1，已知集合 R=$\left\{\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \middle| x,y,z \in Z\right\}$

按照通常矩阵的加法运算和乘法运算构成一个环，

试证明映射φ: R→Z，$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$→z 是环的满同态，并求同态核，

证明(1)对属于 Z 的任意 z，有原像$\begin{pmatrix} 0 & 0 \\ 0 & z \end{pmatrix}$，即$\varphi$是满射，

对属于 R 的任意 A=$\begin{pmatrix} x_1 & y_1 \\ 0 & z_1 \end{pmatrix}$，B=$\begin{pmatrix} x_2 & y_2 \\ 0 & z_2 \end{pmatrix}$，有下列等式成立

$$\varphi\left(\begin{pmatrix} x_1 & y_1 \\ 0 & z_1 \end{pmatrix} + \begin{pmatrix} x_2 & y_2 \\ 0 & z_2 \end{pmatrix}\right) = \varphi\begin{pmatrix} x_1 + x_2 & y_1 + y_2 \\ 0 & z_1 + z_2 \end{pmatrix} = z_1 + z_2$$

$$= \varphi\begin{pmatrix} x_1 & y_1 \\ 0 & z_1 \end{pmatrix} + \varphi\begin{pmatrix} x_2 & y_2 \\ 0 & z_2 \end{pmatrix}$$

$$\varphi\left(\begin{pmatrix} x_1 & y_1 \\ 0 & z_1 \end{pmatrix}\begin{pmatrix} x_2 & y_2 \\ 0 & z_2 \end{pmatrix}\right) = \varphi\begin{pmatrix} x_1x_2 & x_1y_2 + y_1z_2 \\ 0 & z_1z_2 \end{pmatrix} = z_1z_2$$

$$= \varphi\begin{pmatrix} x_1 & y_1 \\ 0 & z_1 \end{pmatrix}\varphi\begin{pmatrix} x_2 & y_2 \\ 0 & z_2 \end{pmatrix}$$

即φ是满同态，

(2)$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in \mathrm{Ker}\,\varphi \Leftrightarrow \varphi\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = 0 \Leftrightarrow z = 0$，从而 $\ker\varphi$=$\left\{\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \middle| x,y, \in Z\right\}$

2，设 $R=Q[\sqrt{2}]=\{a+b\sqrt{2}|a,b$ 属于 $Q\}$，

试证明$\varphi: Q[x]\rightarrow R, f(x)\rightarrow f(\sqrt{2})$

是有理数域 Q 上的一元多项式环 Q[x]到环 R 的满同态 ，且 $\mathrm{Ker}\,\varphi=\langle x^2-2\rangle$

证明: 对属于 Q[x]的 f(x)，g(x)，有

$\varphi(f(x)+g(x))=f(\sqrt{2})+g(\sqrt{2})=\varphi(f(x))+\varphi(g(x))$，

$\varphi(f(x)g(x))=f(\sqrt{2})g(\sqrt{2})=\varphi(f(x))\varphi(g(x))$，

且对属于 R 的 $a+b\sqrt{2}$ ，存在属于 R 的 $f(x)=a+bx$，使得$\varphi(f(x))=f(\sqrt{2})$，

故φ是满同态

若任意 f(x)属于 Ker φ，则$\varphi(f(x))=f(\sqrt{2})=0$，即$\sqrt{2}$是 f(x)的一个根 ，

又因 f(x)属于 Q[x]，从而 x^2-2 为 f(x)的一个因式 ，

即 $f(x)=(x^2-2)g(x)$属于$\langle x^2-2\rangle$，从而有 ker φ包含于$\langle x^2-2\rangle$，

若 h(x)属于$\langle x^2-2\rangle$，则可设 $h(x)=(x^2-2)m(x)$，从而$\varphi(h(x))=0$，

即$\langle x^2-2\rangle$包含于 Ker φ，故 $\mathrm{Ker}\,\varphi=\langle x^2-2\rangle$，

3，设φ是环 R 到环 R'的环同态 ，若 R 中元素 a 的加法运算的阶为 t，

试证明φ(a)的加法运算的阶是 t 的因数 ，

证明: 因为 $t\varphi(a)=\varphi(ta)=\varphi(0)=0$ 属于 R'，

故φ(a)的加法运算的阶是 t 的因数 ，

4，问环 2Z 与 3Z 是否同构?

