近世代数 (H) 第二周作业

涂嘉乐 PB23151786

2025 年 3 月 9 日

Exercise 1 设 R 为含幺交换环，且 R 为有限环，求证：R 是整环 $\iff$ R 是域

Proof $(\Leftarrow)$: 由 R 是域知，若 $\exists a,b \in R, \text{s.t. } ab = 0_R$，若 $a \neq 0_R$，则 a 可逆，两边同时左乘 a^{-1} 可得 $b = 0_R$，故 R 是整环

$(\Rightarrow)$: 由 R 有限知，可设 $R = \{a_0, a_1, \cdots, a_n\}$，且 $a_0 = 0_R, a_1 = 1_R$，对 $\forall r \in R\backslash\{0_R\}$，考虑

$$Rr = \{a_0 r, a_1 r, \cdots, a_n r\} \tag{0.1}$$

首先，$Rr \subseteq R$；其次，由 R 是整环，满足消去律知，$\forall i \neq j$，若 $a_i r = a_j r$，则 $a_i = a_j$，这就说明了 Rr 中的元素两两不同，故 $\#Rr = \#R$，再结合包含关系知，$Rr = R, \forall r \neq 0_R$，从而 $\exists i_r \in \{1, \cdots, n\}, \text{s.t. } a_{i_r} r = 1_R$，因此 $r^{-1} = a_{i_r}$，由 r 的任意性知，R 中任意非零元均可逆，故 R 为域 □

Exercise 2 分类 $\mathbb{Q}$ 的子环

Proof 设 $S \subseteq \mathbb{Q}$ 是子环，则 $1 \in S \Rightarrow -1, 0 \in S$，进而有 $\mathbb{Z} \in S$，这是因为 $\forall n \in \mathbb{Z}$，$n > 0$ 时看作 n 个 1 相加；$n < 0$ 时看作 $(-n)$ 个 (-1) 相加

Case 1. $S = \mathbb{Z}$ 为 $\mathbb{Q}$ 的子环

Case 2. $S \supsetneqq \mathbb{Z}$，考虑全体素数的集合 $\mathcal{P}$ 的子集

$$P = \left\{ m\text{的素因子} \left| \frac{n}{m} \in S, \text{且为既约分数} \right. \right\} \subseteq \mathcal{P}$$

由 $S \supsetneqq \mathbb{Z}$ 知，$\exists \frac{x}{y} \in S$，且它是既约分数，因此 y 的素因子一定属于 P，故 P 非空，我们考虑集合

$$\mathbb{Z}_P = \left\{ \frac{n}{\prod\limits_{p_i \in P} p_i^{e_i}} \left| n \in \mathbb{Z}, e_i \in \mathbb{N} \right. \right\}$$

则 $\mathbb{Z}_P$ 是一个子环，这是因为 $1 = \frac{1}{\prod\limits_{p_i \in P} p_i^0} \in \mathbb{Z}_P$；且 $\forall x, y \in \mathbb{Z}_P$，根据 $\mathbb{Z}_P$ 的定义，我们可以写为

$$x = \frac{n_x}{\prod\limits_{p_i \in P} p_i^{e_{i_x}}}, \quad y = \frac{n_y}{\prod\limits_{p_i \in P} p_i^{e_{i_y}}}$$

所以

$$\begin{cases} x \pm y = \dfrac{n_x \prod\limits_{p_i \in P} p_i^{\max\{e_{i_x}, e_{i_y}\} - e_{i_x}} \pm n_y \prod\limits_{p_i \in P} p_i^{\max\{e_{i_x}, e_{i_y}\} - e_{i_y}}}{\prod\limits_{p_i \in P} p_i^{\max\{e_{i_x}, e_{i_y}\}}} \in S \\ xy = \dfrac{n_x n_y}{\prod\limits_{p_i \in P} p_i^{e_{i_x} + e_{i_y}}} \in S \end{cases}$$

故首先，$\mathbb{Z}_P$ 是子环

Claim：$S = \mathbb{Z}_P$

①.$S\subseteq\mathbb{Z}_P$：$\forall s\in S$，若 $s\in\mathbb{Z}$，则 $s=\frac{s}{\prod\limits_{p_i\in P}p_i^0}\in\mathbb{Z}_P$；若 $s\notin\mathbb{Z}$，则 $\forall$既约分数$\frac{x}{y}\in S$，我们有 y 的素因子分解

$$y=p_1^{e_1}\cdots p_t^{e_t}$$

由 P 的定义知，$p_1,\cdots,p_t\in P$，这就说明 $\frac{x}{y}=\frac{x}{p_1^{e_1}\cdots p_s^{e_s}}\in\mathbb{Z}_P$

②.$\mathbb{Z}_P\subseteq S$：对 $\forall p_0\in P$，由 P 的定义知，$\exists$既约分数$\frac{n}{m}\in S,\text{s.t.}\ p_0$ 为 m 的素因子，我们设 m 有素因子分解

$$m=p_0^{e_0}p_1^{e_1}\cdots p_s^{e_s}$$

则由子环对乘法封闭知

$$\frac{n}{p_0}=\frac{n}{m}\cdot p_0^{e_0-1}p_1^{e_1}\cdots p_s^{e_s}\in S$$

因为 $(n,m)=1$，由贝祖等式，$\exists u,v\in\mathbb{Z},\text{s.t.}\ nu+mv=1$，将 m 用 $p_0^{e_0}p_1^{e_1}\cdots p_s^{e_s}$ 代入得

$$nu+p_0(p_0^{e_0-1}p_1^{e_1}\cdots p_s^{e_s}v)=1$$

所以

$$\frac{1}{p_0}=u\cdot\frac{n}{p_0}+p_0^{e_0-1}p_1^{e_1}\cdots p_s^{e_s}\in S$$

进而，$\forall p\in P,\frac{1}{p}\in S$，则 $\forall x\in\mathbb{Z}_P$，我们有

$$x=\frac{n}{\prod\limits_{p_i\in P}p_i^{e_i}}=n\cdot\prod_{i\in I}\left(\frac{1}{p_i}\right)^{e_i}\in S$$

