作业十　（1月5日课堂上交）

1. 本题是关于 $\mathbb{R}^n$ 上的刚体变换的。本题中，采用如下定义：在 $\mathbb{R}^n$ 中，我们说子集 A 和 B 是刚体等价的，如果存在 $\mathbb{R}^n$ 上的刚体变换 ρ ，使得 $\rho(A)=B$ 。我们说集合 $A\in\mathbb{R}^n$ 是有界的，如果存在 $K\in\mathbb{R}_{>0}$ ，使得 $\sup\limits_{x,y\in A}\mathrm{d}(x,y)<K$ ，其中 $x=(x_1,\cdots,x_n)$ ， $y=(y_1,\cdots,y_n)$ ，且 $\mathrm{d}(x,y)$ 定义为 $\sqrt{\sum\limits_{i=1}^{n}(x_i-y_i)^2}$ 。

a) 构造 $\mathbb{R}^2$ 中的有界子集 A ，使得 A 刚体等价于 A 的某个真子集。

b) 构造 $\mathbb{R}$ 中的子集 A ，使得 A 刚体等价于 A 的某个真子集。

c) 证明：不存在 $\mathbb{R}$ 中的有界子集 A，使得 A 刚体等价于 A 的某个真子集。

注：在 c) 的证明中，可以直接使用《数学分析》课程中学到的所有概念和相关性质，比如上/下确界、函数连续性（刚体变换一定是连续的）、单调性（可以考虑先证明 $\mathbb{R}$ 到 $\mathbb{R}$ 的刚体变换作为函数来看一定是单调函数）等。

2. 本题目是关于课上提过的 “$\mathbb{E}_3$ 包含自由群 $\mathbb{F}_2$” 这个事实之部分验证，这里 $\mathbb{E}_3$ 是 $\mathbb{R}^3$ 上的刚体变换群。

a) 对于任意的一个 3×3 实矩阵 A，我们可以将其看为一个从 $\mathbb{R}^3$ 到 $\mathbb{R}^3$ 的映射，定义如下：

$$A\colon\mathbb{R}^3\longrightarrow\mathbb{R}^3,\ x\longmapsto A\cdot x\quad,$$

其中 $A=\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ ，$x=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ ，而 $A\cdot x$ 就是标准的矩阵乘法。

对于任意给定的 $\theta\in\mathbb{R}$ ，令 $P=\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$ ，

$Q=\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$ 。

证明：P 和 Q 都是 $\mathbb{R}^3$ 上的刚体变换（保距变换），这里 $x=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ 和 $y=\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$ 之间的距离定义为 $\sqrt{\sum_{i=1}^{3}(x_i-y_i)^2}$ 。

b) 对于 a) 中的 P 和 Q ，令 $\theta=\arccos 3/5$ 。令 $e_1=\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ 。

证明：对于任意的 $k\in\mathbb{N}_{\geq 1}$ 和 $n_1,\cdots,n_k\in\mathbb{N}_{\geq 1}$ ，以及任意的 $S=T_1^{n_1}\cdots T_k^{n_k}P$ ，我们有 $S\cdot e_1\neq e_1$ ，这里 $T_i\in\{P,Q\}$ ，$\forall\, i\in\{1,\cdots,k\}$ 。

提示：先证明如下事实：对于上述的 $S=T_1^{n_1}\cdots T_k^{n_k}P$ ，我们有

$$S\cdot e_1=\frac{1}{5^{n_1+\cdots+n_k+1}}\cdot\begin{pmatrix} a \\ b \\ c \end{pmatrix},$$

其中 $a,b,c\in\mathbb{Z}$ 并且 $5\nmid b$ （读作“ 5 不整除 b ”）。该事实的证明可以用数学归纳法得到。这里可以不假证明的使用如下事实（基于 5 是素数）：对于任意 $x,y\in\mathbb{Z}$ ，如果 $5\nmid x$ 且 $5\nmid y$ ，则 $5\nmid(x\cdot y)$ 。

参考答案：

一、

a) 在 $\mathbb{R}^2$ 中，令 $x=(1,0)$ 。选定无理数 θ ，并定义

$$\rho\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2,\ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} \cos 2\pi\theta & -\sin 2\pi\theta \\ \sin 2\pi\theta & \cos 2\pi\theta \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

