第 8 章 环与域

前面我们讨论了群的基本性质．现在我们将讨论具有两种运算的代数系环与域．环与域的概念对我们来讲并不陌生．在高等代数里我们已经介绍过环与域的实例整数环、实数域、复数域等．可见环与域这两个概念的重要性．在这一章里，我们将讨论一般的抽象环与域的基本概念及其最基本的性质，并且分析几种重要的环与域．

环为带两种运算的代数体系，比群复杂，但在环论中有关问题的研究及处理问题的方法与群论中有许多相似之处．

§1　环的定义

我们熟悉的群论里的多数群的代数运算习惯上称为乘法．实际上运算的称呼并不重要，重要的是群或者其它代数体系关于这种运算的结构与性质．但是在环中有两种不同结构的运算，为了区分这两种运算，需要给出这两种运算的不同称呼．另外，环的其中一个运算与我们习惯的数的加法运算结构相似．因此我们称这个运算为加法运算．而另外一个运算我们称之为乘法运算．

定义 1　一个交换群叫做一个**加群**，我们把这个群上的代数运算叫做加法，并且用符号 + 来表示．

有了加法的定义，相应的许多与符号相关的表示及计算规则的形式也要相应改变．

（1）　由于加群的加法适合结合律，n 个元 $a_1, a_2, \cdots, a_n$ 的和有意义，这个和我们用下面符号来表示

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n .$$

当 n 是正整数时，na 表示 n 个 a 的和．

（2）　加群的单位元称为零元，记为 0．显然对任意的 a 都有

$$0 + a = a + 0 = a .$$

值得强调的是这里的 0 表示加群中的单位元，和整数中的 0 是不同的．

（3）　元 a 的唯一的逆元用 $-a$ 表示，叫做 a 的**负元**．显然 $-(-a) = a$．将 $a + (-b)$ 简写成 $a - b$，习惯上称为 a 减 b．

有了负元的定义及“减”的定义，当 n 为任意整数时，na 有了定义．特别地，当 n 为负数时，na 表示 $|n|$ 个 $-a$ 的和．下列的规定是合理的．

定义整数与加群中的元的乘法

$$n\cdot a=na\ ,\ \ (-n)a=-(na)\ ,$$

当$n=0$时，$0a=0$.

注：左边的 0 为整数中的 0，而右边的零为加群中的零元.

在新的符号下，加群的一个非空子集S作成一个子群的充分必要条件是

$$a,b\in S\Rightarrow a+b\in S,\quad a\in S\Rightarrow -a\in S.$$

或是

$$a,b\in S\Rightarrow a-b\in S\ .$$

有了加群及上述符号的定义，我们给出环的定义.

定义 2 R是一个非空集合，其上有两个运算：加法$(+)$和乘法$(*)$，如果这些运算满足

1. $(R,+)$是一个加群，即$(R,+)$对于叫加法的代数运算作成一个交换群.

2. $(R,*)$对于另一个叫做乘法的代数运算构成半群，即对于运算$(*)$具有封闭性与满足

结合律，对于任意的$a,b,c\in R$有

$$ab\in R,\qquad a(bc)=(ab)c\ ,$$

3 乘法的左右分配律成立，即对于任意的$a,b,c\in R$有

$$a(b+c)=ab+ac,\quad (b+c)a=ba+ca\ ,.$$

称$(R,+,*)$是一个环．并把这个环记为R.

在环的定义中，我们将乘法运算符省略，即将$a*b$简记为ab.

在介绍环的其他代数性质之前，我们先熟悉一下环的关于两种运算的一些运算律，这些算规则表现在整数环中都是大家所熟悉．证明留给读者自己补出.

1. 加法消去律成立：

$$a+b=a+c\Rightarrow b=c\ .$$

特别地，

$$x+a=a\Rightarrow x=0\ ,\ \ x+a=0\Rightarrow x=-a\ .$$

2. 对任意的$n\in Z$有，$n(a+b)=na+nb$.

3. 对任意的$m,n\in Z$有，$ma+na=(m+n)a$.

4. 对任意的$m,n\in Z$有，$m\cdot na=mn\cdot a$.

5. 对任意的 $a \in R$ 有，$0a = a0 = 0$，其中 0 均为 R 中零元.

6. 对任意的 $a, b \in R$ 有，$(-a)b = -ab = a(-b)$.

7. 对任意的 $a, b \in R$ 有，$(-a)(-b) = ab$.

8. 对任意的 $a, b, c \in R$ 有，$a(b-c) = ab - ac, (b-c)a = ba - ca$.

9．对任意的 $n \in Z$ 有，$(na)b = a(nb) = n(ab)$.

最后，我们定义 a 的 n 次方的定义．环 R 中，a^n 表示

$$a^n = \overbrace{aa\cdots a}^{n个}$$

显然

$$a^n \cdot a^m = a^{m+n}, \qquad (a^n)^m = a^{mn}.$$

下面我们通过几个例子熟悉一下环的定义：

例 1 全体整数所成集合 Z 对于数的加法，乘法作成一个环．元素为整数的一切 n 阶方阵所成集合 $(Z)_n$ 关于方阵的加法和乘法作成一个环．同样，$(Q)_n, (R)_n, (C)_n$ 关于方阵的加法与乘法都作成环．一般的设 A 是任一数环，$(A)_n$ 也作成一个环，叫做 A 上的 n 阶方阵环.

例 2 模 n 的剩余类对于模 n 的加法和模 n 的乘法成为一个环.

解 $Z_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$；

（1） 前面已经证明对于模 n 加法 Z_n 构成一个交换群.

（2） Z_n 对模 n 乘法是闭的.

（3） 结合律，分配律显然成立.

例 3 设 $(G, +)$ 是一个加法群，$E = Hom(G, G)$ 表示 G 到 G 的一切自同态组成的集合. 容易证明 $(E, \circ)$ 是一个乘法半群，$\circ$ 为映射的合成.

对任意 $f, g \in E$，规定

$$(f+g)(x) = f(x) + f(x), \quad \forall x \in G,$$

下面证明这样规定的加法是 E 的一个二元运算，即证 $f + g \in E$.