解: 环 2Z 与 3Z 不同构 ，

反证 ，若φ为 2Z 到 3Z 的同构映射 ，则

$\varphi(2m_1\times 2m_2)=\varphi(2\times 2m_1m_2)=2m_1m_2\varphi(2)$，

$\varphi(2m_1)\times\varphi(2m_2)=m_1\varphi(2)\times m_2\varphi(2)=m_1m_2[\varphi(2)]^2$，

因此 ，$\varphi(2)=2$ 不属于 3Z，故 2Z 和 3Z 不同构 ，

5，设φ是环 R 到环 R'的环同态，证明

(1)若 S 是 R 的子环，则$\varphi(S)$是 R'的子环;

(2)若 S'是 R'的子环，则$\varphi^{-1}(S')$是 R 的子环;

(3)若 I'是 R'的理想，则$\varphi^{-1}(I')$是 R 的理想，

证明: (1)$\varphi(S)$为 R'的非空子集合，若 a，b 属于 S，则 a−b 属于 S，ab 属于 S，

因此$\varphi(a)-\varphi(b)=\varphi(a-b)$属于$\varphi(S)$，$\varphi(a)\varphi(b)=\varphi(ab)$属于$\varphi(S)$，

故$\varphi(S)$为 R'的子环，

(2)0 属于不为空集的$\varphi^{-1}(S')$，

若 s_1，s_2 属于$\varphi^{-1}(S')$，则$\varphi(s_1)$属于 S'，$\varphi(s_2)$属于 S'

从而$\varphi(s_1-s_2)=\varphi(s_1)-\varphi(s_2)$属于 S'，$\varphi(s_1s_2)=\varphi(s_1)\varphi(s_1)$属于 S'，

即 s_1-s_2，s_1s_2 属于$\varphi^{-1}(S')$，故$\varphi^{-1}(S')$是 R 的子环，

(3)由(2)知$\varphi^{-1}(I')$是 R 的子环，

若任意 a 属于$\varphi^{-1}(I')$，任意 r 属于 R，则

$\varphi(a)$属于 I'，$\varphi(ra)=\varphi(r)\varphi(a)$属于 I'，$\varphi(ar)=\varphi(a)\varphi(r)$属于 I'，

即 ra，ar 属于$\varphi^{-1}(I')$，故$\varphi^{-1}(I')$是 R 的理想，

6，设φ是环 R 到环 R'的满同态，试证明

(1)若 R 是交换环，则 R'也是交换环;