这就说明了 $\mathbb{Z}_P\subseteq S$，实际上，当 $P=\varnothing\subseteq\mathcal{P}$ 时，$\mathbb{Z}_P=\mathbb{Z}_\varnothing=\mathbb{Z}$，因此每个 $\mathbb{Q}$ 的子环，均 $\exists P\subseteq\mathcal{P}$（$\mathcal{P}$ 为全体素数的集合），使得 $S=\mathbb{Z}_P$，且 P 由 S 中的元素唯一确定 $\square$

Exercise 3 设 R,S 是环，$\theta:R\to S$ 为环同态，求证：$\forall a,b\in R,\theta(a-b)=\theta(a)-\theta(b)$

Proof 因为 $0_S=\theta(0_R)=\theta(a+(-a))=\theta(a)+\theta(-a)$，所以 $\theta(-a)=-\theta(a)$，进而

$$\theta(a-b)=\theta(a+(-b))=\theta(a)+\theta(-b)=\theta(a)-\theta(b)$$

$\square$

Exercise 4 证明：不存在环同态 $\theta:\mathbb{Z}_8\to\mathbb{Q}$

Proof 假设存在环同态 $\theta:\mathbb{Z}_8\to\mathbb{Q}$，则 $\theta(\bar{1})=1\Rightarrow\forall n,\theta(\bar{n})=n$，所以

$$9=\theta(\bar{9})=\theta(\bar{1})=1\quad\text{in }S$$

矛盾！ $\square$

Exercise 5 证明：$\mathrm{Aut}(\mathbb{Z}[\sqrt{-1}])=\{\mathrm{Id}_{\mathbb{Z}[\sqrt{-1}]},\tau\}$，其中

$$\begin{aligned}\tau:\mathbb{Z}[\sqrt{-1}]&\longrightarrow\mathbb{Z}[\sqrt{-1}]\\ a+b\sqrt{-1}&\longmapsto a-b\sqrt{-1}\end{aligned}$$

Proof 设 $\theta\in\mathrm{Aut}(\mathbb{Z}[\sqrt{-1}])$，则 $\theta(1)=1$，先证明 $\theta(n)=n,\forall n\in\mathbb{Z}$

$n>0$ 时，因为 $\theta(2)=\theta(1+1)=\theta(1)+\theta(1)=1+1=2$，假设命题对 $n=k$ 成立，则当 $n=k+1$ 时

$$\theta(k+1)=\theta(k)+\theta(1)=k+1$$

故 $n>0$ 时命题成立

$n=0$ 时，因为 *Exercise 3* 证明环同态保持减法，所以 $\theta(0)=\theta(1-1)=\theta(1)-\theta(1)=1-1=0$

$n<0$ 时，此时 $-n>0$，则有 $\theta(-n)=-n$，进而 $\theta(n)=-\theta(-n)=n$

这就证明了 θ 在 $\mathbb{Z}$ 上的限制为恒等映射，接下来考虑 $\theta(\sqrt{-1})$，因为

$$\theta(\sqrt{-1})^2=\theta(\sqrt{-1})\theta(\sqrt{-1})=\theta(-1)=-1$$

所以 $\theta(\sqrt{-1})=\pm\sqrt{-1}$

Case 1. $\theta(\sqrt{-1})=\sqrt{-1}$，则 $\forall m+n\sqrt{-1}\in\mathbb{Z}[\sqrt{-1}]$，有

$$\begin{aligned}\theta(m+n\sqrt{-1})&=\theta(m)+\theta(n)\theta(\sqrt{-1})\\&=m+n\sqrt{-1}\end{aligned}$$

故 $\theta=\mathrm{Id}_{\mathbb{Z}[\sqrt{-1}]}$

Case 2. $\theta(\sqrt{-1})=-\sqrt{-1}$，则 $\forall m+n\sqrt{-1}\in\mathbb{Z}[\sqrt{-1}]$，有

$$\begin{aligned}\theta(m+n\sqrt{-1})&=\theta(m)+\theta(n)\theta(\sqrt{-1})\\&=m-n\sqrt{-1}\end{aligned}$$

故 $\theta=\tau$

这就说明 $\mathrm{Aut}(\mathbb{Z}[\sqrt{-1}])\subseteq\{\mathrm{Id},\tau\}$，反之，因为 $\mathrm{Id}_{\mathbb{Z}[\sqrt{-1}]}$ 显然为环同构，对于 τ，因为

1. $\tau(1)=1$
2. $\tau((a+b\sqrt{-1})+(c+d\sqrt{-1}))=(a+c)-(b+d)\sqrt{-1}=(a-b\sqrt{-1})+(c-d\sqrt{-1})=\tau(a+b\sqrt{-1})+\tau(c+d\sqrt{-1})$
3. $\tau((a+b\sqrt{-1})(c+d\sqrt{-1}))=(ac-bd)-(ad+bc)\sqrt{-1}=(a-b\sqrt{-1})(c-d\sqrt{-1})=\tau(a+b\sqrt{-1})\tau(c+d\sqrt{-1})$
4. $\tau(a+b\sqrt{-1})=\tau(a'+b'\sqrt{-1})\iff a-b\sqrt{-1}=a'-b'\sqrt{-1}\iff a=a',b=b'\iff a-b\sqrt{-1}=a'-b'\sqrt{-1}$
   故 τ 是单射
5. $\forall a+b\sqrt{-1}\in\mathbb{Z}[\sqrt{-1}],\tau(a-b\sqrt{-1})=a+b\sqrt{-1}$，故 τ 是满射