不难验证（通过计算）ρ 的确为 $\mathbb{R}^2$ 上的保距变换（刚体变换）。

事实上，ρ 相当于将 $\mathbb{R}^2$ 中的点绕着原点逆时针旋转 $2\pi\theta$ 角度。因为 θ 是无理数，对于任意 $m,n\in\mathbb{N}$ 并且 $m\neq n$ ，均有 $\rho^m(x)\neq\rho^n(x)$ 。

定义

$$A=\{x,\rho(x),\rho^2(x),\rho^3(x),\cdots\}\text{ 。}$$

则

$$\rho(A)=\{\rho(x),\rho^2(x),\rho^3(x),\rho^4(x),\cdots\}\subsetneq A\text{ 。}$$

至于 A 的有界性，由于 A 在单位圆上，A 显然是有界的。

b) 在 $\mathbb{R}$ 中，令 $A=\mathbb{N}_{\geq 0}$ ，并令 ρ 为 $\mathbb{R}$ 上的“加 1 ”变换。则 ρ 显然为刚体变换。

易验证

$$\rho(A)=\rho(\mathbb{N}_{\geq 0})=\mathbb{N}_{\geq 1}\subsetneq\mathbb{N}_{\geq 0}=A\text{ 。}$$

c) 证明：用反证法。

假定存在 A 中的有界子集和 $\mathbb{R}$ 上的刚体变换 ρ ，使得 $\rho(A)\subsetneq A$ 。

因为 A 是 $\mathbb{R}$ 中有界集，故 $\sup A$ 和 $\inf A$ 均存在。令 $L=\inf A$ ，$R=\sup A$ 。

断言：若 ρ 为 $\mathbb{R}$ 上的刚体变换，则作为函数，ρ 一定是严格单调函数。

断言之证明：在 $\mathbb{R}$ 中取定 $a<b$ ，因为 ρ 是刚体变换，不可能有 $\rho(a)=\rho(b)$ 。我们来证明更强的结论：若 $\rho(a)<\rho(b)$ ，则 ρ 为严格单调增函数。事实上，$\rho(x)=x+(\rho(a)-a)$。若 $\rho(a)>\rho(b)$ ，则 ρ 为严格单调减函数，事实上，$\rho(x)=-x+(\rho(a)+a)$ 。

假定 $\rho(a)<\rho(b)$ 。对于任意 $x\in\mathbb{R}$ ，我们来证明：$\rho(x)=x+(\rho(a)-a)$ 。事实上，根据刚体变换之定义，我们知道

$$|\rho(x)-\rho(a)|=|x-a| \text{ 且 } |\rho(x)-\rho(b)|=|x-b| \text{ 。}$$

注意到如下事实：在 $\mathbb{R}$ 上，如果 $y_1\neq y_2$ ，那么对于任意的 $d_1,d_2\in\mathbb{R}_{>0}$，则最多存在一个 $y\in\mathbb{R}$ ，使得 $|y-y_1|=d_1$ 且 $|y-y_2|=d_2$ 。（为什么？）

由于 $\rho(a)\neq\rho(b)$ ，上述两个条件会唯一的确定 $\rho(x)\in\mathbb{R}$ 。由于 $a<b$ 以及 $\rho(a)<\rho(b)$ ，我们有

$$\rho(x)-\rho(a)=x-a \text{ ，}$$

从而 $\rho(x)=x+(\rho(a)-a)$，$\forall x\in\mathbb{R}$ ，这样 ρ 是单调递增函数。

类似的，若 $\rho(a)>\rho(b)$ ，我们可以证明 $\rho(x)=-x+(\rho(a)+a)$ ，从而 ρ 是单调递减函数。断言证毕。

我们不妨假定 $\rho(x)=x+(\rho(a)-a)$，$\forall x\in\mathbb{R}$ 。令 $L'=\inf\rho(A)$ ，$R'=\sup\rho(A)$ 。 由于 $\rho(A)\subset A$ ，我们有 $L\leq L'$ 且 $R'\leq R$ 。事实上，由于 ρ 是刚体变换，我们有

$$R-L=\sup_{x_1,x_2\in A}|x_1-x_2|=\sup_{x_1,x_2\in A}|\rho(x_1)-\rho(x_2)|=R'-L' \text{ 。}$$