(2)若 I 是 R 的理想，则$\varphi(I)$是 R'的理想，

证明(1)由于φ是 R 到 R'的满射，

从而若 a'，b'属于 R'，则存在属于 R 的 a，b，使得$\varphi(a)=a'$，$\varphi(b)=b'$，

从而 $a'b'=\varphi(a)\varphi(b)=\varphi(ab)=\varphi(ba)=b'a'$，即 R'是交换环，

(2)显然$\varphi(I)$是非空集合，

若$\varphi(a)$，$\varphi(b)$属于$\varphi(I)$，r'属于 R'，则存在属于 R 的 r，使得$\varphi(r)=r'$，

从而$\varphi(a)-\varphi(b)=\varphi(a-b)$属于$\varphi(I)$，

$r'\varphi(a)=\varphi(r)\varphi(a)=\varphi(ra)$属于$\varphi(I)$，

$\varphi(a)r'=\varphi(a)\varphi(r)=\varphi(ar)$属于$\varphi(I)$，

所以，$\varphi(I)$为 R'的理想，

7，用环同态基本定理证明 $R[x]/\langle x^2+1\rangle\cong C$，

证明： 定义映射φ: $R[x]\to C$，$f(x)\to f(i)$，

若 $a+bi$ 属于 C，a，b 属于 R，则$\varphi(a+bx)=a+bi$，即φ是满射，

且$\varphi(f(x)+g(x))=f(i)+g(i)=\varphi(f(x))+\varphi(g(x))$，

$\varphi(f(x)g(x))=f(i)g(i)=\varphi(f(x))\varphi(g(x))$，

从而φ是满同态，

$\mathrm{Ker}\,\varphi=\{f(x)\in R[x]|f(i)=0\}$，易知 $\mathrm{Ker}\,\varphi=\langle x^2+1\rangle$，

故由环同态基本定理知 $R[x]/\langle x^2+1\rangle\cong C$，

8，设 I 和 J 是环 R 的理想，且 $I+J=R$，$I\cap J=\{0\}$，证明 $R/I\cong J$，

证明： 因 $I+J=R$，从而对属于 R 的任意 r，有 $r=r_1+r_2$，其中 r_1 属于 I，r_2 属于 J

下面说明 r 的分解是唯一的，

若 $r_1+r_2=r_1'+r_2'$，r_1，r_1'属于 I，r_2，r_2'属于 J，则 $r_1-r_1'=r_2-r_2'$属于 $I\cap J=\{0\}$，

从而 $r_1=r_1'$，$r_2=r_2'$

作映射φ: $R\to J$，$r_1+r_2\to r_2$，则易知φ是满射，

又因$\varphi(r_1+r_2+r_1'+r_2')=r_2+r_2'=\varphi(r_1+r_2)+\varphi(r_1'+r_2')$，

$\varphi((r_1+r_2)(r_1'+r_2'))=\varphi(r_1r_1'+r_2r_1'+r_1r_2'+r_2r_2')=r_2r_2'=\varphi(r_1+r_2)\varphi(r_1'+r_2')$，

故φ是满同态，

$\mathrm{Ker}\,\varphi=\{r\in R|\varphi(r)=\varphi(r_1+r_2)=r_2=0\}=I$，故 $R/I\cong J$，

9，试证明复数域 C 可以视为四元数体 H 的子域，

证明： $H=\{ae+bi+cj+dk|a,b,c,d\in R\}$，

定义映射φ: $C\to H=\{ae+bi+cj+dk|a,b,c,d\in R\}$，$a+bi\to ae+bi$，

则φ是单同态，故在同构意义下，C 可以视为 H 的子域，

10，试证明在同构意义下，$M_3(R)$可视为$M_2(R)$的扩环，

证明: 定义映射φ: $M_2(R)\to M_3(R)$ $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix}$

易知φ是单同态，因此$M_3(R)$可以看成$M_2(R)$的扩环，

11，(1)求剩余类环Z_6到Z_{15}的所有环同态;

(2)求剩余类环Z_{10}到Z_{10}的所有环同态，

解: φ是Z_6到Z_{15}的环同态的充要条件是$6\varphi(\overline{1})=0$，$\varphi(\overline{1})=(\varphi(\overline{1}))^2$，

设$\varphi(\overline{1})=\overline{a}$，在$Z_{15}$中满足这两个条件的元素有$\overline{0}$，$\overline{10}$，

故Z_6到Z_{15}的所有环同态为$\varphi_1(\overline{1})=\overline{0}$，$\varphi_2(\overline{1})=\overline{10}$，

同理φ是Z_{10}到Z_{10}的环同态的充要条件是$10\varphi(\overline{1})=\overline{0}$，$\varphi(\overline{1})=(\varphi(\overline{1}))^2$，