首先 $f+g$ 是 E 到 E 的一个映射，且任取 $x_1, x_2 \in G$,

$$(f+g)(x_1+x_2) = f(x_1+x_2)+g(x_1+x_2)$$

$$=(f(x_1)+f(x_2))+(g(x_1)+g(x_2))$$

$$=(f+g)(x_1)+(f+g)(x_2)$$

故 $f+g$ 是 G 到 G 的一个同态映射，从而 $f+g \in E$.

可证 $(E,+)$ 是一个加法群，且乘法“$\circ$”对加法的左右分配律都成立，从而 $(E,+,\circ)$ 作成一个环，这个环叫做加群 G 的自同态（对应）环.

§2 整环、域、除环

就像群论一样，给定群的概念，讨论满足各种附加条件的群是极其重要的，如交换群，循环群等. 同样，对于环我们也要讨论各种满足其它附加性质的各类环的定义. 一般来讲，环的种类有很多，我们主要侧重于满足一些常见重要性质的环. 这些重要的特性主要针对环的乘法而言如交换律、消去律、存在逆元、存在单位元等，对应于各种不同的性质，可以定义各种特殊环的定义如整环、除环、域等.

在介绍这些特殊的环：整环、除环、域之前，首先给出与乘法运算有关的一些概念（即运算规律）.

我们考虑的第一个运算规律即乘法的交换律. 在环定义里我们没有要求环的乘法适合交换律，所以在一个环里 ab 未必等于 ba . 但一个环的乘法可能是适合交换律的，如所有的数环（整数环、有理数环、实数环、负数环）.

定义 1 一个环 R 叫做一个交换环，若对任意的 $a,b \in R$ 都有

$$ab = ba .$$

易证，在一个交换环里，对于任何正整数 n 以及环的任意两个元 a,b 来说，都有

$$a^n \cdot b^n = (ab)^n .$$

定义 2 一个环 R 的一个元 e 叫做一个单位元，若对任意的 $a \in R$ 都有

$$ea = ae = a .$$

一般地，一个环未必有单位元. 事实上，一个环也可以仅含有左单位元或仅含有右单位元，但两者都存在时一定相等. 这儿我们仅讨论那些含有单位元的环. 在存在单位元的环中，单位元在环中往往占有很重要的地位.

同半群一样，如果 R 是含有单位元的环，则单位元唯一．习惯上，常用 1 来表示这个唯一的单位元．当然环中的 1 不是普通的整数 1．

在含有单位元的环中可以规定一个非零元的零次方，即任意 $a \in R$ 且 $a \neq 0$

$$a^0 = 1 .$$

例 1　若 R 只包括一个 a，加法和乘法是

$$a + a = a, \quad aa = a .$$

R 显然是一个环．这个环 R 的唯一的元 a 有一个逆元，就是 a 本身（因为 a 本身就是 R 中的单位元）．因此在 R 中，零元等于单位元．

如同半群一样，如果环含有单位元，我们可以相应的定义逆元的概念．

定义 3　一个有单位元环的一个元 b 叫做元 a 的一个逆元，假如

$$ab = ba = e .$$

记 a 的逆元为 a^{-1}．

一般我们考虑的环 R 至少有两个元．这时 R 至少有一个不等于零的元 a．由 $0a = 0 \neq a$，知零元不会是 R 的单位元．再由任意的 $a \in R, 0a = 0$，知零元不会有逆元．同样，跟半群一样，如果一个元 $a \in R$ 有逆元，则逆元唯一．当然一个元 a 未必有逆元．同样一个元也可以仅有左逆元或右逆元，但若两个都存在时一定相等．我们仅讨论两者都存在且相等的元素，即具有逆元的元素．

整数环是一个有单位元的环，但除了 ± 1 以外，其他的整数都没有逆元．

消去律对于一个带有运算的集合来讲是一个很重要的性质．由于消去律与零因子存在密切的关系，因此在描述消去律之前，首先给出零因子的概念．

定义　4　若是在一个环里，如果满足：$a \neq 0, b \neq 0$ 但

$$ab = 0 ,$$

则称 a 是这个环的一个**左零因子**，b 是一个**右零因子**.

一个环若是交换环，一个左零因子也是一个右零因子．但在非交换环中，一个零因子未必同时是左也是右零因子．

一个环当然可以没有零因子，比如整数环．显然在而且只在一个没有零因子的环里式

$$ab = 0 \Rightarrow a = 0 \text{或} b = 0 \qquad (1)$$

才会成立．

例 2　一个数域 F 上一切 $n \times n$ 阶矩阵对于矩阵的加法和乘法来说，做成一个有单位元的环．当 $n \geq 2$ 时，这个环是非交换环，并有零因子．

零因子存在不存在同消去律成立不成立也有密切关系．

定理 1　无零因子环 R 两个消去律都成立，即

$$a \neq 0 , \quad ab = ac \Rightarrow b = c ,$$

$$a \neq 0 , \quad ba = ca \Rightarrow b = c .$$

反过来，在一个环里如果有一个消去律成立，那么这个环没有零因子．

证明　假定环 R 没有零因子．因为

$$ab = ac \Rightarrow a(b-c) = 0 .$$

在上述假定之下

$$a \neq 0 ,\ ab = ac \Rightarrow b - c = 0 \Rightarrow b = c .$$

同样可证

$$a \neq 0, ba = ca \Rightarrow b = c .$$

这样在 R 里两个消去律都成立.

反过来，假定在环 R 里第一个消去律成立．因为

$$ab = 0 \Rightarrow ab = a0 .$$

在上述假定之下，

$$a \neq 0, ab = 0 \Rightarrow b = 0 .$$

这就是说 R 没有零因子．第二个消去律成立的时候情形一样．得证.

推论 在一个环里如果有一个消去律成立，那么另一个消去律也成立.

在模素数 p 的剩余类环中，对任意的元素 $\bar{a}$，有 $p\bar{a} = \bar{0}$；一般地，在环 R 中，环 R 的元构成一个加群，对加群中每个非零元 a 来说，（1）式的成立与否由 a 在加群中的阶是否有限决定.

然而，在无零因子环中，由于（1）式成立，易知所有非零元的阶是相同的，为此先给出阶的定义.

定义 5 一个无零因子环 R 的非零元相同的阶（相对于加法）叫做 R 的**特征.**

定理 2 若无零因子环 R 的特征为有限整数 n，则 n 为素数.