综上所述，τ 为环自同构，这就说明 $\{\mathrm{Id}_{\mathbb{Z}[\sqrt{-1}]},\tau\}\subseteq\mathrm{Aut}(\mathbb{Z}[\sqrt{-1}])$，故有 $\mathrm{Aut}(\mathbb{Z}[\sqrt{-1}])=\{\mathrm{Id},\tau\}$ □

Exercise 6 证明：$\mathrm{Aut}(\mathbb{Q}[\sqrt{-1}])=\{\mathrm{Id}_{\mathbb{Q}[\sqrt{-1}]},\tau\}$，其中

$$\begin{aligned}\tau:\mathbb{Q}[\sqrt{-1}]&\longrightarrow\mathbb{Q}[\sqrt{-1}]\\a+b\sqrt{-1}&\longmapsto a-b\sqrt{-1}\end{aligned}$$

Proof 设 $\theta\in\mathrm{Aut}(\mathbb{Q}[\sqrt{-1}])$，我们首先证明 $\theta|_{\mathbb{Q}}=\mathrm{Id}_{\mathbb{Q}}$，即 $\theta(a)=a,\forall a\in\mathbb{Q}$

同 *Exercise 5* 完全一样的过程，我们有 $\theta|_{\mathbb{Z}}=\mathrm{Id}_{\mathbb{Z}}$，因为

$$1=\theta(1)=\theta\left(n\cdot\frac{1}{n}\right)=\theta(n)\theta\left(\frac{1}{n}\right)=n\cdot\theta\left(\frac{1}{n}\right)\Rightarrow\theta\left(\frac{1}{n}\right)=\frac{1}{n},\quad\forall n\in\mathbb{Z}\backslash\{0\}$$

所以 $\forall\frac{m}{n}\in\mathbb{Q}$，我们有

$$\theta\left(\frac{m}{n}\right)=\theta\left(m\cdot\frac{1}{n}\right)=\theta(m)\theta\left(\frac{1}{n}\right)=\frac{m}{n}$$

这就说明了 $\theta|_{\mathbb{Q}}=\mathrm{Id}_{\mathbb{Q}}$，接下来考虑 $\theta(\sqrt{-1})$，因为

$$\theta(\sqrt{-1})^2=\theta(\sqrt{-1})\theta(\sqrt{-1})=\theta(-1)=-1$$

所以 $\theta(\sqrt{-1})=\pm\sqrt{-1}$，接下来的过程与 *Exercise 5* 完全一致，故 $\mathrm{Aut}(\mathbb{Z}[\sqrt{-1}])=\{\mathrm{Id}_{\mathbb{Z}[\sqrt{-1}]},\tau\}$ $\square$

Exercise 7 设 $\theta: R\xrightarrow{\sim} S$ 为环同构，求证：

1. $a\in U(R)\iff\theta(a)\in U(S)$
2. 群同构：$U(R)\xrightarrow{\sim} U(S)$
3. R 是整环 $\iff$ S 是整环
4. 群同构：$\mathrm{Aut}(R)\xrightarrow{\sim}\mathrm{Aut}(S)$

Proof

1. $(\Rightarrow)$：因为 $a\in U(R)$，所以

$$1_S=\theta(1_R)=\theta(a\cdot a^{-1})=\theta(a)\theta(a^{-1})\Rightarrow\theta(a)^{-1}=\theta(a^{-1})\Rightarrow\theta(a)\in U(S)$$

   $(\Leftarrow)$：因为 $\theta(a)\in U(S)$，所以 $\exists s\in S,\text{s.t.}\ \theta(a)s=1_S$，又因为 θ 是双射，故是满射，所以 $\exists r\in R,\text{s.t.}\ \theta(r)=s$，进而我们有

$$\theta(ar)=\theta(a)\theta(r)=1_S$$

   由 $\theta(1_R)=\theta(1_S)$，且 θ 是单射知，$ar=1_R$，故 $a^{-1}=r,a\in U(R)$

2. 考虑 $\theta:(U(R),\cdot)\to(U(S),\cdot)$，由环同态知

$$\theta(ab)=\theta(a)\theta(b),\quad\forall a,b\in U(R)$$

   这就说明 θ 是群同态，下证 θ 是双射

   单射：若 $\theta(a)=\theta(b)\in U(S)$，则 $1_S=\theta(a)\theta(b)^{-1}=\theta(a)\theta(b^{-1})=\theta(ab^{-1})=\theta(1_R)$，因此 $ab^{-1}=1_R\Rightarrow a=b$

   满射：对 $\forall s\in U(S)\subseteq S$，由 $\theta:R\to S$ 是满射知，$\exists r\in R,\text{s.t.}\ \theta(r)=s$，由因为 $s\in U(S)$，所以 s 可逆且 $s^{-1}\in U(S)\subseteq S$，故 $\exists r'\in R,\text{s.t.}\ \theta(r')=s$，所以

$$1_S=s\cdot s^{-1}=\theta(r)\theta(r')=\theta(rr')=\theta(1_R)$$

   这就说明 $rr'=1_R$，故 $r\in U(R)$，即 $\forall s\in U(S)$，都能找到 $r\in U(R),\text{s.t.}\ \theta(r)=s$，故为满射，因此 θ 是群同构

