近世代数 (H) 第一周作业

涂嘉乐 PB23151786

2025 年 2 月 28 日

Exercise 1

(1) 求证：$f: X \to Y$ 是单射 $\iff \forall g, g': Z \to X$，若 $f \circ g = f \circ g'$，则 $g = g'$，即 f 满足左消去律

(2) 求证：$f: X \to Y$ 是满射 $\iff \forall h, h': Y \to Z$，若 $h \circ f = h' \circ f$，则 $h = h'$，即 f 满足右消去律

(3) 求证：$f: X \to Y$ 是双射 $\iff \exists g: Y \to X, \text{s.t. } g \circ f = \mathrm{Id}_X, f \circ g = \mathrm{Id}_Y$，且此时 g 是唯一的，记 $g = f^{-1}$

Proof

(1) $(\Rightarrow): \forall x \in Z$，若 $f \circ g(x) = f \circ g'(x)$，即 $f(g(x)) = f(g'(x))$，由 f 是单射知，$g(x) = g'(x), \forall x \in Z$，因此 $g = g'$

$(\Leftarrow)$: 考虑 $Z = \{z\}$，对于 $\forall x_1, x_2 \in X$，我们定义 $g(z) = x_1, g'(z) = x_2$，因为

$$f(x_1) = f(x_2) \iff f(g(z)) = f(g'(z)) \iff f \circ g = f \circ g'$$

其中第二个当且仅当是因为 g, g' 的定义域 Z 只有一个元素 z，因为 f 满足左消去律，所以当 $f(x_1) = f(x_2)$ 时，可推出 $g = g'$，故 $x_1 = g(z) = g'(z) = x_2$，由 x_1, x_2 的任意性知，f 是单射

(2) $(\Rightarrow): \forall y \in Y$，由 f 是满射知，$\exists x \in X, \text{s.t. } f(x) = y$，因此

$$h \circ f(x) = h' \circ f(x) \iff h(y) = h'(y), \forall y \in Y$$

这就说明 $h = h'$

$(\Leftarrow)$: 考虑 $Z = \{0, 1\}$，我们定义

$$h(y) = 1, \forall y \in Y, \quad h'(y) = \begin{cases} 1, & y \in \mathrm{Im} f \\ 0, & y \notin \mathrm{Im} f \end{cases}$$

所以 $\forall x \in X, h \circ f(x) = h' \circ f(x) = 1$，故 $h \circ f = h' \circ f$，这推出 $h = h'$，这就说明 $Y = \mathrm{Im} f$，故 f 是满射

(3) $(\Rightarrow)$: 由 f 是双射知，$\forall y \in Y, \exists x_y \in X, \text{s.t. } f(x_y) = y$，我们构造映射

$$\begin{aligned} g: Y &\longrightarrow X \\ y &\longmapsto x_y \end{aligned}$$

则 $\forall y \in Y, f \circ g(y) = f(x_y) = y$，所以 $f \circ g = \mathrm{Id}_Y$；$\forall x \in X, g \circ f(x) = g(f(x)) = x$，所以 $g \circ f = \mathrm{Id}_X$

$(\Leftrightarrow)$: 假设 f 不是满射，则 $\exists y \in Y, \text{s.t. } \forall x \in X, f(x) \neq y$，而 $g(y) \in X, f(g(y)) = y$，矛盾！故 f 是满射；假设 f 不是单射，则 $\exists x_1, x_2 \in X, x_1 \neq x_2, \text{s.t. } f(x_1) = f(x_2)$，所以

$$x_1 = g \circ f(x_1) = g(f(x_1)) = g(f(x_2)) = g \circ f(x_2) = x_2$$

矛盾！故 f 是单射，综上 f 是双射

唯一性：假设 $g_i : X \to Y, g_i \circ f = \mathrm{Id}_X, f \circ g_i = \mathrm{Id}_Y, i = 1, 2$，则

$$g_1 = g_1 \circ \mathrm{Id}_Y = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{Id}_X \circ g_2 = g_2$$

故 g 是唯一的 $\square$

Exercise 2 求证：$\exists$ 双射 $\Phi : \mathrm{Map}(X, \{0,1\}) \xrightarrow{\sim} \mathcal{P}(X)$