证明 若 n 不是素数

$$n = ab,\ n \nmid a, n \nmid b ,$$

那么对环 R 里的非零元 x 来说

$$ax \neq 0 ,\ bx \neq 0 ,\ \text{但}\ (ax)(bx) = abx^2 = nx^2 = 0 ,$$

这就是说（1）式在 R 里不成立．矛盾.

以上介绍了一个环可能存在的四种特性乘法交换律，单位元，逆元，无零因子．下面给出适合上述全部条件或者部分条件的特殊环的定义.

定义 6 一个环 R 叫做**整环**，假如满足

（1） 乘法适合交换律；

（2） R 有单位元 e；

（3） R 没有零因子.

简单说，整环就是有单位元而没有零因子的交换环．整环满足上述描述的三个特性．对于另外一个特性-逆元，整环不一定成立．如整数环是一个整环，但有的元素不存在逆元． 现在我们给出具有上述所有特性的环——域的概念.

定义 7 一个至少含有两个元素的环 R 叫做**域**，假如

1　R 是交换环；

2．R 有一个单位元；

3．R 的每一个不等于零的元有一个逆元．

习惯上，记域 R 为 F . 显然 F 的每一个不等于零的元有一个逆元就意味者 F 无零因子. 因此域满足四个特性．

若 F^* 表示域中所有的非零元，由域的定义知 $(F^*, \bullet)$ 构成群. 因此域的定义等价于下列定义．

定义 7′　一个至少含有两个元素的环 F 定义了两种运算“+”与“$\bullet$”，如果

1　$(F, +)$ 为一个可换加群．

2　$(F^*, \bullet)$ 为可换乘群．

则 F 为域．

域的实例很多，如全体有理数的集合、全体实数、全体复数按普通意义下的加、乘运算构成域，这就是我们熟知的有理数域、实数域与复数域．

例 3　假定 F 是一个有 4 个元的域，则

1．F 的特征是 2；

2．F 的不是 0 或 1 的两个元满足方程 $x^2 = x - 1$．

证明　F 作为加群是有限的，所以其特征为素数 p，并且当然有 $p \mid 4$，所以 1 成立．

设 F 的其它两个元是 x_1，x_2，因为 $(F^*, \bullet)$ 为可换乘群，故 $x_1 x_2 \in F^*$，而且 x_1，x_2 都不是 1，故 $x_1 x_2 = 1$．另一方面，$(F, +)$ 为一个特征是 2 的加群，故又有 $x_1 + x_2 = 1$（考虑为什么不为 0），于是 x_1，x_2 是方程 $x^2 - x + 1 = 0$ 的两个根．

另外还有一种特殊的环是除环（或者称为体），这种环除了不一定满足交换律外，均满足域的其它特性．具体定义如下：

定义 8　一个至少含有两个元素的环 R 叫做**除环**，假如

1．R 有一个单位元．

2．R 的每一个不等于零的元有一个逆元．

在一个除环 R 里，方程

$$ax = b \quad 和 \quad ya = b \qquad (a, b \in R, a \neq 0)$$

各有一个唯一的解，分别记为 $a^{-1}b$ 和 ba^{-1}．在一个除环里，$a^{-1}b$ 未必等于 ba^{-1}．

但在域中，$a^{-1}b = ba^{-1}$．记 $a^{-1}b = ba^{-1} = \dfrac{b}{a}$，这时我们就可以得到类似于数的商的计算．

（1） $\frac{a}{b}=\frac{c}{d}$，当而且只当 $ad=bc$ 的时侯.

（2） $\frac{a}{b}\pm\frac{c}{d}=\frac{ad\pm bc}{bd}$.

（3） $\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}$.

（4） $\frac{a}{b}\Big/\frac{c}{d}=\frac{ad}{bc}$.

我们只证明（1）

$$\frac{a}{b}=\frac{c}{d}\Rightarrow bd\frac{a}{b}=bd\frac{c}{d}\Rightarrow ad=bc$$

并且因为消去律在一个域内成立(域无零因子)，

$$\frac{a}{b}\neq\frac{c}{d}\Rightarrow bd\frac{a}{b}\neq bd\frac{c}{d}\Rightarrow ad\neq bc\ .$$

（2)、(3）个式子的成立也只要两边用 bd 一乘就可以看出.

（4）是很自然的.

例 4　设 R 是一个有单位元 1 的有限整环，则 R 是一个域.

证明　任取 $a\in R^*$，只需证 a^{-1} 存在．考虑 R 到 R 的映射

$$f:x\mapsto ax\ ,$$

此处 x 是 R 的任意元，由于 R 中消去率成立，故

$$x_1\neq x_2\Rightarrow ax_1\neq ax_2\ .$$

设 R 含有 n 个元，则

$$f(R)=\{ax\mid x\in A\}$$

也含有 n 个元．故 $f(R)=R$，即 f 是双射．从而存在 $x\in R$ 满足 $ax=1$，即 $x=a^{-1}$.

例 5　当 p 是素数时，模 p 的剩余类环 Z_p 是一个域.

证明　易知 Z_p 是一个含有 p 个元的交换环，且有单位元 $\overline{1}$．如果证明 Z_p 不含零因子，那么 Z_p 是一个有限整环，从而是一个域.

设 $\overline{a}$ 是 Z_p 的一个零因子，于是存在 $\overline{b}\in Z_p,\overline{b}\neq\overline{0},\quad \overline{ab}=\overline{0}$.　因 $\overline{b}\neq\overline{0}$，　所以 $p\nmid b$．又　$\overline{ab}=\overline{0},$　故

$$p \mid ab \Rightarrow p \mid a \Rightarrow \bar{a} = \bar{0}\ .$$

这就是说 Z_p 的零因子 $\bar{a}$ 只有 $\bar{0}$，从而 Z_p 是一个整环.

例6 $F = \{$ 所有实数 $a + b\sqrt{3}, (a, b$ 是有理数$)\}$，证明 F 对普通加法和乘法来说是一个域.

证明 （1）首先证明 F 对于数的加乘运算封闭对任意 $a_1 + b_1\sqrt{3},\ \ a_2 + b_2\sqrt{3} \in F$，

$$(a_1 + b_1\sqrt{3}) + (a_2 + b_2\sqrt{3}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{3} \in F\ ,$$

$$(a_1 + b_1\sqrt{3})(a_2 + b_2\sqrt{3}) = (a_1a_2 + 3b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{3} \in F\ ,$$

所以 F 对乘法和加法运算是封闭的.