3. 先证明 θ^{-1} 也是环同构：由 θ 是双射知，θ^{-1} 也是双射，故只需证明 θ^{-1} 是环同态，对 $\forall x,y\in S$，因为

$$\begin{cases}\theta(\theta^{-1}(x+y))=x+y\\ \theta(\theta^{-1}(x)+\theta^{-1}(y))=\theta(\theta^{-1}(x))+\theta(\theta^{-1}(y))=x+y\end{cases}$$

$$\begin{cases}\theta(\theta^{-1}(xy))=xy\\ \theta(\theta^{-1}(x)\theta^{-1}(y))=\theta(\theta^{-1}(x))\theta(\theta^{-1}(y))=xy\end{cases}$$

   所以 $\theta^{-1}(x+y)=\theta^{-1}(x)+\theta^{-1}(y),\theta^{-1}(xy)=\theta^{-1}(x)\theta^{-1}(y)$，又因为 $\theta^{-1}(1_S)=1_R$，故 θ^{-1} 也是环同构

   $(\Rightarrow)$：若 R 是整环，因为 $\forall s\in S,s=0_S\iff\theta^{-1}(s)=0_R$，所以

$$\forall a,b\in S\backslash\{0\},\theta^{-1}(a),\theta^{-1}(b)\neq 0_S\Rightarrow\theta^{-1}(ab)=\theta^{-1}(a)\theta^{-1}(b)\overset{R\text{整环}}{\neq}0_R\Rightarrow ab\neq 0_S$$

   故 S 是整环

$(\Leftarrow)$: 若 S 是整环，因为 $\forall r \in R, r = 0_R \iff \theta(r) = 0_S$，所以

$$\forall a, b \in R \backslash \{0\}, \theta(a), \theta(b) \neq 0_S \Rightarrow \theta(ab) = \theta(a)\theta(b) \overset{S\text{整环}}{\neq} 0_S \Rightarrow ab \neq 0_R$$

故 R 是整环

4. 前面已证：若 $\theta : R \to S$ 是环同构，则 $\theta^{-1} : S \to R$ 也是环同构。考虑映射

$$\begin{aligned} \Theta : \mathrm{Aut}(R) &\longrightarrow \mathrm{Aut}(S) \\ \varphi &\longmapsto \theta \circ \varphi \circ \theta^{-1} \end{aligned}$$

Step 1. 验证 $\forall \varphi \in \mathrm{Aut}(R), \theta \circ \varphi \circ \theta^{-1} \in \mathrm{Aut}(S)$

(1.1). 同态：$\forall x, y \in S$

$$\begin{aligned} \theta \circ \varphi \circ \theta^{-1}(x+y) &= \theta \circ \varphi(\theta^{-1}(x+y)) = \theta \circ \varphi(\theta^{-1}(x) + \theta^{-1}(y)) \\ &= \theta(\varphi(\theta^{-1}(x)) + \varphi(\theta^{-1}(y))) \\ &= \theta(\varphi(\theta^{-1}(x))) + \theta(\varphi(\theta^{-1}(y))) \end{aligned}$$

$$\begin{aligned} \theta \circ \varphi \circ \theta^{-1}(x \cdot y) &= \theta \circ \varphi(\theta^{-1}(x \cdot y)) = \theta \circ \varphi(\theta^{-1}(x) \cdot \theta^{-1}(y)) \\ &= \theta(\varphi(\theta^{-1}(x)) \cdot \varphi(\theta^{-1}(y))) \\ &= \theta(\varphi(\theta^{-1}(x))) \cdot \theta(\varphi(\theta^{-1}(y))) \end{aligned}$$

(1.2). 双射：由 θ, φ 均为双射知，$\theta \circ \varphi \circ \theta^{-1}$ 也为双射

所以，$\theta \circ \varphi \circ \theta^{-1} \in \mathrm{Aut}(S)$，故 Θ 确实是合理的

Step 2. 验证 Θ 是群同构

(2.1). 群同态：$\forall \varphi, \psi \in \mathrm{Aut}(R)$，有

$$\begin{aligned} \Theta(\varphi \circ \psi) &= \theta \circ (\varphi \circ \psi) \circ \theta^{-1} \\ &= \theta \circ (\varphi \circ (\theta^{-1} \circ \theta) \circ \psi) \circ \theta^{-1} \\ &= (\theta \circ \varphi \circ \theta^{-1}) \circ (\theta \circ \psi \circ \theta^{-1}) \\ &= \Theta(\varphi) \circ \Theta(\psi) \end{aligned}$$

(2.2). 单射：若 $\Theta(\varphi) = \Theta(\psi)$，由 θ 可逆知

$$\theta \circ \varphi \circ \theta^{-1} = \theta \circ \psi \circ \theta^{-1} \iff \theta \circ \varphi = \theta \circ \psi \iff \varphi = \psi$$

(2.3). 满射：对 $\forall \phi \in \mathrm{Aut}(S)$，因为

$$\Theta(\theta^{-1} \circ \phi \circ \theta) = \theta \circ (\theta^{-1} \circ \phi \circ \theta) \circ \theta^{-1} = \phi$$

故我们找到了 ϕ 的原像 $\theta^{-1} \circ \phi \circ \theta$，所以 Θ 是满射

综上，Θ 为群同构 □

Exercise 8 设 R 是环，$I \lhd R$，定义商集 R/I 上的乘法运算：$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$，验证这样定义是合理的

Proof 假设 $\overline{a} = \overline{a_0}, \overline{b} = \overline{b_0}$，则 $a - a_0, b - b_0 \in I$，因为理想对“倍”封闭，$a_0, b \in R$，所以

$$ab - a_0 b_0 = (a - a_0)b + (b - b_0)a_0 \in I \Rightarrow \overline{a \cdot b} = \overline{a_0 \cdot b_0}$$

