第一章　环、模

1.1　环的定义

1.1.1　环的定义

定义 1.1.1

R 是一个集合，如果存在两个运算 $+: R\times R\to R$ 和 $\cdot: R\times R\to R$

分别称为加法和乘法，满足下列条件：

①（加法单位元存在）存在一个元素 $0_R\in R$，称为加法单位元，使得对于任意 $x\in R$，有 $x+0_R=0_R+x=x$。

②（加法交换律）$\forall x,y\in R, x+y=y+x$

③（加法结合律）$\forall x,y,z\in R,(x+y)+z=x+(y+z)$

④（加法逆存在）$\forall x\in R,\exists -x\in R$，称为加法逆，使得 $x+(-x)=0_R$

⑤（乘法结合律）$\forall x,y,z\in R,(x\cdot y)\cdot z=x\cdot(y\cdot z)$

⑥（左分配律）$\forall x,y,z\in R,x\cdot(y+z)=x\cdot y+x\cdot z$

（右分配律）$\forall x,y,z\in R,(y+z)\cdot x=y\cdot x+z\cdot x$

那么我们称 $(R,+,\cdot)$ 是一个环，简称为环 R。

相比域的定义，环的定义仅涉及 6 条性质，去除了单位元存在、可交换、可逆三条性质。在研究环时，我们有时也会考虑存在单位元和可交换的环，因此有以下定义：

定义 1.1.2: 交换环、幺环

如果环 R 满足：$\forall x,y\in R,x\cdot y=y\cdot x$，那么我们称 R 是一个交换环；

如果环 R 满足：$\exists 1_R\in R,\forall x\in R,1_R\cdot x=x\cdot 1_R=x$，称为乘法单位元，

1.1.2 环的性质

1.1.3 整环

定义 1.1.3: 零因子

设 R 是一个环，如果 $\exists x, y \in R, x, y \neq 0_R$，使得 $x \cdot y = 0_R$，那么我们称 x, y 是 R 的零因子。

定义 1.1.4: 整环

如果环 R 是一个交换幺环，并且不包含零因子，那么我们称 R 是一个整环。

定理 1.1.1: 循环的整环必有素零因子

设 R 是一个整环，

我们定义：$N : \mathbb{Z} \ni n \mapsto n_R \in R$，满足 $(n+1)_F = n_F + 1_F$

如果 $\exists a \in R, a \neq 0, \exists n \in \mathbb{N}_+, n_F a = 0_R$

那么存在素数 p，$\forall b \in R, p_R b = 0_R$

证明: 取 $\forall b \in R$,

$0_R = 0_R \cdot b = (n_R a)b = a(n_R b)$

因为 $a \neq 0$，而 R 是整环，所以一定有 $n_R b = 0$，因此，$\{k \in \mathbb{N}_+ | k_R b = 0\}$ 不是空集。

取 p 为使 $p_R b = 0$ 的最小正整数。如果 p 是素数，命题成立；

如果 p 不是素数，那么只需要对 p 作唯一分解，那么有 $\left(\prod_{i=1}^{q} p_{i_R}\right) b = 0$

那么，一定存在一个 $p_{i_R} b = 0$，此时命题也是成立的。 □

1.1.4 子环

我们也类似地提出后续我们会提及的子环的概念。

定义 1.1.5: 子环

设 R 是一个环，集合 $S \subseteq R$，

如果 S 对 R 上的加法和乘法也构成一个环，那么我们称 S 是 R 的子环。

1.2 环的同态

我们类似于域的同态，定义出环的同态。

1.2.1 定义

定义 1.2.1: 环同态

设 R, S 是两个环，如果映射 $\varphi : R \to S$ 满足：

$\forall a, b \in R, \varphi(a+b) = \varphi(a) + \varphi(b), \varphi(ab) = \varphi(a)\varphi(b)$

并且如果 R, S 均是幺环，$\varphi(1_R) = 1_S$

那么我们称 φ 是一个 R 到 S 的环同态。

显然，同态一定将零元映射到零元

命题 1.2.1. 设 $\varphi : R \to S$ 是一个环同态，那么 $\varphi(0_R) = 0_S$

证明: $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$

$\Rightarrow -\varphi(0_R) + \varphi(0_R) = -\varphi(0_R) + \varphi(0_R) + \varphi(0_R)$