（2）容易验证，F 满足乘法和加法结合律，分配律.

（3）加法单位元为 0，乘法单位元为 1.

（4）任意的 $a + b\sqrt{3} \in F$，加法逆元为 $-(a + b\sqrt{3})$, 乘法逆元为 $(a - b\sqrt{3})/(a^2 - 3b^2)$，

所以 F 对加法构成群，F^* 对乘法构成群.

容易看出 $(F, +)$ 和 $(F^*, \times)$ 都为可换群，所以 F 为域.

§3 子环、理想、环的同态

给定环 R 的定义，本节将讨论给定环的一个子集 S 关于环 R 的加、乘运算也构成环的充要条件．给定一个子环 S，子环关于加法构成 R 的子加群，因此环 R 关于子加群的陪集在同样的加、乘运算下也构成一个环-商环，这样的子环称为理想．另外，如同群论一样，我们还将讨论在环同态的条件下，商环和理想的关系．所有这一切即为本节描述的内容.

首先给出子环的定义.

定义 1 一个环 R 的一个子集 S 叫做 R 的一个**子环**，假如 S 本身对于 R 的代数运算来说作成一个环.

一个除环 R 的一个子集 S 叫做 R 的一个**子除环**，假如 S 本身对于 R 的代数运算来说作成一个除环.

同样，我们可以规定子整环．子域的概念.

定理 1 一个环 R 的非空子集 S 作成一个子环的充要条件是

$$a, b \in S \Rightarrow a - b \in S,\ ab \in S\ .$$

证明留作习题.

R 本身也是 R 的一个子环，此外，R 中仅含有一个零元的子集 $\{0\}$ 也是 R 的一个子环．故任一环至少有两个子环.

例 1 模 6 剩余类环 $Z_6=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$，子环为 $\{\bar{0}\}$，$\{\bar{0},\bar{2},\bar{4}\}$，$\{\bar{0},\bar{3}\}$，$Z_6$.

作为练习，留给读者自己证明 R 的两个子环 S_1, S_2 的交集 $S_1 \cap S_2$ 是 R 的一个子环．一般的，设 $\{S_\alpha\}_{\alpha\in B}$ 是 R 的子环的族，则 $\bigcap\limits_{\alpha\in B} S_\alpha$ 也是 R 的子环.

任取 R 的一个非空子集 T，则 R 中总存在子环含有 T，例如 R 本身就是这样的一个子环，命 $\{S_\alpha \mid \alpha\in B\}$ 是 R 中含有 T 的所有环的族，于是 $\bigcap\limits_{\alpha\in B} S_\alpha$ 是 R 的含有 T 的最小子环，称这个子环为 T 生成的子环，通常记为 $[T]$.

设 F 是一个域，S 是 F 的一个非空子集，则 F 中含有 S 的所有子域的交集是 F 的一个子域，这是 F 中含有 S 的最小子域，称之为 F 中 S 生成的子域.

设 S 是域 F 的一个子环，则 F 中 S 生成的子域恰好由一切形如 ab^{-1} 的元所组成，此处 $a,b\in S$，$b\neq 0$.

例 2 一个环 R 的可以同每一个元交换的元作成一个子环 I，这个子环叫做 R 的**中心**.

证明 只需证任意的 $x,y\in I$，有

$$x-y\in I,\quad xy\in I.$$

而对任意 $a\in R$，

$$(x-y)a=xa-ya=ax-ay=a(x-y);$$

$$(xy)a=x(ay)=(xa)y=a(xy).$$

所以 I 构成环.

显然，一个环的中心是一个交换子环．并且，当 R 为除环时，R 的中心是一个交换的除环，即一个域.

显然子环 S 关于加法构成的子加群 $(S,+)$ 为加群 $(R,+)$ 的不变子加群．由此知子加群 $(S,+)$ 的陪集关于陪集的加运算构成加商群．现在我们考虑的一个问题是，如何定义这个加商群的另一运算-乘运算，使之构成环．首先介绍一个相关的概念-理想．理想是一种特别重要的子环，这种子环在环论里的地位如同不变子群在群论里的地位.

定义 2 环 R 的一个非空子集 A 叫做一个理想子环，简称理想，假如

(1) $a,b\in A\Rightarrow a-b\in A$，

(2) $a \in A, r \in R \Rightarrow ra, ar \in A$.

由(1)知理想 A 是一个加群；由(2)知 A 对于乘法来说是闭的，所以理想一定是子环．一个环至少有以下两个理想：

1．只包含零元的集合，这个理想叫做 R 的零理想；

2． R 本身为 R 的理想．

除了以上两种理想，其它的理想称为真理想．

例 3 除环没有真理想．

证明 假定 A 是 R 的一个理想而 A 不是零理想．那么 $0 \neq a \in A$，由理想的定义，$a^{-1}a = 1 \in A$，因而 R 的任意元 $B = B \cdot 1 \in A$． 这就是说， $A = R$ ．证完．

因此，理想这个概念对于除环或域没有多大用处．

定义 3 设 R 是一个环， $a \in R$， R 中含 a 的最小理想叫做 a 生成的一个主理想，用符号 (a) 表示．

设 R 是任意环，命 A 表示 R 中一切如下形式的元素的集合

$$\sum x_i a y_i + sa + at + na\,, \qquad (1)$$

此处 a 是从 R 中取定的元素， x_i, y_i, s, t 是 R 的任意元， $n \in Z$ ，则 A 作成 R 的一个理想．

这是因为，任意 $x, y \in A$，则 $x - y$ 仍可表成（1）的形式，并且任取 $r \in R$，

$$y = \sum x_i a y_i + sa + at + na \in A\,,$$

则

$$ry = \sum (rx_i) a y_i + (rs)a + rat + (nr)a\,, \quad yr = \sum x_i a (y_i r) + sar + a(tr + nr)$$