故乘法是良定的 $\square$

Exercise 9 设 R 是整环，求证：$\mathrm{Char}(R)=0$ 或素数 p

Proof 考虑特征映射

$$\begin{aligned}\varphi:\mathbb{Z}&\longrightarrow R\\ n&\longmapsto n1_R\end{aligned}$$

则 $\mathrm{Ker}\varphi=(n)$，由环同态基本定理，我们有同构

$$\mathbb{Z}/(n)\cong\mathrm{Im}\varphi$$

因为 $\mathrm{Im}\varphi$ 是 R 的子环，则 $\mathrm{Im}\varphi$ 也是整环（否则，$\exists a,b\in\mathrm{Im}\varphi\backslash\{0_R\}\subseteq R\backslash\{0_R\},\mathrm{s.t.}\ ab=0$，这与 R 是整环矛盾!)，由环同构知，$\mathbb{Z}/(n)=\mathbb{Z}/n\mathbb{Z}$ 为整环

(1). $n=0$ 时，$\mathbb{Z}/(0)=\mathbb{Z}$ 显然是整环

(2). $n\geq 2$ 时，若 n 为合数，则 $\exists 1<p\leq q<n,\mathrm{s.t.}\ n=pq$，则在 $\mathbb{Z}/n\mathbb{Z}$ 中，$\overline{p},\overline{q}\neq\overline{0}$，但 $\overline{0}=\overline{n}=\overline{p\cdot q}=\overline{p}\cdot\overline{q}$，这就说明 $\mathbb{Z}/n\mathbb{Z}$ 不是整环；若 n 为素数，则 $\forall\overline{a},\overline{b}\neq\overline{0}$，则 $p\nmid a,p\nmid b\Rightarrow p\nmid ab$，即 $\overline{ab}\neq\overline{0}$，故 $\mathbb{Z}/p\mathbb{Z}$ 为整环

因此 $\mathrm{Char}(R)=0$ 或素数 p $\square$

Exercise 10 设 $I\subseteq J,I\lhd R,J\lhd R$，定义如下映射

$$\begin{aligned}R/I&\longrightarrow R/J\\ (a+I)&\longmapsto(a+J)\end{aligned}$$

验证这是良定的

Proof 设 $(a+I)=(a'+I)$，则 $a-a'\in I\subseteq J$，故 $(a+J)=(a'+J)$ $\square$

Exercise 11 给定 $I\lhd R$，则存在双射

$$\begin{aligned}\theta:\{J\lhd R|I\subseteq J\subseteq R\}&\longrightarrow\{R/I\text{的理想}\}\\ J&\longmapsto J/I=\{\overline{a}=a+I|a\in J\}\end{aligned}$$

Proof 首先验证 θ 是合理的，即 $\theta(J)=J/I$ 确实是 R/I 的理想：

(a). $\forall j_1+I,j_2+I\in J/I$，由 J 为理想知，$j_1+j_2\in J$，故 $(j_1+I)+(j_2+I)=((j_1+j_2)+I)\in J/I$

(b). $\forall j+I\in J/I,r+I\in R/I$，由 J 是理想知，$jr\in J$，故 $(j+I)(r+I)=(jr+I)\in J/I$

因此 $\theta(J)=J/I$ 为 R/I 的理想，下证明 θ 是双射

单射：假设 $I\subseteq J_1,J_2\subseteq R$，若 $\theta(J_1)=\theta(J_2)$，即 $J_1/I=J_2/I$，则 $\forall j_1\in J_1,\exists j_2\in J_2,\mathrm{s.t.}\ j_1+I=j_2+I$，因此 $j_1-j_2\in I\subseteq J_2\Rightarrow j_1=(j_1-j_2)+j_2\in J_2$，故 $J_1\subseteq J_2$；同理我们有 $J_2\subseteq J_1$，因此 $J_1=J_2$

满射：对 $\forall S\lhd(R/I)$，设 $S_0=\{s\in R|\overline{s}=s+I\in S\}$，下证明 $S_0\lhd R$ 且 $I\subseteq S_0$

(1). 加法封闭性：$\forall s_1,s_2\in S_0$，则 $(s_1+I),(s_2+I)\in S$，因为 $S\lhd(R/I)$，则 $((s_1+s_2)+I)=(s_1+I)+(s_2+I)\in S\Rightarrow s_1+s_2\in S_0$

(2). 倍元封闭性：$\forall s\in S_0$，则 $(s+I)\in S$，对 $\forall r\in R,(r+I)\in R/I$，由 S 是理想知 $(s+I)(r+I)=(sr+I)\in S\Rightarrow sr\in S_0$

(3). $I\subseteq S_0$：$\forall a\in I$，我们有 $a+I=I=0_{(R/I)}\in S$，由 S_0 的定义知，$a\in S_0$，故 $I\subseteq S_0$

综上，我们有 $\theta(S_0)=S$，故满射得证，则 θ 确实是双射 $\square$

Exercise 12 分类 $\mathbb{Z}/n\mathbb{Z}$ 的理想（提示：利用上一题）

Solution 由上一题知，$\mathbb{Z}/n\mathbb{Z}$ 的理想一定形如 $S/n\mathbb{Z}$，其中 $S \lhd \mathbb{Z}, n\mathbb{Z} \subseteq S \subseteq \mathbb{Z}$，因为 $\mathbb{Z}$ 的理想都形如 $m\mathbb{Z}$，因此不妨设 $S = m\mathbb{Z}$，因为 $n\mathbb{Z} \subseteq m\mathbb{Z}$，所以 $\exists k \in \mathbb{Z}, \text{s.t. } mk = n$，故 $m \mid n$；反之，若 $m \mid n$，则 $\exists k \in \mathbb{Z}, \text{s.t. } mk = n$，则 $\forall nl \in n\mathbb{Z}, nl = mkl \in m\mathbb{Z}$，故 $n\mathbb{Z} \subseteq m\mathbb{Z}$，所以我们证明了 $n\mathbb{Z} \subseteq m\mathbb{Z} \iff m \mid n$