Proof 对 $\forall f : X \to \{0,1\}$，我们定义 $X_f = \{x \in X | f(x) = 1\}$，则 $X_f \in \mathcal{P}(X)$，考虑映射

$$\begin{aligned} \Phi : \mathrm{Map}(X, \{0,1\}) &\longrightarrow \mathcal{P}(X) \\ f &\longmapsto X_f \end{aligned}$$

(1).Φ 是单射：假设 $X_f = X_g$，则 $\forall x \in X_f = X_g, f(x) = g(x) = 1, \forall x \notin X_f = X_g, f(x) = g(x) = 0$，所以 $f = g$
(2).Φ 是满射：对 $\forall E \in \mathcal{P}(X)$，考虑映射 $\varphi : X \to \{0,1\}$，满足

$$\varphi(x) = \begin{cases} 1, & x \in E \\ 0, & x \in X \backslash E \end{cases}$$

则 $\Phi(\varphi) = E$，这说明 Φ 是双射 $\square$

Exercise 3 证明存在双射：

(1) $\mathrm{Map}(X \sqcup Y, Z) \xrightarrow{\sim} \mathrm{Map}(X, Z) \times \mathrm{Map}(Y, Z)$

(2) $\mathrm{Map}(X, Y \times Z) \xrightarrow{\sim} \mathrm{Map}(X, Y) \times \mathrm{Map}(X, Z)$

(3)（伴随）$\mathrm{Map}(X \times Y, Z) \xrightarrow{\sim} \mathrm{Map}(X, \mathrm{Map}(Y, Z))$

Proof

(1) 对 $\forall f \in \mathrm{Map}(X \sqcup Y, Z)$，考虑

$$\mathrm{inc}_{X, X \sqcup Y} \circ f \overset{\text{def}}{=} f|_X : X \to Z, \quad \mathrm{inc}_{Y, X \sqcup Y} \circ f \overset{\text{def}}{=} f|_Y : Y \to Z$$

则我们有

$$f(a) = \begin{cases} f|_X(a), & a \in X \\ f|_Y(a), & a \in Y \end{cases}$$

因此我们考虑映射

$$\begin{aligned} \Phi : \mathrm{Map}(X \sqcup Y, Z) &\longrightarrow \mathrm{Map}(X, Z) \times \mathrm{Map}(Y, Z) \\ f &\longmapsto (f|_X, f|_Y) \end{aligned}$$

$(1a)$.Φ 是单射：假设 $\Phi(f) = \Phi(g)$，则 $f|_X = g|_X, f|_Y = g|_Y$，即

$$\begin{cases} X \cap Y = \varnothing \\ \forall x \in X, f(x) = f|_X(x) = g|_X(x) = g(x) \\ \forall y \in Y, f(y) = f|_Y(y) = g|_Y(y) = g(y) \end{cases}$$

所以 $f = g$，故 Φ 是单射

$(1b).\Phi$ 是满射：假设 $(g,h) \in \mathrm{Map}(X,Z)\times\mathrm{Map}(Y,Z)$，则 $g: X\to Z, h: Y\to Z$，考虑映射 $\sigma: X\sqcup Y\to Z$，对应法则如下

$$\begin{cases}\sigma(x)=g(x), \quad x\in X \iff \sigma|_X = g\\ \sigma(y)=h(y), \quad y\in Y \iff \sigma|_Y = h\end{cases}$$

这就说明了 $\Phi(\sigma)=(g,h)$，故 Φ 是满射；综上所述，$\Phi:\mathrm{Map}(X\sqcup Y,Z)\to\mathrm{Map}(X,Z)\times\mathrm{Map}(Y,Z)$ 是双射

(2) 对 $\forall f\in\mathrm{Map}(X,Y\times Z)$，我们可以将 f 写为分量的形式 f_1,f_2，即

$$\begin{aligned} f: X &\longrightarrow Y\times Z\\ x&\longmapsto (f_1(x),f_2(x))\end{aligned}$$

因此我们考虑映射

$$\begin{aligned}\Phi:\mathrm{Map}(X,Y\times Z)&\longrightarrow\mathrm{Map}(X,Y)\times\mathrm{Map}(X,Z)\\ f&\longmapsto (f_1,f_2)\end{aligned}$$