都是（1）的形式，故 $ry, yr \in A$．即 A 是 R 的一个理想．

下证 A 是 R 中包含 a 的最小理想，首先， A 是含有 a 的一个理想，其次，设 B 是 R 中含 a 的一个理想，则对任意 x_i, y_i, s, t,

$$\sum x_i a y_i + sa + at + na \in B\,,$$

故 $A \subseteq B$．

在一些特殊环中， 一个主理想 (a) 的元的形式可以简化．如当 R 是交换环时， (a) 的元显然都可以写成

$$ra + na (r \in R, n \text{ 是整数})$$

的形式．当 R 有单位元的时候，(a) 的元都可以写成

$$\sum x_i a y_i \ (x_i, y_i \in R)$$

的形式，因为这时 $sa = sae, at = eat, na = (ne)ae.$ 当 R 既是交换环又有单位元的时候，(a) 的元可以写成

$$ra \ (r \in R)$$

的形式．

容易证明，R 的两个理想 A，B 的交集 $A \cap B$ 仍是 R 的一个理想．一般的，设 $\{A_a\}_{a \in B}$ 是 R 的理想的非空集合，则 $\bigcap\limits_{a \in B} \{A_a\}$ 仍是 R 的理想．取 T 是 R 的任一非空子集，命 $\{A_a\}$ 表示 R 中一切包含 T 的理想（这样的理想一定存在，例如 R 就是其中之一），和子环的情形类似，我们称理想 $\bigcap \{A_a\}$ 为 R 中 T 生成的理想，用符号 (T) 表示．特别，当 $T = \{a\}$ 时，(T) 即 a 生成的主理想．当 $T = \{a_1, a_2, \cdots, a_n\}$ 时，(T) 记为 $(a_1, a_2, \cdots, a_n)$．

一个很自然的问题是 (T) 由 A 中哪些元素所组成．容易证明

$$(T) = \{\sum x_i \mid x_i \in (t_i), t_i \in T\}.$$

设

$$A = \{\sum x_i \mid x_i \in (t_i), t_i \in T\},$$

显然 A 是一个理想，且 $T \subseteq A$，故 $(T) \subseteq A$．

另一方面，对任意 $t_i \in T$，$(t_i) \subseteq (T)$，故 $\sum x_i \in (T)$，此处 $x_i \in (t_i)$，于是，有 $A \subseteq T$，即 $T = A$．

例 4　假定 $R[x]$ 是整数环 R 上的一元多项式环，证明理想 $(2, x)$ 不是主理想．

证明　因为 $R[x]$ 是有单位元的交换环，所以

$$(2, x) = \{2 f(x) + x g(x) \mid f(x), g(x) \in R[x]\} \qquad (2)$$

从而

$$(2,x)=\{2a_0+a_1x+\cdots+a_nx^n \mid a_i\in R, n\geq 0\}.$$

若$(2,x)$是一个主理想，不妨设

$$(2,\ x)=(p(x)),$$

因而

$$2=q(x)p(x),\quad x=h(x)p(x).$$

由

$$2=q(x)p(x),$$

知 $p(x)=a,$且$a=\pm 1$或± 2；从而

$$x=ah(x)$$

知$a=\pm 1$，这样$\pm 1=p(x)\in(2,x)$．从而

$$(2,x)=R[x]$$

与（2）的形式矛盾．得证．

有了理想，就可以定义商环的概念．

给了一个环R和R的一个理想A，若我们只就加法来看，R作成一个加群，A作成R的一个不变加子群．这样A的陪集集合

$$R/A=\{\overline{a} \mid a\in R\}$$

上很自然就已经定义了一个加法运算：

$$\overline{a}+\overline{b}=\overline{a+b}$$

其中$\overline{a}=\{a+x \mid a\in R, x\in A\}$．$R/A$关于加法运算构成一个加群．通常 R/A也称为模A的剩余类．

现在我们规定的R/A运算：

$$\overline{a}\cdot\overline{b}=\overline{ab} \qquad (2)$$

首先证明该乘法运算为R/A上的二元运算．若$a_1\in\overline{a}$，$b_1\in\overline{b}$，只要证明

$$\overline{a_1b_1}=\overline{ab}.$$

由于

$$a_1 = a + x_1,\ \ b_1 = b + x_2,\ \ x_1, x_2 \in A\ ,$$

我们有

$$a_1 b_1 = (a + x_1)(b + x_2) = ab + x_1 b + a x_2 + x_1 x_2 = ab + x_3\ ,$$

因为 $x_3 \in A$ 即

$$a_1 b_1 - ab \in A \Rightarrow \overline{a_1 b_1} = \overline{ab}\ .$$

即（2）规定的 R/A 的乘法为二元运算．因

$$(\overline{a} \cdot \overline{b})\overline{c} = \overline{ab} \cdot \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}\,\overline{bc} = \overline{a}(\overline{b} \cdot \overline{c})$$

故 $(R/A, \cdot)$ 是一个半群．

我们知道， R/A 的加法也是用代表相加来规定的，故有

$$\overline{a}(\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b + c} = \overline{a(b + c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}\ .$$

同样，

$$(\overline{b} + \overline{c})\overline{a} = \overline{b} \cdot \overline{a} + \overline{c} \cdot \overline{a}\ .$$

即 $(R/A, +, \cdot)$ 作成一个环．

定义 5　设 R 是一个环， A 是 R 的一个理想，商群 R/A 关于乘法（2）所作成的环，叫做 R 关于 A 的商环．仍用记号 R/A 表示．商环 R/A 也叫做 R 关于 A 的剩余类环．

例 5　取整数环 Z 的主理想 (m)，则商环 $Z/(m)$ 含有 m 个元，任一元 $\overline{a}$ 由所有被 m 除余 a 的整数组成，故称 $\overline{a}$ 为模 m 的一个剩余类， $Z/(m)$ 为模 m 的剩余类环．

例 6　A 是偶数环， $\alpha = \{4x \mid x \in Z\}$，则 α 是 A 的一个理想，而且就是 (4)，而二元环 A/α 不是域．

证明　对任意 $x, y \in z$，

$$4x - 4y = 4(x - y) \in \alpha\ ,$$

而且对 $z \in A$，

$$z \times 4x = 4zx \in \alpha\ ,$$

所以 α 作成 A 的理想．又由于 $4 \in \alpha$，且 $4 \mid 4x$，故 $\alpha = (4)$．而 A/α 是集合 $\{\overline{0}, \overline{2}\}$，其中的

加法构成加群，单位元为 $\overline{0}$；乘法封闭．所以 A/α 是环．但由 $\overline{2}\times\overline{2}=\overline{0}$，所以乘法中没有单位元，故 A/α 不是域．