设$\varphi(\overline{1})=\overline{a}$，在$Z_{10}$中满足这两个条件的元素有$\overline{0}$，$\overline{1}$，$\overline{5}$，$\overline{6}$，

故Z_6到Z_{15}的所有环同态为$\varphi_1(\overline{1})=\overline{0}$，$\varphi_2(\overline{1})=\overline{1}$，$\varphi_3(\overline{1})=\overline{5}$，$\varphi_4(\overline{1})=\overline{6}$，

习题 1 确定$\{Z;+,\bullet\}$的所有自同态映射和自同构映射，

证明: 若φ是$\{Z;+,\bullet\}$的自同态映射，则$\varphi(m)=m\varphi(1)$，$\varphi(1)=\varphi(1)\varphi(1)$，

此时，

$\varphi(m+n)=(m+n)\varphi(1)=m\varphi(1)+n\varphi(1)=\varphi(m)+\varphi(n)$，

$\varphi(mn)=(mn)\varphi(1)=mn\varphi(1)\varphi(1)=\varphi(m)\varphi(n)$，

即φ由$\varphi(1)$决定，而$\varphi(1)=0$或者 1，

故$\{Z;+,\bullet\}$的自同态映射有两个，一个是零映射，一个是恒等映射，

显然，$\{Z;+,\bullet\}$的自同构映射只有一个，为恒等映射，

习题 2 设 R 是有单位元的环，若用 Aut(R)表示环 R 的所有自同构映射的集合，则 Aut(R)对于映射的乘法运算构成群，称为环 R 的自同构群，

求证 $Aut(Z)=\{id\}$，$Aut(Z_n)=\{id\}$，

证明: 由上题知 $Aut(Z)=\{id\}$，

若φ是 Z_n 的自同构映射，则对于 Z_n 的任意一个元素$\overline{b}$，存在$\overline{a}$使得$\varphi(\overline{a})=\overline{b}$，

从而 $a\varphi(\overline{1})=\varphi(\overline{a})=\overline{b}$，即$\varphi(\overline{1})$是 Z_n 加法群的生成元，

若令$\varphi(\overline{1})=\overline{m}$，则 $m=1,2,\cdots,n$ 且$(m,n)=1$，再由$\overline{m}^2=\overline{m}$知 $n|m(m-1)$，

显然 $n|(m-l)$，从而 $m=1$，即$\varphi(\overline{1})=\overline{1}$，$Aut(Z_n)=\{id\}$，

习题 3 设φ: $R\to R'$是环同态映射，I，I'分别是 R，R'的理想，且$\varphi(I)$包含于 I'，

求证φ可以诱导 R/I 到 R'/I'的同态映射，

证明: 定义$\overline{\varphi}$: $R/I\to R'/I'$，$a+I\to\varphi(a)+I'$，

若 $a+I=b+I$，则 $a-b$ 属于 I，从而$\varphi(a)-\varphi(b)=\varphi(a-b)$属于 I'，

即$\varphi(a)+I'=\varphi(b)+I'$，$\overline{\varphi}(a+I)=\overline{\varphi}(b+I)$，所以$\overline{\varphi}$是 R/I 到 R'/I'的映射，

又由于

$\overline{\varphi}((a+I)+(b+I))=\overline{\varphi}(a+b+I)=\varphi(a+b)+I'=\varphi(a)+I'+\varphi(b)+I'=\overline{\varphi}(a+I)+\overline{\varphi}(b+I)$，

$\overline{\varphi}((a+I)(b+I))=\overline{\varphi}(ab+I)=\varphi(ab)+I'=\varphi(a)\varphi(b)+I'=(\varphi(a)+I')(\varphi(b)+I')$

$=\overline{\varphi}(a+I)\overline{\varphi}(b+I)$，

因此$\overline{\varphi}$是 R/I 到 R'/I 的同态映射

习题 4 证明环 $Z/\langle 3\rangle$与环 $Z/\langle 12\rangle$的子环$\langle 4\rangle/\langle 12\rangle$同构，