$(2a).\Phi$ 是单射：假设 $\Phi(f)=\Phi(g)$，则 $(f_1,f_2)=(g_1,g_2) \iff f_i=g_i, i=1,2$，这就说明

$$\forall x\in X, f(x)=(f_1(x),f_2(x))=(g_1(x),g_2(x))=g(x)$$

所以 $f=g$，故 Φ 是单射

$(2b).\Phi$ 是满射：假设 $(g,h)\in\mathrm{Map}(X,Y)\times\mathrm{Map}(X,Z)$，则 $g:X\to Y, h: X\to Z$，我们考虑映射 $\sigma: X\to Y\times Z$，对应法则如下

$$\sigma(x)=(g(x),h(x)), \quad \forall x\in X$$

这就说明了 $\Phi(\sigma)=(g,h)$，故 Φ 是满射；综上所述，$\Phi:\mathrm{Map}(X,Y\times Z)\to\mathrm{Map}(X,Y)\times\mathrm{Map}(X,Z)$ 是双射

(3) 对 $\forall f\in\mathrm{Map}(X\times Y,Z)$，固定 $x\in X$，考虑映射 $f_x: Y\to Z$，对应法则如下

$$\begin{aligned} f_x: Y&\longrightarrow Z\\ y&\longmapsto f(x,y)\end{aligned}$$

对 $\forall x\in X$，以及上面对应的 f_x，我们再定义映射 $\Theta_f: X\to\mathrm{Map}(Y,Z)$，对应法则如下

$$\begin{aligned}\Theta_f: X&\longrightarrow\mathrm{Map}(Y,Z)\\ x&\longmapsto f_x\end{aligned}$$

因此我们考虑映射

$$\begin{aligned}\Phi:\mathrm{Map}(X\times Y,Z)&\longrightarrow\mathrm{Map}(X,\mathrm{Map}(Y,Z))\\ f&\longmapsto\Theta_f\end{aligned}$$

$(3a).\Phi$ 是单射：假设 $\Phi(f)=\Phi(g)$，则我们有映射 $\Theta_f: X\to\mathrm{Map}(Y,Z), \Theta_g: X\to\mathrm{Map}(Y,Z)$，且 $\Theta_f=\Theta_g$，故

$$\forall x\in X, f_x=\Theta_f(x)=\Theta_g(x)=g_x$$

因此我们有映射 $f_x,g_x: Y\to Z$，且 $f_x=g_x$，即

$$\forall y\in Y, f(x,y)=f_x(y)=g_x(y)=g(x,y)$$

由 x 的任意性知，$f(x,y)=g(x,y),\forall(x,y)\in X\times Y$，即 $f=g$，故 Φ 是单射

$(3b).\Phi$ 是满射：假设 $\Theta \in \mathrm{Map}(X, \mathrm{Map}(Y, Z))$，则 $\forall x \in X$，我们有映射 $\Theta(x) : Y \to Z$，对应法则如下

$$\begin{aligned} \Theta(x) : Y &\longrightarrow Z \\ y &\longmapsto \big(\Theta(x)\big)(y) \end{aligned}$$

则对 $\forall (x, y) \in X \times Y$，我们定义映射

$$\begin{aligned} \theta : X \times Y &\longrightarrow Z \\ (x, y) &\longmapsto \big(\Theta(x)\big)(y) \end{aligned}$$

***Claim*:** $\Phi(\theta) = \Theta_\theta = \Theta$

pf of Claim：因为 $\forall x \in X$，同上构造我们可以得到映射 θ_x：

$$\begin{aligned} \theta_x : Y &\longrightarrow Z \\ y &\longmapsto \theta(x, y) = \big(\Theta(x)\big)(y) \end{aligned}$$

由 x, y 的任意性知，$\Theta_\theta(x, y) = \Theta(x, y), \forall (x, y) \in X \times Y$，这样断言就得证了，因此我们找到了 Θ 的原像 θ，故 Φ 是满射；综上所述，$\Phi : \mathrm{Map}(X \times Y, Z) \to \mathrm{Map}(X, \mathrm{Map}(Y, Z))$ 是双射 $\square$

Exercise 4 求证：在一个等价关系中，设 $[a], [a']$ 是两个等价类，则有 $[a] \cap [a'] \neq \varnothing \iff [a] = [a']$

Proof $(\Rightarrow)$: 假设 $x \in [a] \cap [a']$，则

$$\begin{cases} x \in [a] \Rightarrow x \overset{\mathrm{R}}{\sim} a \\ x \in [a'] \Rightarrow x \overset{\mathrm{R}}{\sim} a' \end{cases}$$