例7 系数取值于数域 F 的所有 x 的多项式关于多项式的加法和乘法构成一个环 $F[x]$，叫做多项式环．任取 F 上的一个 n 次多项式 $f(x)$ 构成理想为

$$(f(x))=\{f(x)g(x)\mid \forall g(x)\in F[x]\}.$$

商环

$$F[x]/(f(x))=\{\overline{r(x)}\mid \forall r(x)\in F[x], r(x)\text{的次数小于}n.\}.$$

$F[x]/(f(x))$ 是一个域充要条件是 $f(x)$ 是不可约多项式．

证明 前两个问题证明比较简单留给读者自己补出．我们只给出最后充要条件的证明．

充分性：$f(x)$ 是不可约多项式，只需证明它的非零元 $\overline{g(x)}\neq 0$ 有逆元．因为 $\overline{g(x)}\neq 0$，故 $f(x)\nmid g(x)$．由 $f(x)$ 不可约，所以 $g(x)$ 和 $f(x)$ 互素，这时必有多项式 $s(x)$ 和 $t(x)$ 使得

$$s(x)f(x)+t(x)g(x)=1,$$

从而

$$\overline{t(x)}\cdot\overline{g(x)}=\overline{1},$$

即 $\overline{g(x)}$ 有逆元 $\overline{t(x)}$．

必要性：若 $f(x)$ 是可约多项式，则存在两个次数小于 n 的多项式 $g(x),h(x)$，使

$$f(x)=g(x)h(x),$$

所以

$$\overline{h(x)}\cdot\overline{g(x)}=\overline{0},$$

从而 $F[x]/(f(x))$ 有零因子，矛盾．得证．

定义 6 设 R, R' 是两个环，如果存在 R 到 R' 的一个映射

$$f:\ R\to R'$$

使得

$$f(a+b)=f(a)+f(b),\quad f(ab)=f(a)\cdot f(b)$$

对一切$a,b\in R$均成立，那么就说f是R到R'上的一个同态映射．如果f是R到R'的满射，那么就说f是满同态，用符号$R\sim R'$表示．如果R到R'的同态映射f是R到R'的单射，那么就说f是R到R'的单一同态．如果这个f是环R到R'的双射，那么就说f是R到R'的一个同构映射．存在同构映射的两个环叫做同构的，记为$R\cong R'$．

例 8　设$T=R[x], A=(x^2+1)$，证明　$T/A\cong C$，其中C为复数乘群．

证明　任取$f(x)\in T$，则

$$f(x)=q(x)(x^2+1)+ax+b,$$

此处$a,b\in R$，即

$$f(x)\equiv ax+b(\mathrm{mod}\,A).$$

任取两个次数至多为 1 的多项式$ax+b, cx+d$, 当且仅当$a=c, b=d$时，

$$(ax+b)-(cx+d)\in A,$$

即

$$ax+b\equiv cx+d(\mathrm{mod}\,A),$$

由此可知

$$T/A=\{\overline{ax+b}\,|\,a,b\in R\}.$$

令

$$f: ax+b\mapsto ai+b$$

显然f为T/A到C的双射．

下证f保持环的运算

$$f(\overline{ax+b}+\overline{cx+d})=f(\overline{(a+c)x+(b+d)})=(a+c)i+(b+d)$$

$$=f(\overline{ax+b})+f(\overline{cx+d})$$

$$f(\overline{ax+b}\cdot\overline{cx+d})=f(\overline{acx^2+(ad+bc)x+bd})=f(\overline{(ad+bc)x+bd-ac})$$

$$=(ad+bc)i+bd-ac=f(\overline{ax+b})\cdot f(\overline{cx+d}).$$

得证，即

$$R[x]/(x^2+1)\cong C.$$

例 9　设 A 是高斯整数环，即一切形如 $a+bi$ $(a,b$ 是任意整数）的复数（叫做高斯整数）作成的数环.

设 $\alpha=(1+i),$　我们看 A/α 由那些元素所组成. 为此，首先弄清楚 α 由哪些元所组成. 由于 A 是有单位元的可换环，故 α 由一切形如

$$(x+yi)(1+i)=(x-y)+(x+y)i$$

的复数所组成，此处 x,y 是任意整数. 注意 $x-y$，$x+y$ 只能同时为奇，或同时为偶，而且，对于任意高斯整数 $a+bi$，只要 a,b 的奇偶性相同，则方程组

$$\begin{cases}x-y=a\\x+y=b\end{cases}$$

恒有整数解，即 $a+bi\in\alpha$，因此，α 由一切高斯整数 $a+bi$ 所组成，此处 a,b 的奇偶性相同. 由此可见，对任意 $a+bi\in A$，只要 a,b 奇偶性相同，恒有

$$a+bi\equiv 0(\alpha),$$

若 $a+bi\in A, a, b$ 的奇偶性不同，则

$$a+bi\equiv 1(\alpha),$$

即 $A/\alpha=\{\bar{0},\bar{1}\}$，从而 A/α 是仅含两个元的域，即 $A/\alpha\cong Z_2$.

环与同态环之间，由下列性质.

定理 2　假定 R 和 $\overline{R}$ 是两个环，并且 R 与 $\overline{R}$ 同态. 那么 R 的零元的象是 $\overline{R}$ 的零元，R 的元 a 的负元的象是 a 的象的负元. 并且假如 R 是交换环，那么 $\overline{R}$ 也是交换环. 假如 R 有单位元1，那么 $\overline{R}$ 也有单位元 $\bar{1}$，而且 $\bar{1}$ 是1的象.

定理 3　若是存在一个环 R 到 $\overline{R}$ 的满射，使得 R 与 $\overline{R}$ 对于一对加法以及一对乘法来说都同态，那么 $\overline{R}$ 也是一个环.

同群的情形类似，留作习题.

定理 4　　设 f 是满同态 $R \sim R'$，$\ker f \supseteq A$，A 是 R 的一个理想，则存在 R/A 到 R' 的唯一的满同态 f_*，对 R 到 R/A 的自然同态（即 R 到 R/A 的满同态）φ，满足 $f = f_* \circ \varphi$. 当且仅当 $\ker f = A$ 时，f_* 是 R/A 到 R' 的同构.

证明　由于 f, φ 都是群同态，故由的群的同态定理，适合要求的 f_*（作为群同态）是唯一存在的.