所以 $\mathbb{Z}/n\mathbb{Z}$ 的理想形如 $m\mathbb{Z}/n\mathbb{Z}$，其中 $m \mid n$，此外还有平凡理想（$m = 0$ 或 n） □

Exercise 13 设 R 是环，S 是 R 的子环，$I \lhd R$，求证：

1. $S + I = \{a + x | a \in S, x \in I\}$ 是 R 的子环

2. $S \cap I \lhd S$

3. 有环同构 $S/(S \cap I) \xrightarrow{\sim} (S + I)/I$

Proof

1. 由于子环 S 和理想 I 都对加、减、乘封闭，所以

(a) $1_R = 1_R + 0 \in S + I$

(b) 设 $a_1 + x_1, a_2 + x_2 \in S + I$，则 $(a_1 + x_1) + (a_2 + x_2) = (a_1 + a_2) + (x_1 + x_2) \in S + I$

(c) 设 $a_1 + x_1, a_2 + x_2 \in S + I$，则 $(a_1 + x_1) - (a_2 + x_2) = (a_1 - a_2) + (x_1 - x_2) \in S + I$

(d) 设 $a_1 + x_1, a_2 + x_2 \in S + I$，则

$$(a_1 + x_1)(a_2 + x_2) = a_1a_2 + (a_1x_2 + x_1a_2 + x_1x_2) \in S + I$$

故 $S + I$ 是 R 的子环

2. 验证加法与倍元的封闭性

(a) 加法封闭性：$\forall s_1, s_2 \in S \cap I$，则 $s_1, s_2 \in S \Rightarrow s_1 + s_2 \in S$；$s_1, s_2 \in I \Rightarrow s_1 + s_2 \in I$，故 $s_1 + s_2 \in S \cap I$

(b) 倍元封闭性：$\forall s \in S, a \in S \cap I$，则 $a \in S, a \in I \Rightarrow sa \in I, sa \in I \Rightarrow sa \in S \cap I$

故 $S \cap I \lhd S$

3. 考虑映射

$$\begin{aligned} \sigma : S &\longrightarrow (S + I)/I \\ s &\longmapsto s + I \end{aligned}$$

则 σ 是环同态（实际上是 $R \to R/I$ 的自然同态 π 在 S 上的限制），因为

(a) $\sigma(1_S) = 1_S + I$

(b) $\sigma(a + b) = ((a + b) + I) = (a + I) + (b + I) = \sigma(a) + \sigma(b)$

(c) $\sigma(ab) = (ab + I) = (a + I)(b + I) = \sigma(a)\sigma(b)$

且我们有

$$\begin{aligned} \text{Ker}\sigma &= \{s \in S | \sigma(s) = 0_{(S+I)/I}\} = \{s \in S | s + I = I\} \\ &= \{s \in S | s \in I\} = S \cap I \end{aligned}$$

对 σ 使用环同态基本定理，则我们有环同构 $S/(S \cap I) \xrightarrow{\sim} (S + I)/I$

□

Exercise 14 设 $I \lhd R$，则存在双射

$$\theta : \{S \overset{\text{子环}}{\subseteq} R | I \subseteq S\} \longrightarrow \{R/I\text{的子环}\}$$
$$S \longmapsto S/I$$

Proof 首先验证 θ 是合理的，即 $\theta(S) = S/I$ 确实是 R/I 的子环：

(a). $\forall s_1 + I, s_2 + I \in S/I$，由 S 为子环知，$s_1 \pm s_2 \in J$，故 $(s_1 + I) \pm (s_2 + I) = ((s_1 \pm s_2) + I) \in S/I$

(b). $\forall s_1 + I, s_2 + I \in S/I$，由 S 是子环知，$s_1 s_2 \in S$，故 $(s_1 + I)(s_2 + I) = (s_1 s_2 + I) \in S/I$

(c). $1_R \in S \Rightarrow 1_{R/I} = 1_R + I \in S/I$

因此 $\theta(S) = S/I$ 为 R/I 的子环，下证明 θ 是双射

单射：若 $\exists S_1, S_2$ 为 R 的子环，且 $I \subseteq S_1, S_2$，若 $\theta(S_1) = \theta(S_2)$，即 $S_1/I = S_2/I$ 则对 $\forall s_1 \in S_1, s_1 + I \in S_1/I = S_2/I$，故 $\exists s_2 \in S_2, \text{s.t. } s_1 + I = s_2 + I$，所以 $s_1 - s_2 \in I \subseteq S \Rightarrow s_1 = (s_1 - s_2) + s_2 \in S_2$，因此 $S_1 \subseteq S_2$，类似地我们有 $S_2 \subseteq S_1$，因此 $S_1 = S_2$

满射：若对 $\forall R/I$ 的子环 S，设 $S_0 = \{s \in R | \overline{s} = s + I \in S\}$，下证明 S_0 是 R 的子环，且 $I \subseteq S_0$

