm{Inv}_\sigma \coloneqq \{(i,j) \mid 1 \le i < j \le n,\ \sigma(i) > \sigma(j)\} = \bigcup_{i=1}^{n} \{(i,j) \mid 1 \le i < j \le n\} \implies \sharp\mathrm{Inv}_\sigma = \frac{n(n-1)}{2}.$$

And hence, $\mathrm{sign}(\sigma) = (-1)^{n(n-1)/2}$. ■

题目 17 . Show that if α is any permutation, then

$$\alpha(i_1 i_2 \cdots i_r)\alpha^{-1} = (\alpha(i_1)\alpha(i_2)\cdots\alpha(i_r))$$

解答.[25] For $k \in [r]$ and addition in the sense of mod r:

$$\alpha(i_k) \overset{\alpha^{-1}}{\longmapsto} i_1 \overset{(i_1 i_2 \cdots i_r)}{\longmapsto} i_{k+1} \overset{\alpha}{\longmapsto} \alpha(i_{k+1}).$$

For elements that fixed by α:

$$\ell \overset{\alpha^{-1}}{\longmapsto} \ell \overset{(i_1 i_2 \cdots i_r)}{\longmapsto} \ell \overset{\alpha}{\longmapsto} \ell.$$

Above all, the equality holds. ■

题目 18 . Show that S_n is generated by the $n-1$ transpositions $(12), (13), \ldots, (1n)$ and also by the $n-1$ transpositions $(12), (23), \ldots, (n-1\ n)$. 第 2 章第 10 题

解答.[26] We know that S_n is generated by $\{(ij) \mid 1 \le i < j \le n\} =: B$. Now, B is generated by $C \coloneqq \{(12), (13), \ldots, (1n)\}$ since

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

Also, C is generated by $(12), (23), \ldots, (n-1\ n)$, since

$$\begin{aligned}
(13) &= (12)(23)(12),\\
(14) &= (13)(34)(13),\\
&\cdots = \cdots,\\
(1\ n) &= (1\ n-1)(n-1\ n)(1\ n-1).
\end{aligned}$$

■

环论

第一章

题目 43 . $C[0,1]$ 为全体定义在闭区间 $[0,1]$ 上的连续函数组成的环。证明：

(i) 对于 $C[0,1]$ 的任一非平凡的理想 I, 一定有一实数 θ, $0 \leq \theta \leq 1$, 使 $f(\theta) = 0$ 对所有的 $f(x) \in I$ 都成立;

(ii) $f(x) \in C[0,1]$ 是一零因子当且仅当点集

$$\{x \in [0,1] \mid f(x) = 0\}$$

包含一个开区间。

解答.[27] 反证, 假若结论不成立, 则对每个点 $\theta \in [0,1]$ 有 $f_\theta \in I$ 使得 $f_\theta(\theta) \neq 0$. 由连续性, $f_\theta|_{U_\theta} \neq 0$ 对某个开集 $U_\theta \ni \theta$ 成立. 利用 $[0,1]$ 的紧致性, 找出有限个 $U_1, \ldots, U_m$ 覆盖 $[0,1]$ 和相应区间上非零的 $f_1, \ldots, f_m$. 则 $f \coloneqq \sum_{i=1}^m f_i^2 \in I$ 且 f 可逆, 因为 $f > 0$. 现在, $I = C[0,1]$, 矛盾.

充分性: 容易构造一个非零函数, 在 $f^{-1}\{0\}$ 上非零而在 $[0,1] \setminus f^{-1}\{0\}$ 上恒为 0. 于是 f 是零因子.
必要性: 反证法, 若 $f^{-1}\{0\}$ 不含任何开区间, 且存在 $g \in C[0,1], g \cdot f = 0$ 则 $[0,1] \setminus g^{-1}\{0\} \subseteq f^{-1}\{0\}$ 是一个开集, 故而 $= \varnothing$, 即 $g = 0$. ■

题目 44 . 令 $F = \mathbb{Z}/p\mathbb{Z}$ 为 p 个元素的域。求

(i) 环 $M_n(F)$ 的元素的个数;

(ii) 群 $GL_n(F)$ 的元素的个数。

解答.[28] 直接的: $|M_n(F)| = |F^{n^2}| = p^{n^2} > \theta$.