设 $x \in R$，则

$$f(x) = (f_* \circ \varphi)(x) = f_*(\varphi(x)).$$

故对于 $a, b \in R$，有

$$f(ab) = f_*(\varphi(ab)) = f_*(\varphi(a)\varphi(b)) = f_*(\varphi(a)) f_*(\varphi(b)) = f(a) f(b)$$

即 f_* 保持乘法. 所以 f_* 也是环里的同态. 定理得证.

由上边的定理可以推出.

定理 5（环的同态定理）　设 R 是一个环，则 R 的任一商环都是 R 的同态象. 反之，若 R' 是 R 在 f 下的同态象，则 $R' \cong R/\ker f$.

§4　商　域

我们知道，整数环是有理数域的一个子环；有理数域是包含整数环的最小的一个域. 现在我们问，给了一个环 R，是不是可以找得到一个域包含这个 R. 一个环 R 要能被一个域包含，有一个必要条件就是 R 不能有零因子，并且 R 为交换环. 我们在这一节里要证明当 R 是无零因子交换环时，一定存在一个最小的域，使环中的任意元素在域中恰有逆元.

定理 1　每一个没有零因子的交换环 R 都是一个域 Q 的子环.

证明　当 R 只包含零元的时候，定理显然是对的.

假定 R 至少有两个元. 用 $a, b, c\cdots$ 来表示 R 的元，我们作一个集合

$$A=\{(a,b)\mid a,b\in R,b\neq 0\}.$$

实际上 A 为加氏积 $R\times R$ 的子集．在 A 的元间我们规定一个关系

$$\backsim:\quad (a,b)\backsim(a',b')\Leftrightarrow ab'=a'b\ .$$

很明显这样定义的关系满足

(a) $(a,b)\backsim(a,b)$；

(b) $(a,b)\backsim(a',b')$，则 $(a',b')\backsim(a,b)$；

(c) $(a,b)\backsim(a',b')$，$(a',b')\backsim(a'',b'')\Rightarrow(a,b)\backsim(a'',b'')$.

这样, ～是一个等价关系. 这个等价关系把集合 A 分成若干类 $\overline{(a,b)}$，将等价类 $\overline{(a,b)}$ 记为 $\overline{\frac{a}{b}}$，

令

$$Q_0=\left\{\overline{\frac{a}{b}}\mid a,b\in R,b\neq 0\right\}.$$

对于 Q_0 的元我们规定以下两个运算

$$\overline{\frac{a}{b}}+\overline{\frac{c}{d}}=\overline{\frac{ad+bc}{bd}}\qquad \overline{\frac{a}{b}}\cdot\overline{\frac{c}{d}}=\overline{\frac{ac}{bd}}$$

下证上述两个规定为 Q_0 上的二元运算．因为

（1） 由 $b\neq 0,d\neq 0\Rightarrow bd\neq 0$ 知

$$\overline{\frac{ad+bc}{bd}},\ \overline{\frac{ac}{bd}}\in Q_0\ .$$

（2）若 $\overline{\frac{a}{b}}=\overline{\frac{a'}{b'}}$，$\overline{\frac{c}{d}}=\overline{\frac{c'}{d'}}$，那么

$$ab'=a'b,\ \ cd'=c'd$$
$$ab'dd'=a'bdd',\ \ cd'bb'=c'dbb',$$
$$(ad+bc)b'd'=(a'd'+b'c')bd,$$

所以

$$\overline{\frac{a}{b}}+\overline{\frac{c}{d}}=\overline{\frac{a'}{b'}}+\overline{\frac{c'}{d'}}\quad .$$

由 $ab'cd'=a'bc'd$，所以

$$\overline{\frac{a}{b}}\cdot\overline{\frac{c}{d}}=\overline{\frac{a'}{b'}}\cdot\overline{\frac{c'}{d'}}.$$

两类相加相乘的结果与类的代表无关，因此两者均为二元运算.

现在证明 Q_0 对于对于上述加法、乘法运算构成域.

1 $(Q_0,+)$ 为加群；

(1) $$\overline{\frac{a}{b}}+\overline{\frac{c}{d}}=\overline{\frac{c}{d}}+\overline{\frac{a}{b}}.$$

(2) $$\overline{\frac{a}{b}}+\left(\overline{\frac{c}{d}}+\overline{\frac{e}{f}}\right)=\overline{\frac{a}{b}}+\overline{\frac{cf+de}{df}}\quad=\overline{\frac{adf+bcf+bde}{bdf}}.$$

(3) $$\overline{\frac{0}{b}}+\overline{\frac{c}{d}}=\overline{\frac{bd}{bd}}+\overline{\frac{0}{b}}.$$

(4) $$\overline{\frac{a}{b}}+\overline{\frac{-a}{b}}=\overline{\frac{0}{b}}.$$

Q_0 的不等于零的元对于乘法来说作成一个交换群，法适合交换律与结合律，显然 $\overline{\frac{a}{a}}$ 是单位元；$\overline{\frac{a}{b}}$ 的逆元是 $\overline{\frac{b}{a}}$．容易验算，分配律也成立． 这样，Q_0 作成一个域.

我们把 Q_0 的所有的元 $\overline{\frac{qa}{q}}$ （q 是一个固定的元，a 任意）放在一起，作成一个集合 R_0，那么 $a\to\overline{\frac{qa}{q}}$ 是一个 R 与 R_0 间的一一映射．由于

$$\overline{\frac{qa}{q}}+\overline{\frac{qb}{q}}=\overline{\frac{q^2(a+b)}{q^2}}=\overline{\frac{q(a+b)}{q}}.$$

$$\overline{\frac{qa}{q}}\cdot\overline{\frac{qb}{q}}=\overline{\frac{q(ab)}{q}}.$$

以上映射是同构映射 $R\cong R_0$．这样由环的同态定理知，有一个包含 R 的域 Q 存在．证完．

Q 既然是包含 R 的域， R 的一个元 $b\neq 0$ 在 Q 里有逆元 b^{-1}，因而 $ab^{-1}=b^{-1}a=\frac{a}{b}$（$a,b\in R,b\neq 0$）在 Q 里有意义．我们有

定理 2 Q 刚好是由所有元

$$\frac{a}{b}\quad（a,b\in R,b\neq 0）$$

所作成的, 这里 $\frac{a}{b}=ab^{-1}=b^{-1}a$.