(1). 加法、减法封闭性：因为 S 是 R/I 的子环，所以 $\forall s_1, s_2 \in S_0$，有 $s_1 + I, s_2 + I \in S$，则 $(s_1 + I) \pm (s_2 + I) = (s_1 \pm s_2) + I \in S$，因此 $s_1 \pm s_2 \in S$

(2). 乘法封闭性：$\forall s_1, s_2 \in S_0$，有 $s_1 + I, s_2 + I \in S$，则 $(s_1 + I)(s_2 + I) = s_1 s_2 + I \in S$，因此 $s_1 s_2 \in S_0$

(3). 因为 S 为 R/I 的子环，所以 $1_S = 1_R + I \in S$，由 S_0 的定义知 $1_R \in S_0$

(4). $I \subseteq S_0$：$\forall a \in I, a + I = I = 0_{(R/I)} \in S$，由 S_0 的定义知，$a \in S_0$，故 $I \subseteq S_0$

综上，我们有 $\theta(S_0) = S$，故满射得证，则 θ 确实是双射 □

Exercise 15 验证 $\text{Frac}(R)$ 中加法的良定性

Proof 假设 $\frac{a}{x} = \frac{a'}{x'}, \frac{b}{y} = \frac{b'}{y'}$，则 $\begin{cases} ax' = a'x \cdots ① \\ by' = b'y \cdots ② \end{cases}$， $① \cdot (yy') + ② \cdot (xx')$ 得

$$ax'(yy') + by'(xx') = a'x(yy') + b'y(xx') \Rightarrow (ay)(x'y') + (bx)(x'y') = (a'y')(xy) + (b'x')(xy)$$

所以 $(ay + bx)(x'y') = (xy)(a'y' + b'x')$，即 $\frac{ax+by}{xy} = \frac{a'x'+b'y'}{x'y'}$，因此加法是良定的 □

Exercise 16 考虑典范单同态

$$\text{can}_R : R \longrightarrow \text{Frac}(R)$$
$$a \longmapsto \frac{a}{1_R}$$

求证：can_R 是同构 $\iff$ R 是域

Proof $(\Rightarrow)$：已知 can_R 是同构，故为满射，因为 $\frac{a}{x} \neq 0_{\text{Frac}(R)} \iff a \neq 0_R$ 则 $\forall a \in R \backslash \{0\}$，考虑 $\frac{1_R}{a}$，则 $\exists b \in R, \text{s.t. } \text{can}_R(b) = \frac{1_R}{a}$，故

$$\text{can}_R(ab) = \text{can}_R(a)\text{can}_R(b) = \frac{a}{1_R} \cdot \frac{1_R}{a} = 1_{\text{Frac}(R)}$$

由 can_R 为单射、$\text{can}_R(1_R) = 1_{\text{Frac}(R)}$ 知，$ab = 1_R$，即 $b = a^{-1}$，因此 R 的任意非零元均可逆，故 R 是域

$(\Leftarrow)$：已知 R 是域，因为 can_R 是已经是单同态，只需证明 can_R 为满同态：对 $\forall \frac{a}{x} \in \text{Frac}(R)$，因为 $\text{can}_R(a) = \frac{a}{1_R}, \text{can}_R(x) = \frac{x}{1_R}$，由 R 是域知，x 有逆元 x^{-1}，所以 $\text{can}_R(x^{-1}) = \frac{x^{-1}}{1_R}$，故

$$\text{can}_R(ax^{-1}) = \text{can}_R(a)\text{can}_R(x^{-1}) = \frac{ax^{-1}}{1_R}$$

因为 $ax^{-1} \cdot x = a \cdot 1_R$，所以 $\frac{ax^{-1}}{1_R} = \frac{a}{x}$，故 $\text{can}_R(ax^{-1}) = \frac{a}{x}$，这就说明 can_R 为满射，则 can_R 是同构 □

Exercise 17 求证：$\mathrm{Frac}(\mathbb{Z}[i]) \cong \mathbb{Q}(i)$

Proof 考虑典范单同态 $\mathrm{can}_{\mathbb{Z}[i]}$（简记为 can）以及嵌入映射 $\mathrm{inc}_{\mathbb{Z}[i],\mathbb{Q}(i)}$（简记为 inc）

$$\begin{aligned} \mathrm{can}: \mathbb{Z}[i] &\longrightarrow \mathrm{Frac}(\mathbb{Z}[i]) \\ a+bi &\longmapsto \frac{a+bi}{1} \end{aligned}$$

$$\begin{aligned} \mathrm{inc}: \mathbb{Z}[i] &\longrightarrow \mathbb{Q}(i) \\ a+bi &\longmapsto a+bi \end{aligned}$$

由 can 的泛性质得 $\widetilde{\mathrm{inc}} \circ \mathrm{can} = \mathrm{inc}$，即下面的图交换

$$\begin{tikzcd} \mathbb{Z}[i] \arrow[r, hook, "\mathrm{inc}"] \arrow[d, hook, "\mathrm{can}"'] & \mathbb{Q}(i) \\ \mathrm{Frac}(\mathbb{Z}[i]) \arrow[ur, dotted, hook, "\widetilde{\mathrm{inc}}"] & \end{tikzcd}$$

其中

$$\begin{aligned} \widetilde{\mathrm{inc}}: \mathrm{Frac}(\mathbb{Z}[i]) &\longrightarrow \mathbb{Q}(i) \\ \frac{a+bi}{c+di} &\longmapsto \mathrm{inc}(a+bi)\mathrm{inc}(c+di)^{-1} \end{aligned}$$

下面证明 $\widetilde{\mathrm{inc}}$ 是环同构：

①. 环同态：

(1). $\widetilde{\mathrm{inc}}(\frac{1}{1}) = \mathrm{inc}(1)\mathrm{inc}(1)^{-1} = 1$