由对称性与传递性得

$$x \overset{\mathrm{R}}{\sim} a \Longrightarrow a \overset{\mathrm{R}}{\sim} x \overset{x \overset{\mathrm{R}}{\sim} a'}{\Longrightarrow} a \sim a'$$

一方面，$\forall y \in [a], y \overset{\mathrm{R}}{\sim} a \overset{a \overset{\mathrm{R}}{\sim} a'}{\Longrightarrow} y \overset{\mathrm{R}}{\sim} a'$，故 $y \in [a']$，进而 $[a] \subseteq [a']$

另一方面，$\forall y \in [a'], y \overset{\mathrm{R}}{\sim} a' \overset{a' \overset{\mathrm{R}}{\sim} a}{\Longrightarrow} y \sim a$，故 $y \in [a]$，进而 $[a'] \subseteq [a]$，因此 $[a] = [a']$

$(\Leftarrow)$: 这是平凡的，因为 $[a] \cap [a'] = [a]$ 非空 $\square$

Exercise 5 设 $P : \{X_i | i \in I\}$ 是 X 上的一个分拆，定义关系 $\overset{P}{\sim}$：

$$x \overset{P}{\sim} y \iff \exists i \in I, \text{s.t. } x, y \in X_i$$

验证 $\overset{P}{\sim}$ 是一个等价关系

Proof

(1). 自反性：由 $P = \{X_i | i \in I\}$ 是 X 的一个分拆知

$$X = \bigsqcup_{i \in I} X_i$$

$\forall x \in X$，一定存在唯一的 $X_i \in \{X_i | i \in I\}, \text{s.t. } x \in X_i$，故 $x \overset{\mathrm{P}}{\sim} x$

(2). 对称性：假设 $x \overset{\mathrm{P}}{\sim} y$，则 $\exists i \in I, \text{s.t. } x, y \in X_i$，故显然有 $y \overset{\mathrm{P}}{\sim} x$

(3). 传递性：假设 $x \overset{\mathrm{P}}{\sim} y, y \overset{\mathrm{P}}{\sim} z$，则 $\exists X_i, X_j, \text{s.t. } x, y \in X_i$、$y, z \in X_j$ 由分拆是无交并知，$y \in X_i \cap X_j \Rightarrow X_i = X_j$，则 $x, z \in X_i = X_j$，故 $x \overset{\mathrm{P}}{\sim} z$ $\square$

Exercise 6 设 $f:X\to Y$，考虑等价关系 $\overset{f}{\sim}$，则 f 诱导双射

$$\begin{aligned}\bar{f}: X/\overset{f}{\sim} &\longrightarrow \operatorname{Im}(f)\\ [x] &\longmapsto f(x)\end{aligned}$$

若 $\exists h: X/\overset{f}{\sim}\to \operatorname{Im}(f)$，满足 $f=\operatorname{inc}\circ h\circ\pi_f$，则 $h=\bar{f}$

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, two heads, "\pi_f"'] & Y \\ X/\overset{f}{\sim} \arrow[r, "\bar{f}"] & \operatorname{Im}(f) \arrow[u, "\operatorname{inc}"'] \end{tikzcd} \qquad \begin{tikzcd} x \arrow[r, mapsto, "f"] \arrow[d, mapsto, "\pi_f"'] & f(x) \\ {[x]} \arrow[r, mapsto, "\bar{f}"] & f(x) \arrow[u, mapsto, "\operatorname{inc}"'] \end{tikzcd}$$

Proof 因为 $f=\operatorname{inc}\circ\bar{f}\circ\pi_f=\operatorname{inc}\circ h\circ\pi_f$，所以对 $\forall x\in X$

$$\begin{cases} f(x)=\operatorname{inc}\circ\bar{f}\circ\pi_f(x)=\operatorname{inc}\circ\bar{f}([x])\\ f(x)=\operatorname{inc}\circ h\circ\pi_f(x)=\operatorname{inc}\circ h([x])\end{cases}$$

因为 $\pi_f: X\to X/\overset{f}{\sim}$ 是满射，故遍历所有 $x\in X$，我们得到 $\forall[x]\in X, \operatorname{inc}\circ\bar{f}([x])=\operatorname{inc}\circ h([x])\Rightarrow \operatorname{inc}\circ\bar{f}=\operatorname{inc}\circ h$，因为 inc 是单射，*Exercise 1* 已证单射满足左消去律，所以 $\bar{f}=h$ □