注意矩阵 $A \in GL_n(F)$ 当且仅当其列向量是线性无关组. 分步计数: 第一列列向量, 可以选择的非零向量有 $p^n - 1$ 个; 第二列的选择范围剔除第一列生成的子空间, 即 $p^n - p$ 种; 第三列的选择范围, 剔除前两个列向量生成的子空间, 即 $p^n - p^2$ 种; 类似继续... 结论即

$$|GL_n(F)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}).$$

■

第三章

题目 5 . 设 F 为一个特征 p 的域, p 为素数, 证明

$$(a+b)^p = a^p + b^p, \quad \text{对所有的} a, b \in F.$$

域的特征概念可以推广到幺环上去。如果幺环 R 的单位元素 e 生成的加法群 $G = \{ne \mid n \in \mathbb{Z}\}$ 是一个无限群, 则 R 叫做特征 0 的环; 若 G 是一个有限群, 令 $k = |G|$, 则 k 叫做环 R 的特征。证明: 若 R 为整环, 则 R 的特征为 0 或为一个素数, 而且若 R 的特征为素数 p, 则上面等式对 R 也成立。

解答.[29] 对特征 p 的域 F, 按照二项式定理, 只需证明 $p \mid \binom{p}{j}$, $\forall j \in [p-1]$. 这当然成立: 只有分子出现了 p, 分母没有出现.

下证明整环有特征 0 或者素数 (等式的成立性证明一样). 设 G 是有限群, 且设 k 为特征, 则 $k\mathbf{1}=0$. 若 $k=mn$, $m,n\in\mathbb{Z}_{\geq 1}$, 注意 $k\mathbf{1}=m\mathbf{1}\cdot n\mathbf{1}=0$, 所以 $m\mathbf{1}=0$ 或者 $n\mathbf{1}=0$. 特征的定义保证 $m=k$ 或者 $n=k$. 综上所述, k 是素数. ■

更多习题

题目 19 . Determine the ideals and the maximal ideals and prime ideals of $\mathbb{Z}/(60)$.

解答.[30] In a PID (especially, $\mathbb{Z}/(60)$), maximal ideals are the same as prime ideals. There is a natural projection $\mathbb{Z}\twoheadrightarrow\mathbb{Z}/(60)$. Thus we have a correspondence:

$$\{\text{Ideals } I_2\subseteq\mathbb{Z}/(60)\}\overset{1:1}{\longleftrightarrow}\{\text{Ideals } I_1\subseteq\mathbb{Z}:I_1\supseteq\ker[\mathbb{Z}\twoheadrightarrow\mathbb{Z}/(60)]\}.$$

The maximal ideals are those ideals generated by $\overline{2},\overline{3},\overline{5}$ as Figure 1.

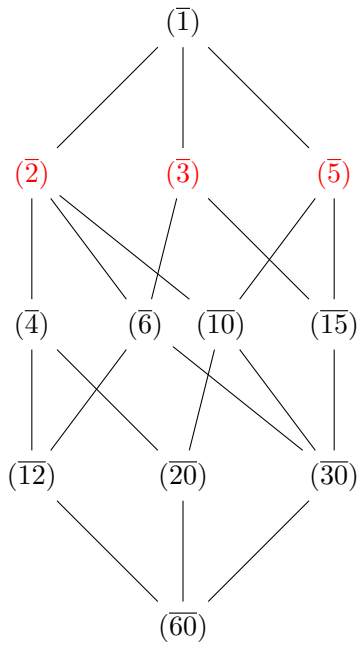

图 1: Ideals of $\mathbb{Z}/60\mathbb{Z}$

■

题目 20 . Let G be an abelian group with a finite set of generators which is periodic in the sense that all of its elements have finite order. Show that G is finite.

解答.[31] Let $\{g_1,\ldots,g_m\}$ be a periodic set of generators. Then it suffices to show that

$$g_1^{k_1}g_2^{k_2}\cdots g_m^{k_m},\quad k_i\in\mathbb{Z}$$

have only finitely many results, since G is Abelian. By periodicity, we can restrict $|k_i| \leq k$ for some $k \in \mathbb{Z}$ and then we have $|G| \leq k^m$. ■

题目 24 . Verify that for $a, b \in \mathbb{R}$, the mapping

$$a + b\sqrt{-1} \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

is an isomorphism of $\mathbb{C}$ with a subring of $M_2(\mathbb{R})$.

解答.[32] Denote the mapping by φ, then it is additive. For multiplication,

$$\begin{aligned} \varphi((a + b\sqrt{-1})(c + d\sqrt{-1})) &= \varphi(ac - bd + (ad + bc)\sqrt{-1}) \\ &= \begin{pmatrix} ac - bd & ad + bc \\ ad + bc & ac - bd \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\ &= \varphi(a + b\sqrt{-1})\varphi(c + d\sqrt{-1}). \end{aligned}$$

Thus, $\varphi\colon \mathbb{C} \to \varphi(\mathbb{C})$ is an isomorphism, where $\varphi(\mathbb{C}) = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$ is a subring of $M_2(\mathbb{R})$. ■