(2). 对任意 $\frac{a_1+b_1i}{c_1+d_1i}, \frac{a_2+b_2i}{c_2+d_2i} \in \mathrm{Frac}(\mathbb{Z}[i])$，则

$$\begin{aligned} \widetilde{\mathrm{inc}}\left(\frac{(a_1+b_1i)(a_2+b_2i)}{(c_1+d_1i)(c_2+d_2i)}\right) &= \mathrm{inc}((a_1+b_1i)(a_2+b_2i))\mathrm{inc}((c_1+d_1i)(c_2+d_2i))^{-1} \\ &= \mathrm{inc}(a_1+b_1i)\mathrm{inc}(a_2+b_2i)\mathrm{inc}(c_1+d_1i)^{-1}\mathrm{inc}(c_2+d_2i)^{-1} \\ &= [\mathrm{inc}(a_1+b_1i)\mathrm{inc}(c_1+d_1i)^{-1}] \cdot [\mathrm{inc}(a_2+b_2i)\mathrm{inc}(c_2+d_2i)^{-1}] \\ &= \widetilde{\mathrm{inc}}\left(\frac{a_1+b_1i}{c_1+d_1i}\right)\widetilde{\mathrm{inc}}\left(\frac{a_2+b_2i}{c_2+d_2i}\right) \end{aligned}$$

关于上面第二行，我们补充证明 $\mathrm{inc}(ab)^{-1} = \mathrm{inc}(a)^{-1}\mathrm{inc}(b)^{-1}$，这是因为

$$\begin{cases} \mathrm{inc}(ab)^{-1}\mathrm{inc}(ab) = 1 \\ (\mathrm{inc}(a)^{-1}\mathrm{inc}(b)^{-1})\mathrm{inc}(ab) = \mathrm{inc}(a)^{-1}\mathrm{inc}(b)^{-1}\mathrm{inc}(a)\mathrm{inc}(b) = [\mathrm{inc}(a)^{-1}\mathrm{inc}(a)][\mathrm{inc}(b)\mathrm{inc}(b)^{-1}] = 1 \end{cases}$$

由 $\mathrm{inc}(ab)$ 的逆元唯一故得证；

(3). 对任意 $\frac{a_1+b_1i}{c_1+d_1i}, \frac{a_2+b_2i}{c_2+d_2i} \in \mathrm{Frac}(\mathbb{Z}[i])$，则

$$\begin{aligned} \widetilde{\mathrm{inc}}\left(\frac{a_1+b_1i}{c_1+d_1i} + \frac{a_2+b_2i}{c_2+d_2i}\right) &= \widetilde{\mathrm{inc}}\left(\frac{(a_1+b_1i)(c_2+d_2i)+(a_2+b_2i)(c_1+d_1i)}{(c_1+d_1i)(c_2+d_2i)}\right) \\ &= \mathrm{inc}[(a_1+b_1i)(c_2+d_2i)+(a_2+b_2i)(c_1+d_1i)]\mathrm{inc}[(c_1+d_1i)(c_2+d_2i)]^{-1} \\ &= [\mathrm{inc}(a_1+b_1i)\mathrm{inc}(c_2+c_2i)+\mathrm{inc}(a_2+b_2i)\mathrm{inc}(c_1+d_1i)]\left[\mathrm{inc}(c_1+d_1i)^{-1}\mathrm{inc}(c_2+d_2i)^{-1}\right] \\ &= [\mathrm{inc}(a_1+b_1i)\mathrm{inc}(c_1+d_1)^{-1}] + [\mathrm{inc}(a_2+b_2i)\mathrm{inc}(c_2+d_2)^{-1}] \\ &= \widetilde{\mathrm{inc}}\left(\frac{a_1+b_1i}{c_1+d_1i}\right) + \widetilde{\mathrm{inc}}\left(\frac{a_2+b_2i}{c_2+d_2i}\right) \end{aligned}$$

②. 单射：若 $\widetilde{\mathrm{inc}}\left(\frac{a_1+b_1 i}{c_1+d_1 i}\right)=\widetilde{\mathrm{inc}}\left(\frac{a_2+b_2 i}{c_2+d_2 i}\right)$，则 $\mathrm{inc}(a_1+b_1 i)\mathrm{inc}(c_1+d_1)^{-1}=\mathrm{inc}(a_2+b_2 i)\mathrm{inc}(c_2+d_2)^{-1}$，因此

$$\mathrm{inc}[(a_1+b_1 i)(c_2+d_2 i)]=\mathrm{inc}[(a_2+b_2 i)(c_1+d_1 i)]\Rightarrow (a_1+b_1 i)(c_2+d_2 i)=(a_2+b_2 i)(c_1+d_1 i)$$

（因为 inc 为单射），所以 $\frac{a_1+b_1 i}{c_1+d_1 i}=\frac{a_2+b_2 i}{c_2+d_2 i}$

③. 满射：对任意 $\frac{a+bi}{c+di}\in\mathbb{Q}(i)$，可通过通分使得 $a,b,c,d\in\mathbb{Z}$，故不妨设 a,b,c,d 为整数，且 $c^2+d^2\neq 0$，则显然有 $\frac{a+bi}{c+di}=\mathrm{inc}(a+bi)\mathrm{inc}(c+di)^{-1}=\widetilde{\mathrm{inc}}\left(\frac{a+bi}{c+di}\right)$，这就找到了原像

综上，$\widetilde{\mathrm{inc}}$ 为环同构，故 $\mathrm{Frac}(\mathbb{Z}[i])\cong\mathbb{Q}(i)$ □