Exercise 7 求证：设 R 是环，0_R 为 R 中的零元素，则 $-0_R=0_R$；$\forall a\in R, -(-a)=a$

Proof 因为 $0_R+0_R=0_R$，且负元唯一，所以我们有 $-0_R=0_R$；因为 $-a$ 是 a 的负元，所以 $a+(-a)=0$，故 a 是 $-a$ 的负元，即 $-(-a)=a$ □

Exercise 8 在同余类环 $\mathbb{Z}_n=\{\bar{0},\bar{1},\cdots,\overline{n-1}\}$ 中定义加法与乘法

$$\bar{i}+\bar{j}=\overline{i+j},\quad \bar{i}\cdot\bar{j}=\overline{i\cdot j}$$

验证这样的加法、乘法是良定的

Proof 设 $\bar{i}=\bar{i}_0,\bar{j}=\bar{j}_0$，因为

$$\begin{cases}\bar{i}=\bar{i}_0 \iff i\equiv i_0 \mod n \iff n\mid i-i_0\\ \bar{j}=\bar{j}_0 \iff j\equiv j_0 \mod n \iff n\mid j-j_0\end{cases}$$

所以 $n\mid(i-i_0)+(j-j_0)=(i+j)-(i_0+j_0)$，故 $i+j\equiv i_0+j_0 \mod n \iff \overline{i+j}=\overline{i_0+j_0}$，故加法是良定的；又因为 $n\mid j(i-i_0)+i_0(j-j_0)=ij-i_0j_0$，故 $ij\equiv i_0j_0 \mod n\iff \overline{ij}=\overline{i_0j_0}$，故乘法是良定的 □

Exercise 9 设 R 是环，$a\in R, n\in\mathbb{Z}$，定义 a 的 n 倍 na：

$$na=\begin{cases}0_R, \quad n=0\\ \overbrace{a+\cdots+a}^{n\text{个}}, \quad n>0\\ \overbrace{(-a)+\cdots+(-a)}^{-n\text{个}}, \quad n<0\end{cases}$$

证明：$\forall m,n\in\mathbb{Z}, a\in R$，有 $(n+m)a=na+ma$

Proof

***Case** 1.* $n,m>0$，则 $(n+m)a=\overbrace{a+\cdots+a}^{(n+m)\text{个}}=\overbrace{(a+\cdots+a)}^{n\text{个}}+\overbrace{(a+\cdots+a)}^{m\text{个}}=na+ma$

***Case** 2.* $n,m<0$，则 $(n+m)a=\overbrace{(-a)+\cdots+(-a)}^{-(n+m)\text{个}}=\overbrace{[(-a)+\cdots+(-a)]}^{-n\text{个}}+\overbrace{[(-a)+\cdots+(-a)]}^{-m\text{个}}=na+ma$

***Case** 3.* n,m 异号，不妨设 $n>0>m$

***Case** 3.1* $n+m=0$，即 $m=-n$，则

$$\begin{aligned}
na+(-n)a&=\overbrace{(a+\cdots+a)}^{n\text{个}}+\overbrace{[(-a)+\cdots+(-a)]}^{(-n)\text{个}}=\overbrace{(a+\cdots+a)}^{(n-1)\text{个}}+[a+(-a)]+\overbrace{[(-a)+\cdots+(-a)]}^{(-n+1)\text{个}}\\
&=\overbrace{(a+\cdots+a)}^{(n-1)\text{个}}+\overbrace{[(-a)+\cdots+(-a)]}^{(-n+1)\text{个}}\overset{\text{同理}}{=\!=}\overbrace{(a+\cdots+a)}^{(n-2)\text{个}}+\overbrace{[(-a)+\cdots+(-a)]}^{(-n+2)\text{个}}\\
&\qquad\qquad\cdots\cdots\cdots\\
&=a+(-a)=0_R=0a=(m+n)a
\end{aligned}$$

***Case** 3.2* $(n+m)>0$，则 $na=[(n+m)+(-m)]a=(n+m)a+(-m)a$，故

$$\begin{aligned}
na+ma&=[(n+m)a+(-m)a]+(ma)=(n+m)a+[(-m)a+(ma)]\\
&=(n+m)a
\end{aligned}$$

***Case** 3.3* $(n+m)<0$，由 *Case 3.1* 知，$(-n)a$ 与 na 互为逆元，而由 *Case 3.2* 知 $(-n-m)a=(-n)a+(-m)a$，因此

$$\begin{aligned}
(n+m)a&=-[(-n-m)a]=-[(-n)a+(-m)a]\\
&=-[(-n)a]-[(-m)a]\\
&=na+ma
\end{aligned}$$