证明: 由环的第二同构定理知$(\langle 3\rangle+\langle 4\rangle)/\langle 3\rangle\cong\langle 4\rangle/(\langle 4\rangle\cap\langle 3\rangle)$，

而$\langle 3\rangle+\langle 4\rangle=Z$，$\langle 4\rangle\cap\langle 3\rangle=\langle 12\rangle$，故 $Z/\langle 3\rangle\cong\langle 4\rangle/\langle 12\rangle$，

习题 5 试证明任何不含单位元的环可以嵌入到有单位元的环中，

证明: 设环 R 无单位元，定义 $R\times Z$ 上的加法和乘法运算如下:

$(r_1, m)+(r_2, n)=(r_1+r_2, m+n)$,

$(r_1, m)(r_2, n)=(r_1r_2+mr_2+nr_1, mn)$,

其中 r_1, r_2 属于 R, m, n 属于 Z,

则 $R\times Z$ 对于这样的加法和乘法运算是有单位元(0, 1)的环

定义映射 φ: $R\to R\times Z$, $r\to(r, 0)$,

则 φ 是环 R 到 $R\times Z$ 的单同态映射，即 $R\cong\varphi(R)$ 包含于 $R\times Z$,

习题 6 试证明整数加法群的自同态环与整数环同构，

证明: 令整数加法群的所有自同态构成集合为 End(Z),

若 φ, τ 是整数加法群的两个自同态，

定义 $(\varphi+\tau)(n)=\varphi(n)+\tau(n)$, $(\varphi\tau)(n)=\varphi(\tau(n))$,

则 End(Z)是有单位元的环，称为整数加法群的自同态环，

若 φ 属于 End(Z)，则 $\varphi(n)=n\varphi(1)$，此时

$\varphi(m+n)=(m+n)\varphi(1)=m\varphi(1)+n\varphi(1)=\varphi(m)+\varphi(n)$，即 φ 完全由 $\varphi(1)$ 决定，

定义映射 ψ: $End(Z)\to Z$, $\varphi\to\varphi(1)$，由上述讨论知 ψ 是双射，

且 $\psi(\varphi+\tau)=\varphi(1)+\tau(1)=\psi(\varphi)+\psi(\tau)$,

再由 $\varphi(n)=n\varphi(1)$ 知 $\varphi(\tau(1))=\tau(1)\varphi(1)$,

从而 $\psi(\varphi\tau)=(\varphi\tau)(1)=\varphi(\tau(1))=\varphi(1)\tau(1)=\psi(\varphi)\psi(\tau)$,

所以 ψ 是 End(Z)到 Z 的同构映射，

习题 7 试证明有理数域 Q 的自同构映射是恒等映射 id,

证明: 设 φ 是 Q 的自同构映射，则对属于 Z 的 m, n, $m\neq0$,

有 $\varphi(n)=n$, $\varphi(m^{-1})=\varphi(m)^{-1}=m^{-1}$，进而 $\varphi\left(\frac{n}{m}\right)=\frac{n}{m}$，故 $\varphi=id$,

习题 8 试证明实数域 R 的自同构映射是恒等映射 id，

证明: 若φ是 R 的自同构映射，则对属于 Z 的 m，n，$m\neq 0$，

有$\varphi(n)=n$，$\varphi(m^{-1})=\varphi(m)^{-1}=m^{-1}$，进而$\varphi(n/m)=n/m$，

因而对属于 Q 的任意 a 有$\varphi(a)=a$，

若α属于 R，且$\alpha>0$，则$\alpha=\sqrt{\alpha}\sqrt{\alpha}$，因此$\varphi(\alpha)=\varphi(\sqrt{\alpha})\varphi(\sqrt{\alpha})>0$，