$\Rightarrow \varphi(0_R) = 0_S$ □

定义 1.2.2: 单同态、满同态、同构

假设有环同态 $\psi : R \to S$

如果 ψ 是单射，那么称它是一个单同态；

如果 ψ 是满射，那么称它是一个满同态；

如果 ψ 是双射，称它是一个同构；

同构是最严格的同态，表示两个环在结构上是完全相同的，有以下显而易见的事实：

命题 1.2.2. 如果 $\psi : R \to S$ 是一个环同构，那么 $\psi^{-1} : S \to R$ 也是一个环同构

证明: $\psi\left(\psi^{-1}(a) + \psi^{-1}(b)\right) = \psi\left(\psi(a)\right) + \psi\left(\psi(b)\right) = a + b$

因为 ψ 是双射，所以有 $\psi^{-1}(a) + \psi^{-1}(b) = \psi(a+b)$

同理，$\psi\left(\psi^{-1}(a)\psi^{-1}(b)\right) = \psi\left(\psi(a)\right)\psi\left(\psi(b)\right) = ab$

$\Rightarrow \psi^{-1}(a)\psi^{-1}(b) = \psi(ab)$，于是命题得证 □

1.2.2 同态的核、像

定义 1.2.3: 环同态的核、像

设 $\psi : R \to S$ 是一个环同态，我们定义：

$\ker\psi = \{a \in R|\psi(a) = 0_S\}$，称为 ψ 的核

$\mathrm{Im}\ \psi = \{\psi(a)|a \in R\}$，称为 ψ 的像

与域的同态不同，环的同态的核并不是平凡的，因为域同态未必是单射。因此，我们需要研究环同态的核与像。

但是，受限于目前的知识，我们暂时无法证明核与像的一些进阶性质，我们仅仅证明一些简单的性质。

命题 1.2.3. *设 $\psi : R \to S$ 是一个环同态，那么 $\ker\psi$ 是一个 R 的子环*

证明： 取 $\forall a, b \in \ker\psi$，那么有 $\psi(a) = \psi(b) = 0$

我们注意到：$\psi(0_R) = 0_S \Rightarrow 0_R \in \ker\psi, a + 0_R = a$

$\psi(a + (-a)) = 0_S \Rightarrow \psi(a) + \psi(-a) = 0_S \Rightarrow \psi(-a) = 0_S \Rightarrow -a \in \ker\psi, a + (-a) = 0_R$

加法的交换律、结合律，乘法的结合律，左、右分配律是显然成立的。 □

命题 1.2.4. *设 $\psi : R \to S$ 是一个环同态，那么 $Im\ \psi$ 是一个 S 的子环*

证明： 取 $\forall a, b \in \mathrm{Im}\ \psi$，那么有 $\exists x, y \in R, \psi(x) = a, \psi(y) = b$

我们注意到：$\psi(0_R) = 0_S \Rightarrow 0_S \in \mathrm{Im}\ \psi, \psi(x) + \psi(0_R) = \psi(x)$

$\psi(x) + \psi(-x) = \psi(x + (-x)) = \psi(0_R) = 0_S \Rightarrow \psi(-x) = -\psi(x) = -a \in \mathrm{Im}\ \psi, a + (-a) = 0_S$

加法的交换律、结合律，乘法的结合律，左、右分配律是显然成立的。 □

1.3 环的理想

1.3.1 理想的定义

定义 1.3.1: 理想

设 R 是一个环，R 是 R 的一个子环。

如果 $\forall a \in S, b \in R, ab \in S$，那么我们称 S 是 R 的一个左理想；

如果 $\forall a \in S, b \in R, ba \in S$，那么我们称 S 是 R 的一个右理想；

如果 S 既是 R 的左理想，又是 R 的右理想，那么我们称 S 是 R 的一个双理想。

显然，$\{0_R\}, R$ 都是 R 的理想，我们称之为平凡理想。

我们观察到：一些环，比如说 $\mathbb{Z}$，他们有一种特殊的理想，比如说 $\forall m \in \mathbb{Z}, m\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个理想。我们把这种直接由一个元素“生成”的理想叫主理想。

定义 1.3.2: 主理想

设 R 是一个环，如果 R 的一个理想 S 满足：

$\exists a \in R, S = aR := \{ab | b \in R\}$，那么我们称 S 是由 a 生成的主理想，记作 (a)

1.3.2 理想的性质

1.

命题 1.3.1. 设 $\psi : R \to S$ 是一个环同态，那么 $\ker \psi$ 是 S 的一个理想

证明: 取 $\forall a \in \ker \psi$，依核的定义，$\psi(a) = 0_S$

那么，$\forall b \in R, \psi(ab) = \psi(a)\psi(b) = 0_S, \psi(ba) = \psi(b)\psi(a) = 0_S$

因此，$ab, ba \in \ker \psi$，于是命题得证。 □

2.