□

Exercise 10 求证：对 $\forall n\in\mathbb{Z},a\in R$，有 $na=(n1_R)\cdot a$

Proof

***Case** 1.* $n=0$，则 $LHS=0a=0_R,RHS=(01_R)\cdot a=0_R\cdot a=0_R$，故 $LHS=RHS=0_R$

***Case** 2.* $n>0$，当 $n=1$ 时，$LHS=1a=a,RHS=(1\cdot 1_R)\cdot a=1_R\cdot a=a$，故 $LHS=RHS$；假设 $n=k$ 时命题成立，下证 $n=k+1$ 时，因为

$$(k+1)a=ka+a=(k1_R)\cdot a+1_R\cdot a=(k1_R+1_R)\cdot a=[(k+1)1_R]\cdot a$$

由数学归纳法知，命题对 $\forall n>0$ 成立

***Case** 3.* $n<0$，因为 $-n>0$，故由 *Case 2* 可知

$$\begin{cases}na+(-n)a=0_R\\(n1_R)\cdot a+(-n)a=(n1_R)\cdot a+(-n1_R)\cdot a=[n1_R+(-n)1_R]\cdot a=(0\cdot 1_R)\cdot a=0_R\cdot a=0_R\end{cases}$$

由 $(-n)a$ 的逆元唯一知，$na=(n1_R)\cdot a$

□

Exercise 11 求证：对 $\forall a,b\in R, n\in\mathbb{Z}$，有 $a\cdot(nb)=n(a\cdot b)=(na)\cdot b$

Proof ***Case*** *1.* $n=0$，我们有

$$\begin{cases}a\cdot(0b)=a\cdot 0_R=0_R\\0(a\cdot b)=0_R\\(0a)\cdot b=0_R\cdot b=0_R\end{cases}$$

Case *2.* $n>0$，当 $n=1$ 时，显然三者都等于 $a\cdot b$；假设 $n=k$ 时命题成立，下证 $n=k+1$ 时，因为

$$\begin{cases}a\cdot[(k+1)b]=a\cdot(kb+b)=a\cdot(kb)+a\cdot b=k(a\cdot b)+a\cdot b=(k+1)(a\cdot b)\\ [(k+1)a]\cdot b=(ka+a)\cdot b=(ka)\cdot b+a\cdot b=k(a\cdot b)+a\cdot b=(k+1)(a\cdot b)\end{cases}$$

由数学归纳法知，命题对 $\forall n>0$ 成立

Case *3.* $n<0$，此时 $(-n)>0$，我们有 $a\cdot(-nb)=(-n)(a\cdot b)=(-na)\cdot b$，所以

$$\begin{cases}a\cdot(nb)+(-n)(a\cdot b)=a\cdot(nb)+a\cdot(-nb)=a\cdot[nb+(-nb)]=a\cdot 0_R=0_R\\n(a\cdot b)+(-n)(a\cdot b)=[n+(-n)](a\cdot b)=0_R\\(na)\cdot b+(-n)(a\cdot b)=(na)\cdot b+(-na)\cdot b=[na+(-na)]\cdot b=0_R\cdot b=0_R\end{cases}$$

由 $(-n)(a\cdot b)$ 的逆元唯一知，$a\cdot(nb)=n(a\cdot b)=(na)\cdot b$ □

Exercise 12 求证：设 R 为环，$\forall n,m\in\mathbb{N}^*$，$a_1,\cdots,a_n,b_1,\cdots,b_m\in R$，有

$$\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{n}(a_i\cdot b_j)$$

Proof 固定 $m=1$，当 $n=1$ 时，命题平凡成立，设 $n=k$ 时命题成立，当 $n=k+1$ 时

$$\left(\sum_{i=1}^{k+1}a_i\right)\cdot b_1=\left[\left(\sum_{i=1}^{k}a_i\right)+a_{i+1}\right]\cdot b_1=\left(\sum_{i=1}^{k}a_i\right)\cdot b_1+a_{i+1}\cdot b_1=\sum_{i=1}^{k}(a_i\cdot b_1)+(a_{i+1}\cdot b_1)=\sum_{i=1}^{k+1}(a_i\cdot b_1)$$