证明 要证明 Q 的每一个元可以写成 $\frac{a}{b}$ 的样子, 只须证明 Q_0 的每一个元可以写成

$$\overline{\frac{qa}{q}/\frac{qb}{q}}=\overline{\frac{qa}{q}}\cdot\overline{\frac{qb}{q}}^{-1}$$

的样子， 我们看 Q_0 的任意元 $\overline{\frac{q}{b}}$，由于

$$\overline{\frac{qb}{q}}^{-1}=\overline{\frac{q}{qb}}$$

我们的确有

$$\overline{\frac{qa}{q}}\overline{\frac{qb}{q}}^{-1}=\overline{\frac{q^2a}{q^2b}}=\overline{\frac{a}{b}}=\overline{\frac{qa}{q}/\frac{qb}{q}}$$

至于每一个 $\frac{a}{b}$ 都属于 Q 是显然的．证完．

因为 Q 的元都可以写成 $\frac{a}{b}$ 的样子，故它们有以下性质

$$(*)\qquad \begin{cases} \dfrac{a}{b}=\dfrac{c}{d}, \text{当且仅当} ad=bc \\ \dfrac{a}{b}+\dfrac{c}{d}=\dfrac{ad+bc}{bd} \\ \dfrac{a}{b}\cdot\dfrac{c}{d}=\dfrac{ac}{bd} \end{cases}$$

这样，Q 与 R 的关系正同有理数域与整数环的关系一致.

定义 一个域 Q 叫做环 R 的一个商域，假如 Q 包含 R，并且 Q 刚好是由所有元

$$\frac{a}{b}\ （a,b\in R,b\neq 0）$$

所作成的.

由定理 1 和 2，一个有两个以上的元的没有零因子的交换环至少有一个商域.

一般，一个环很可能有两个以上的商域. 我们有

定理 3 假定 R 是一个有两个以上的元的环，F 是一个包含 R 的域. 那么 F 包含 R 的一个商域.

证明 在 F 里

$$ab^{-1}=b^{-1}a=\frac{a}{b}\ （a,b\in R,b\neq 0）$$

有意义. F 的子集

$$\overline{Q}=\left\{\text{所有}\frac{a}{b}\right\}\ （a,b\in R,b\neq 0）$$

$\overline{Q}$ 显然是 R 的一个商域. 证完.

但 R 的每一个商域都适合计算规则(*)，而计算规则(*)完全决定于 R 的加法和乘法;这就是说，R 的商域的构造完全决定于 R 的构造. 所以我们有

定理 4 同构的环的商域也同构.

习题

1．设环 R 有且只有一个右单位元，证明：R 有单位元.

2．证明：$Z[i]=\{a+bi\mid a,b\in Z, i \text{是虚数单位}\}$ 关于数的加法、乘法作成一个环.

3．证明：任意一个不仅含有一个数的有限集关于数的加法和乘法不能做成一个环.

4．在 Z_{15} 中，找出方程 $x^2-1=0$ 的全部根.

5． A 是所有分母为 2 的非负整数次方幂的既约分数所成集合，问 A 关于数的加法、乘法是否作成一个环.

6．设环 R 的加群 $(R,+)$ 是循环群，则 R 是可换环.

7．设环 R 是可换环， A 是 R 的理想， S 是 R 的子集，令

$$(A:S)=\{x \mid x\in R, xS\subseteq A\}$$

证明：$(a:S)$ 是 R 的一个理想.

8．设 S 表示 A 的一切不是零因子的元的集合，证明： S 是 $(A,\cdot)$ 的子半群.

9．设 S 是域 F 的一个子环，证明： S 是子域的充要条件是对任意 $x\in S$， $x\neq 0$，均有 $x^{-1}\in S$.

10．设 F 是域，问多项式环 $F[x]$ 的主理想 (x^2) 含有哪些元． $F[x]/(x^2)$ 含有哪些元.

11．如果对环 R 的元 a 存在正整数 n，使 $a^n=0$，则称 a 为 R 的幂零元．若 R 是含单位元， a 为 R 的幂零元，证明： $1-a$ 是 R 的可逆元，并求其逆元.

12．设 R 是有单位元的含有有限个元的交换环，证明： R 的元不是可逆元（单位）就是零因子，由此证明含有有限个元的整环是域.

13．设 a,b 是环 A 的两个理想，证明： $a\cap b$ 是 A 的一个理想．设 $\{a_\alpha \mid \alpha\in B\}$ 是 A 的理想的族，证明： $\bigcap\limits_{\alpha\in B}a_\alpha$ 仍是 A 的理想.

14．设 a,b 是环 A 的两个理想，证明： $ab\subseteq a\cap b$．举例说明， ab 可以真包含于 $a\cap b$ 中.

15．设 $A=(Z)_3$ 是 Z 上 3 阶方阵环．证明：

$$B=\left\{\begin{pmatrix}0 & a & b\\ 0 & 0 & c\\ 0 & 0 & 0\end{pmatrix}\middle| a,b,c\in Z\right\}$$

是 A 的一个子环， B 不是 A 的理想？求 $B^2=?$ $B^3=?$.

16．举一个环 A 的例子， A 含有子环 $B\neq 0, B^n\neq 0,$ 但 $B^{n+1}=0$.

17．在高斯整数环 $Z[i]$ 中，$a=(2+i)$ 含有哪些元？$Z[i]/(2+i)$ 含有哪些元?

18．设 A 是偶数环，$a=\{4x \mid x\in Z\}$，证明：a 是 A 的一个理想．A/a 是怎样的环？a 是否就是 (4)？$A/(4)$ 是不是域?

19．证明：$(3)/(6)$ 是 $Z/(6)$ 的理想．且

$$\frac{Z/(6)}{(3)/(6)}\cong Z/(3)\,.$$

20．设 $f(x)\in R[x], f(x)=a_0+a_1x+\cdots+a_nx^n$．命

$$f:\ f(x)\mapsto a_0$$

证明：f 是 $R[x]$ 到 R 的满同态，求 $\ker f=?R[x]/\ker f$ 与怎样的环同构？

21．证明：高斯整数环 $Z[i]$ 同构于 $Z[x]/(x^2+1)$

22．找出 Z 到自身的一切同态映射，并找出每一同态的核

23．找出 Z_2 到 Z 的一切同态映射．