若$\alpha_1<\alpha_2<\alpha_3$，由$\varphi(\alpha_2-\alpha_1)=\varphi(\alpha_2)-\varphi(\alpha_1)>0$，$\varphi(\alpha_3-\alpha_2)=\varphi(\alpha_3)-\varphi(\alpha_2)>0$

得$\varphi(\alpha_1)<\varphi(\alpha_2)<\varphi(\alpha_3)$，

于是对属于 Q 的任何 a，b，满足条件 $a\leqslant\alpha\leqslant b$，有$\varphi(a)=a\leqslant\varphi(\alpha)\leqslant\varphi(b)=b$，

故α，$\varphi(\alpha)$同在闭区间$[a,b]$，因而$\varphi(\alpha)=\alpha$，即$\varphi=id$，

习题 9 设 R 是一个环，φ是 R 到 R 的双射，

若对属于 R 的任意 a，b，有$\varphi(a+b)=\varphi(a)+\varphi(b)$，$\varphi(ab)=\varphi(b)\varphi(a)$，

则称φ是 R 的反自同构映射，

令 G(R)表示 R 的自同构与反自同构映射的集合，

试证明 G(R)按照变换的合成运算是一个群，

证明: 设φ_1，φ_2是反自同构映射，σ为自同构映射，

由$(\varphi_1\varphi_2)(a+b)=\varphi_1\varphi_2(a)+\varphi_1\varphi_2(b)$，

$(\varphi_1\varphi_2)(ab)=\varphi_1(\varphi_2(b)\varphi_2(a))=(\varphi_1\varphi_2)(a)(\varphi_1\varphi_2)(b)$，

$(\varphi_1\sigma)(a+b)=\varphi_1\sigma(a)+\varphi_1\sigma(b)$，

$(\varphi_1\sigma)(ab)=\varphi_1(\sigma(a)\sigma(b))=(\varphi_1\sigma)(b)(\varphi_1\sigma)(a)$，

$(\sigma\varphi_1)(a+b)=\sigma\varphi_1(a)+\sigma\varphi_1(b)$，

$(\sigma\varphi_1)(ab)=\sigma(\varphi_1(b)\varphi_1(a))=(\sigma\varphi_1)(b)(\sigma\varphi_1)(a)$，

知$\varphi_1\varphi_2$为自同构映射，$\varphi_1\sigma$与$\sigma\varphi_1$为反自同构映射，即 G(R)的运算封闭，

设φ是 R 的反自同构映射，a，b 属于 R，

由$\varphi^{-1}(a+b)=\varphi^{-1}(a)+\varphi^{-1}(b)$，

$\varphi^{-1}(ab)=\varphi^{-1}(\varphi\varphi^{-1}(a)\varphi\varphi^{-1}(b))=\varphi^{-1}(\varphi(\varphi^{-1}(b)\varphi^{-1}(a)))=\varphi^{-1}(b)\varphi^{-1}(a)$，

知φ^{-1}为反自同构映射，

若φ是 R 的自同构映射，则φ^{-1}为自同构映射，由子群的判别定理知 G(R)是群

习题 10 设 R 是一个环，

G(R)表示 R 的自同构与反自同构集合关于映射的合成运算构成的群，

Aut(R)为 R 的自同构群，

试证明 Aut(R)是 G(R)的正规子群，且|C(R): Aut(R)|等于 1 或 2，

证明: 设φ属于 G(R)，σ属于 Aut(R)，

由上题知$\varphi\sigma\varphi^{-1}$是自同构，所以 Aut(R)是 G(R)的正规子群，

若 Aut(R)=G(R)，则|G(R): Aut(R)|=1，若 Aut(R)≠G(R)，则反自同构映射存在

设φ_1，φ_2是反自同构映射，由$\varphi_1^{-1}\varphi_2$属于 Aut(R)知φ_1Aut(R)=φ_2Aut(R)，

于是|G(R): Aut(R)|=2，