作业八 （12月15日课堂上交）

1. 对于两个非零自然数 m 和 n ，我们在课中已经定义他们的最大公约数为他们所有公约数全体中的最大的那个，并且记为 gcd(m,n) 。类似的，对于三个非零自然数 m,n 和 k，我们这里定义它们的公约数集合为（cd for common divisors）

$$\text{cd}(m,n,k)=\{r\in\mathbb{N}-\{0\}\colon r|m\text{，}\ r|n\text{ 且 }r|k\}\ \text{，}$$

并且定义 gcd(m,n,k) 为 cd(m,n,k) 中的最大值。由于 $1\in$ cd(m,n,k)，并且 cd(m,n,k) 中任意元素大小不会超过 m ，因此 gcd(m,n,k) 也是良性定义的。

基于上述定义（关于三个非零自然数的最大公约数）和课上学过的内容（比如辗转相除法等），完成如下：

i) 证明：对于任意三个非零自然数 m,n 和 k，

$$\text{gcd}(m,n,k)=\text{gcd}(m,\text{gcd}(n,k))=\text{gcd}(\text{gcd}(m,n),k)$$

ii) 证明：对于任意非零自然数 m 和 n， 存在 $p,q\in\mathbb{Z}$ ，使得

$$mp+nq=\text{gcd}(m,n)$$

iii) 证明：对于任意三个非零自然数 m,n 和 k， 存在 $p,q,r\in\mathbb{Z}$ ，使得

$$mp+nq+kr=\text{gcd}(m,n,k)$$

iv) 在 ii) 中，对于给定非零自然数 m 和 n ，满足 $mp+nq=$ gcd(m,n) 的二元整数组（换言之，整数对）$(p,q)\in\mathbb{Z}^2$ 是唯一的吗？若是，给出证明；若否，给出反例。

2. 课上介绍过，群 G 在集合 X 上的作用 $G \times X \longrightarrow X$ 被称为是自由的，如果对于任意 $g \in G - \{e_G\}$ ，g 作用在 X 上都是没有不动点的。换言之，对于任意 $g \in G - \{e_G\}$ 和任意 $x \in X$ ，都有 $g(x) \neq x$ 。

一个在 X 上的作用不存在不动点，并不是始终可以做到的（比如，如果要求该作用是连续的）。下面是一些与此相关的内容。

i) 假定 $f\colon [0,1] \longrightarrow [0,1],\ x \mapsto f(x)$ 是一个从 $[0,1]$ 到 $[0,1]$ 的连续函数，证明一定存在 $a \in [0,1]$ ，使得 $f(a) = a$ 。换言之，证明：任意 $[0,1]$ 到自身（不需要是单射或者满射）的连续映射，一定存在不动点。

注：这里你们可以直接使用在《数学分析》课程中学过的所有关于连续函数的性质。

ii) 在二维实空间 $\mathbb{R}^2$ 中，定义

$$S^1 = \{(x,y) \in \mathbb{R}^2 \colon x^2 + y^2 = 1\} \text{ 。}$$

则 S^1 即为平面中的单位圆。构造 S^1 到自身的双射 f ，使得 f 不存在不动点。

iii) 在三维实空间 $\mathbb{R}^3$ 中，定义

$$S^2 = \{(x,y,z) \in \mathbb{R}^3 \colon x^2 + y^2 + z^2 = 1\} \text{ 。}$$

则 S^2 即为三维空间中的单位球面（其本身是二维的）。构造 S^2 到自身的双射 f ，使得 f 不存在不动点。

iv) 构造映射 $f\colon [0,1] \longrightarrow [0,1]$ ，使得 f 不存在不动点（这里 f 不要求是连续的，也不要求是单射或者满射，更不要求是双射，只要求是映射）。换言之，构造一个 $[0,1]$ 到自身的映射 f，使得 $f(x) \neq x,\ \forall\, x \in [0,1]$ 。

v) [选做题/思考题] 构造双射 $f\colon [0,1] \longrightarrow [0,1]$ ，使得 f 不存在不动点（这里的 f 不要求是连续的，但要求是双射）。

参考答案：

1.

i) 我们只需证明

$$\gcd(m,n,k)=\gcd(m,\gcd(n,k)),\quad \forall m,n,k\in\mathbb{N}_{>0}\text{。}$$

若此成立，则

$$\gcd(\gcd(m,n),k)=\gcd(k,\gcd(m,n))=\gcd(k,m,n)=\gcd(m,n,k)\text{。}$$

为了证明 $\gcd(m,n,k)=\gcd(m,\gcd(n,k))$ ，令

$$x=\gcd(m,n,k),\quad y=\gcd(m,\gcd(n,k))\text{。}$$

断言：若非零自然数 z 同时整除 p 和 q （换言之，$z\in\mathrm{cd}(p,q)$ ），则 $z|\gcd(p,q)$ 。

断言之证明：根据 ii) 中结论，存在 $a,b\in\mathbb{Z}$ ，使得

$$ap+bq=\gcd(p,q)\text{。}$$

由于 $z|p$ ，故 $z|ap$ 。由于 $z|q$ ，故 $z|bq$ 。因此 $z|(ap+bq)$ 。换言之，$z|\gcd(p,q)$ 。证毕。□

如果 $z\in\mathrm{cd}(m,n,k)$ ，则 $z|m$ ，$z|n$ 且 $z|k$ 。根据上面的断言，我们有 $z|m$ 且 $z|\gcd(n,k)$ 。从而 $z\in\mathrm{cd}(m,\gcd(n,k))$ 。故 $z\le\gcd(m,\gcd(n,k))=y$ 。

由于 $x=\gcd(m,n,k)\in\mathrm{cd}(m,n,k)$ ，故

$$x\le\gcd(m,\gcd(n,k))=y\text{。}$$

如果 $z\in\mathrm{cd}(m,\gcd(n,k))$ ，则 $z|m$ 且 $z|\gcd(n,k)$ 。由于 $\gcd(n,k)|n$ 且 $\gcd(n,k)|k$ ，我们可以得到 $z|m$ ， $z|n$ 且 $z|k$ 。换言之，$z\in\mathrm{cd}(m,n,k)$ 。因此 $z\le\gcd(m,n,k)=x$ 。

由于 $y = \gcd(m, \gcd(n,k)) \in \mathrm{cd}(m, \gcd(n,k))$ ，我们有

$$y \leq \gcd(m,n,k) = x \text{ 。}$$

综上，我们有 $x = y$ ，即 $\gcd(m,n,k) = \gcd(m, \gcd(n,k))$ 。证毕。 □

ii) 如课件中提示和课上演示一样，将辗转相除法反过来走一遍即可。

iii) 根据 i) ，$\gcd(m,n,k) = \gcd(m, \gcd(n,k))$ 。运用两次 ii) 中结论即可。

iv) 不是唯一的。比如 $m = n = 5$ 。则 $\gcd(5,5) = 5$ ，但是我们有

$$1 \cdot 5 + 0 \cdot 5 = 5 \text{ 以及 } 2 \cdot 5 + (-1) \cdot 5 = 5, \text{ 等等。}$$

2.

i) 提示：介值定理。

ii) 考虑如下映射

$$f \colon S^1 \longrightarrow S^1,\ (x,y) \mapsto (-x,-y)$$

即可。

iii) 考虑如下对径映射 (antipodal map)

$$f \colon S^2 \longrightarrow S^2,\ (x,y,z) \mapsto (-x,-y,-z)$$

即可。

iv) 令

$$f(x)=\begin{cases}0 & x\neq 0\\ 1 & x=0\end{cases}$$

即可。

v) 这样的构造不是特别困难。