由于 $R-L=R'-L'$ ，$L\leq L'$ 且 $R'\leq R$ ，我们有 $L=L'$ 和 $R=R'$ 。

由于

$$L'=\inf\rho(A)=\inf_{x\in A}\{\rho(x)\}=\inf_{x\in A}\{x+(\rho(a)-a)\}=\rho(a)-a+\inf_{x\in A}\{x\}=\rho(a)-a+\inf A=\rho(a)-a+L \text{ ，}$$

我们有 $\rho(a)-a=0$ ，从而 $\rho(x)=x$ ，$\forall\, x\in A$ 。故 $\rho(A)=A$ ，而这与 $\rho(A)\subsetneq A$ 矛盾。

下面讨论 ρ 严格单调减的情形。这种情形下 $\rho(x)=-x+(\rho(a)+a)$ 。我们可以借助上面 ρ 严格单调增情形的论述来说明在 ρ 严格单调减时，$\rho(A)=A$ 。

考虑刚体变换（同时也是严格单调减函数）

$$\rho\colon A \longrightarrow A \text{ 。}$$

由于 ρ 是刚体变换，因此 $\rho^2 := \rho \circ \rho$ 也是刚体变换。由于 ρ 是严格单调减函数，故 ρ^2 为严格单调增函数。考虑刚体变换（同时也是严格单调增函数）

$$\rho^2\colon A \longrightarrow A \text{ 。}$$

根据上面严格单调增情形的论述，我们知道 $\rho^2 = \mathrm{id}_A$ 。注意以下事实（为什么下述事实成立？）：

“对于映射 $f\colon X \to Y$ 和 $g\colon Y \to X$ ，如果 $f \circ g = \mathrm{id}_Y$ ，则 f 为满射。”

，我们可以得到 $\rho\colon A \to A$ 是满射（为什么？）。

由于刚体变换 ρ 必然是单射（为什么？），因此 $\rho\colon A \to A$ 是双射，这与 $\rho(A) \subsetneq A$ 矛盾。证毕。

□

二、

a) 我们证明 P 的保距性。Q 的保距性之证明是几乎完全平行的。

对于任意 $\mathbb{R}^3$ 中 $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ ，我们有

$$P \cdot x = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1\cos\theta - x_2\sin\theta \\ x_1\sin\theta + x_2\cos\theta \\ x_3 \end{pmatrix} \text{ 。}$$

直接验证可得

$$(x_1\cos\theta - x_2\sin\theta)^2 + (x_1\sin\theta + x_2\cos\theta)^2 + x_3^2 = x_1^2 + x_2^2 + x_3^3 \text{ ,}$$

因此 P 为保距变换（刚体变换）。类似的， Q 也是刚体变换。证毕。 □

b) 证明：

我们这里给出的证明是个暴力证明（通过计算实现）。

首先，计算 Pe 。有

$$Pe = \begin{pmatrix} \frac{3}{5} & -\frac{4}{5} & 0 \\ \frac{4}{5} & \frac{3}{5} & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{5}\begin{pmatrix} 3 \\ 4 \\ 0 \end{pmatrix} \text{ 。}$$

当 $S = P$ 时，$b = 4 \nmid 5$ 。假定 $S = WP$ ，其中 W 是由 P 和 Q 生成的，总长度为 n 的字。比如 PPQ 的长度为 3 ，P^3Q^2 的长度为 5 ，乘法单位元 e 的长度被认为是 0 。我们计算给定了 S 、以及 $S \cdot e = \frac{1}{5^{n+1}}\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ 后，PS 和 QS 作用在 e 上面所得到的

$$PS \cdot e = \frac{1}{5^{n+2}}\begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} \quad \text{和} \quad QS \cdot e = \frac{1}{5^{n+2}}\begin{pmatrix} a'' \\ b'' \\ c'' \end{pmatrix}$$

中的 a', b', c' 以及 a'', b'', c'' 。

由于 $\theta = \arccos 3/5$ ，不难验证对于任意的 $x_1, x_2, x_3 \in \mathbb{Z}$ ，如果 $5 \mid x_i$ ，$i = 1, 2, 3$ ，则

$$Px = P\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix} \quad \text{和} \quad Qx = Q\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1'' \\ x_2'' \\ x_3'' \end{pmatrix}$$