命题 1.3.2. 设 R 是一个幺环，S 是 R 的一个双理想，如果 $1_R \in S$，那么 $S = R$

证明: 依理想的定义，$\forall b \in R, 1_R b = b 1_R = b \in S$，所以 $R \subseteq S$，所以必须有 $R = S$ □

我们可以立即得出，最特殊的幺环——域，也可以应用上述性质

推论 1.3.1: 域没有非平凡理想

域只有平凡理想

证明： 设 F 是一个域，S 是 F 的一个理想

因为域中任意元素都有逆元素，所以 $\forall a \in S, a^{-1} \in F$

而按照理想的概念，$a \cdot a^{-1} = 1_F \in S$

而按照前面的命题，$1_F \in S$，那么一定有 $S = F$，它是一个平凡理想； □

1.4 商环

1.4.1 商环的定义

我们首先定义等价类，随后定义商环

定义 1.4.1: 关于环的理想的等价类

设 R 是一个环，S 是 R 的一个理想

我们定义 $R \times R$ 上的一个等价关系：$\underset{I}{\sim}: \{(x, y) | x - y \in I\} \subseteq R \times R$

并定义 $a \in R$ 关于 $\underset{I}{\sim}$ 的等价类为：$a + I := \overline{a} := \{x \in R | x \underset{I}{\sim} a\}$

我们其实还需要验证以上关系的确是一个等价关系：

首先，$\forall a \in R, a \sim a$，因为 $a - a = 0_R \in I$，这说明自反性成立；

其次，如果 $a \sim b$，那么有 $a - b \in I$，而 I 是一个理想，所以一定有 $b - a \in I$，所以 $b \sim a$，这说明对称性成立；

最后，如果 $a \sim b, b \sim c$，那么有 $a - b \in I, b - c \in I$，而 I 是一个理想，所以一定有 $(a - b) + (b - c) = (a - c) \in I$，所以 $a \sim c$，这说明传递性成立；

定义 1.4.2: 商环

设 R 是一个环，I 是 R 的一个理想，那么我们定义：

$R/I = \{a + I | a \in R\}$，称为 R 关于 I 的商环

并定义其中的环加法和环乘法为：

$(a + I) + (b + I) = (a + b) + I, (a + I) \cdot (b + I) = (a \cdot b) + I$

事实上，由于 $a + I$ 是一个等价类，我们还需要验证，如果 $a_1 + I = a_2 + I$，即同一等价类选取不同单位元下，运算结果是一致的。

命题 1.4.1. 商环的加法和乘法是良定义的 设 R 是一个环，I 是 R 的一个理想，那么如

果 $a_1+I=a_2+I, b_1+I=b_2+I$

那么 $(a_1+I)+(b_1+I)=(a_2+I)+(b_2+I), (a_1+I)\cdot(b_1+I)=(a_2+I)\cdot(b_2+I)$

证明: 对于第一条，只需证明 $(a_1+b_1)-(a_2+b_2)\in I$。

因为 $(a_1+b_1)-(a_2+b_2)=(a_1-a_2)+(b_1-b_2)$，而 $a_1-a_2\in I, b_1-b_2\in I$，所以 $(a_1+b_1)-(a_2+b_2)\in I$

对于第二条，只需证明 $(a_1\cdot b_1)-(a_2\cdot b_2)\in I$。

因为 $(a_1\cdot b_1)-(a_2\cdot b_2)=(a_1\cdot b_1-a_1\cdot b_2)+(a_1\cdot b_2-a_2\cdot b_2)$

$=a_1(b_1-b_2)+(a_1-a_2)b_2\in I$，因为 I 是一个理想。 □

1.5 同态基本定理

1.5.1 同态基本定理

定理 1.5.1: 同态第一基本定理

设 R, S 是两个环，$\varphi: R\to S$ 是一个环同态，那么：

$R/\ker\varphi\cong \mathrm{Im}\ \varphi$

证明: 我们考虑以下映射：

$\psi: R/\ker\varphi\ni a+\ker\varphi\mapsto\varphi(a)\in\mathrm{Im}\ \varphi$

首先，$\psi((a+\ker\varphi)+(b+\ker\varphi))=\psi((a+b)+\ker\varphi)=\varphi(a+b)=\varphi(a)+\varphi(b)=\psi(a+\ker\varphi)+\psi(b+\ker\varphi)$