由数学归纳法知，对 $\forall n\in\mathbb{N}^*$，均有

$$\left(\sum_{i=1}^{n}a_i\right)\cdot b_1=\sum_{i=1}^{n}(a_i\cdot b_1)$$

类似地，固定 $n=1$ 时，对 $\forall m\in\mathbb{N}^*$，我们有

$$a_1\cdot\sum_{j=1}^{m}b_j=\sum_{j=1}^{m}(a_1\cdot b_j)$$

因此，固定 $m=1$ 时，对 $\forall n\in\mathbb{N}^*$，命题均成立，所以

$$\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right)=\sum_{i=1}^{n}\left[a_i\cdot\left(\sum_{j=1}^{m}b_j\right)\right]=\sum_{i=1}^{n}\left(\sum_{j=1}^{m}(a_i\cdot b_j)\right)=\sum_{i=1}^{n}\sum_{j=1}^{m}(a_i\cdot b_j)$$

□

Exercise 13 证明含幺交换环上的二项式定理：$\forall a,b\in R,n\in\mathbb{N}^*$，则

$$(a+b)^n=\sum_{i=0}^{n}\binom{n}{i}a^ib^{n-i}$$

Proof $n=1$ 时，命题平凡成立，假设 $n=k-1,k\geq 2$ 时命题成立，则当 $n=k$ 时

$$\begin{aligned}(a+b)^k&=(a+b)(a+b)^{k-1}=a\sum_{i=0}^{k-1}\binom{k-1}{i}a^ib^{(k-1)-i}+b\sum_{j=0}^{k-1}\binom{k-1}{j}a^jb^{(k-1)-j}\\&=\sum_{i=0}^{k-1}\binom{k-1}{i}a^{i+1}b^{(k-1)-i}+\sum_{j=0}^{k-1}\binom{k-1}{j}a^jb^{(k-1)-j+1}\\&=a^k+\sum_{i=0}^{k-2}\binom{k-1}{i}a^{i+1}b^{(k-1)-i}+\sum_{j=1}^{k-1}\binom{k-1}{j}a^jb^{k-j}+b^k\end{aligned}$$

令 $i+1=j$，则 $1\leq j\leq k-1$，再结合 $\binom{k-1}{j-1}+\binom{k-1}{j}=\binom{k}{j}$ 得

$$\begin{aligned}(a+b)^k&=a^k+\sum_{j=1}^{k-1}\binom{k-1}{j-1}a^jb^{k-j}+\sum_{j=1}^{k-1}\binom{k-1}{j}a^jb^{k-j}+b^k\\&=\binom{k}{k}a^kb^0+\sum_{j=1}^{k-1}\left[\binom{k-1}{j-1}a^jb^{k-j}+\binom{k-1}{j}a^jb^{k-j}\right]+\binom{k}{0}a^0b^k\\&=\binom{k}{k}a^kb^0+\sum_{j=1}^{k-1}\binom{k}{j}a^jb^{k-j}+\binom{k}{0}a^0b^k\\&=\sum_{j=0}^{k}\binom{k}{j}a^jb^{k-j}\end{aligned}$$

由数学归纳法知，对 $\forall n\in\mathbb{N}^*$，含幺交换环上的二项式定理均成立 □

Exercise 14 求证：$U(\mathbb{Z}_n)=\{\overline{a}|\,\gcd(a,n)=1\}$

Proof 对 $\forall\overline{a}\in\mathbb{Z}_n$，若 $\overline{a}$ 可逆，则 $\exists\overline{x}\in\mathbb{Z}_n,\text{s.t.}\ \overline{a}\cdot\overline{x}=\overline{ax}=1$，即同余方程

$$ax\equiv 1\mod n$$

有解，假设存在解 x_0，则 $ax_0\equiv 1\mod n$，即 $n\mid ax_0-1$，所以 $\exists y,\text{s.t.}\ ax_0-1=ny$，即 $ax_0+ny=1$，由贝祖定理得，$\gcd(a,n)=1$；反之，若 $\gcd(a,n)\neq 1$，则不存在 $x,y,\text{s.t.}\ ax+ny=1$，则不存在 $x\in\mathbb{Z},\text{s.t.}\ ax\equiv 1\mod n$，即 $\overline{a}$ 不存在逆元，综上所述

$$U(\mathbb{Z}_n)=\{\overline{a}|\,\gcd(a,n)=1\}$$

□