中得到的 x_i' 和 x_i'' （ $i = 1, 2, 3$ ）都是 5 的倍数。

基于此，在上述关于 a', b', c' 和 a'', b'', c'' 的计算中，我们只需要关心它们除 5 后的余数（或者是模 5 后的同余类）即可。这里用 $[m]$ 来代表整数 m 模上 5 后的同余类。比如 $[-8] = [12] = [2]$ 。

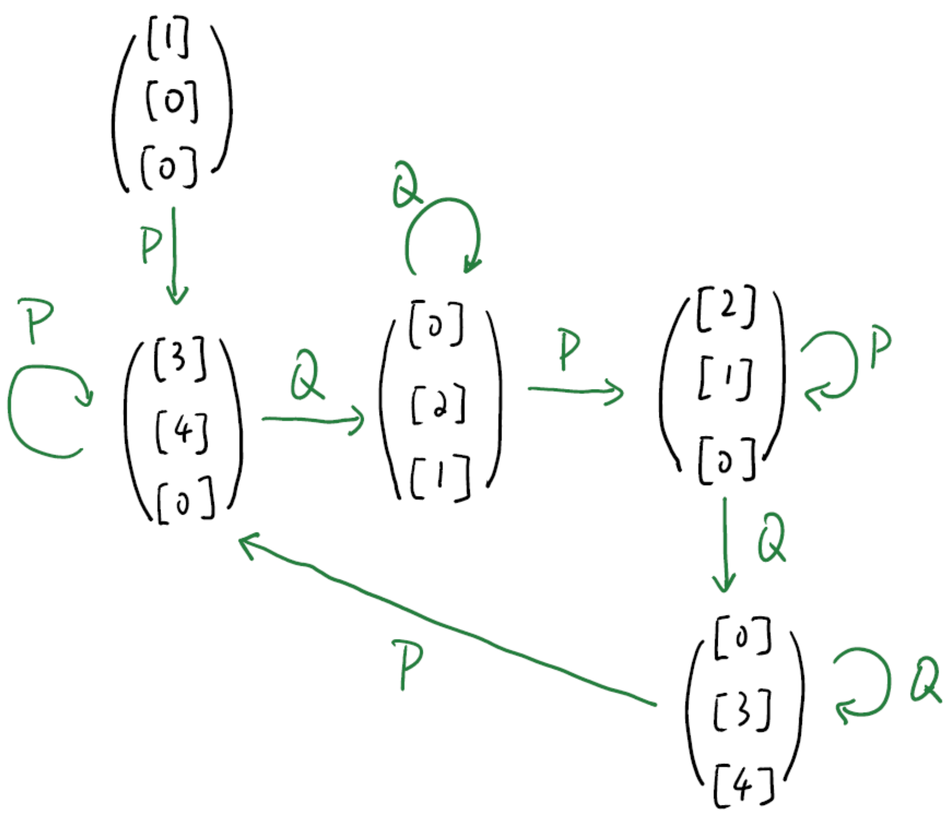
由于 $Pe = P\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{5}\begin{pmatrix} 3 \\ 4 \\ 0 \end{pmatrix}$ ，我们有如下记法：

$$\begin{pmatrix} [1] \\ [0] \\ [0] \end{pmatrix} \xrightarrow{P} \begin{pmatrix} [3] \\ [4] \\ [0] \end{pmatrix} 。$$

注意到 $P \cdot \frac{1}{5^{n+1}}\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \frac{1}{5^{n+2}}\begin{pmatrix} 3a-4b \\ 4a+3b \\ 5c \end{pmatrix}$ 以及 $Q \cdot \frac{1}{5^{n+1}}\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \frac{1}{5^{n+2}}\begin{pmatrix} 5a \\ 3b-4c \\ 4b+3c \end{pmatrix}$ 。

我们可以计算 $\begin{pmatrix} 3 \\ 4 \\ 0 \end{pmatrix}$ 被 P 和 Q 不断作用时，其得到的 a, b, c 的同余类。

根据我们的计算（read: brute force），其同余类的转换图如下：



在上图中的除了起始状态外的所有状态中，b 都不能被 5 整除，证毕。 □