$\psi((a+\ker\varphi)\cdot(b+\ker\varphi))=\psi(ab+\ker\varphi)=\varphi(ab)=\varphi(a)\varphi(b)=\psi(a+\ker\varphi)\cdot\psi(b+\ker\varphi)$

这说明 ψ 是一个同态，我们接下来只需要证明双射性。

首先证明单射性，如果 $\psi(a+\ker\varphi)=\psi(b+\ker\varphi)$，即 $\varphi(a)=\varphi(b)$，那么 $\varphi(a)-\varphi(b)=\varphi(a-b)=0_R$，所以 $a-b\in\ker\varphi$，于是 $a+\ker\varphi=b+\ker\varphi$，单射性成立。

满射性是显然的，因为显然 $\forall b\in\mathrm{Im}\ \varphi, \exists a\in R, \varphi(a)=b, \psi(a+\ker\varphi)=\varphi(a)=b$

于是命题得证。 □

1.6 模

本节我们研究一种“环上的线性空间”，也就是模

1.6.1 模的定义

定义 1.6.1: 左模

设 R 是一个环，M 是一个集合，如果存在两个运算 $+: M\times M\to M, \cdot_R: R\times M\to M$ 分别称为称为加法和纯量乘法，满足下列条件：

① $\exists 0_M\in M$，称为加法单位元，$\forall\alpha\in M, 0_M+\alpha=\alpha+0_M=\alpha$

② $\forall\alpha,\beta\in M, \alpha+\beta=\beta+\alpha$

③ $\forall\alpha,\beta,\gamma\in M, (\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$

④ $\forall\alpha\in M, \exists-\alpha\in M$，称为加法逆，使得 $\alpha+(-\alpha)=0_M$

⑤ $\forall a,b\in R, \alpha\in M, a(b\alpha)=(ab)\alpha$

⑥ $\forall a\in R, \alpha,\beta\in M, a(\alpha+\beta)=a\alpha+a\beta$

⑦ $\forall a,b\in R, \alpha\in M, (a+b)\alpha=a\alpha+b\alpha$

那么我们称 M 是一个左 $R-$ 模

类似地，我们也有右模的定义：

定义 1.6.2: 右模

设 R 是一个环，M 是一个集合，如果存在两个运算 $+: M\times M\to M, \cdot_R: M\times R\to M$ 分别称为称为加法和纯量乘法，满足下列条件：

① $\exists 0_M\in M$，称为加法单位元，$\forall\alpha\in M, 0_M+\alpha=\alpha+0_M=\alpha$

② $\forall\alpha,\beta\in M, \alpha+\beta=\beta+\alpha$

③ $\forall\alpha,\beta,\gamma\in M, (\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$

④ $\forall\alpha\in M, \exists-\alpha\in M$，称为加法逆，使得 $\alpha+(-\alpha)=0_M$

⑤ $\forall a,b\in R, \alpha\in M, (\alpha a)b=\alpha(ab)$

⑥ $\forall a\in R, \alpha,\beta\in M, (\alpha+\beta)a=\alpha a+\beta b$

⑦ $\forall a,b\in R, \alpha\in M, \alpha(a+b)=\alpha a+\alpha b$

那么我们称 M 是一个右 $R-$ 模

如果 M 兼具左模和右模的特征，我们称 M 是一个双模：

定义 1.6.3: 双模

如果 M 既是左 $R-$ 模，又是右 $S-$ 模，并且满足：

$(a\alpha)b = a(\alpha b)$

那么我们称 M 是一个 $(R,S)-$ 双模

我们也知道，环不一定有乘法单位元，因此有以下定义：

定义 1.6.4: 幺模

设 R 是幺环，M 是一个 $R-$ 模

如果 $\forall \alpha \in M, 1_R \cdot \alpha = \alpha$，那么我们称 M 是一个幺模。

在后续中，除非特别做区分，我们都假定我们说的模指的是左模。

1.6.2 模的同态

定义 1.6.5: 模同态

设 M, N 是两个 $R-$ 模，如果映射 $\psi : M \to N$ 满足：

$\forall \alpha, \beta \in M, \psi(\alpha + \beta) = \psi(\alpha) + \psi(\beta)$

$\forall a \in R, \alpha \in M, \psi(a\alpha) = a\psi(\alpha)$

那么称 ψ 是一个从 M 到 N 的模同态。

1.6.3 商模

定义 1.6.6: 商模

设 M 是一个模，N 是 M 的一个子模