1 环和域

1.1 环的定义

在具有两个二元运算的集合R中，如果

①$< R, + >$是交换群；

②$< R, \cdot >$是带幺半群；（封闭性、满足结合律，有乘法单位元1_R）

③乘法对加法的左右分配律都满足；

则称$< R, +, \cdot >$为环。

1.2 一些特殊的环

1.2.1 交换环

如果对于乘法可交换，则称环R为交换环。

tips: R中的元素不一定有乘法逆元，有乘法逆元的元素称为环中的可逆元。且R中所有可逆元构成群。

【举例】n阶整数方阵$(\mathbf{Z})_n$对矩阵加法、乘法构成n阶矩阵环$<(\mathbf{Z})_n, +, \cdot>$，非交换的。

1.2.2 自同态环

$< G, + >$是交换群，$E = \{f|f : G \to G\text{是同态映射}\}$，在E上定义二元运算+和 $\cdot$，使得对于任意的$f, g \in E, x \in G$，有$(f + g)(x) = f(x) + g(x), (f \cdot g)(x) = f[g(x)]$，则E是环，且这就被称作交换群G上的自同态环。

1.2.3 模n同余类环

在$\mathbf{Z}_n$={[0],[1],...,[n-1]}上定义加法和乘法：[i]+[j]=[i+j], [i]·[j]=[i·j]（这种加法和乘法与代表元的选取无关），则$<Z_n, +, \cdot>$称为模n同余类环。

1.2.4 平凡环

$<R, +, \cdot>$中，|R|=1，则R={0_R}。

1.3 整环和域

1.3.1 零因子

若R中元素a, b都不为0，但$a \cdot b = 0$，则称a为左零因子，b为右零因子，如果一个元素既是左零因子又是右零因子，则称之为零因子。

1.3.2 整环

（1）非平凡交换环$<R, +, \cdot>$中，如果没有零因子，则称之为整环。

（2）整环中每个非零元素的加阶或是无限的，或是素数。

（3）在整环中，如果每个非零元素的加阶都是素数p，则称该整环的特征为p，如果每个非零元素的加阶都是无限，则称该整环的特征为0.

（4）在特征为p的整环中，$(a+b)^p = a^p + b^p$

1.3.3 域

（1）非平凡交换环$<R, +, \cdot>$中，如果所有非零元素构成交换群，则该环是域。

域是一种交换环$(F, +, *)$，当中加法单位元（0）不等于乘法单位元（1），且所有非零元素有乘法逆元。

（2）任意一个有限域的元素个数是一个素数q的乘方。任意一个元素个数是素数q的域都同构于$\mathbf{Z}/p\mathbf{Z} = \{0, 1, ..., p-1\}$。

（3）域是整环。

（4）有限整环是域。

【举例】$<Z,+,\cdot>$和$<Z_n,+,\cdot>$都是环，前者是整环但后者不是。

1.4 子环、环同态

1.4.1 子环

（1）环$<R, +, \cdot>$，若S是R的非空子集，如果

① <S,+>是<R,+>的子群；

② S对*运算封闭；

③ R的乘法单位元1_R属于S，

则称$<S, +, \cdot>$是$<R, +, \cdot>$的子环；

（2）子环是环；

（3）R是环，R中与R所有元素可交换的元素构成的集合是R的子环；

1.4.2 环同态

（1）R_1，R_2是环，f是R_1到R_2的映射，$1_{R_1}, 1_{R_2}$分别是R_1, R_2的乘法单位元，任意$a, b \in R_1$满足$f(a+b)=f(a)+f(b)$，$f(a \cdot b)=f(a) \cdot f(b)$，$f(1_{R_1})=1_{R_2}$，则称$f$是$R_1$到$R_2$的环同态。

（2）满环同态、单一环同态、环同构↔f为满射、单射、双射

（3）$f(0_{R_1})=0_{R_2}$；$f(-a)=-f(a)$；若a是R_1的可逆元，则$f(a)$是R_2的可逆元，且$f(a')=[f(a)]'$

（4）环同态不能保持环的全部代数结构，环同构可以保持整环和域的代数结构

（5）R是环，非空集合R'上也有运算+和·，且存在**满射** f:R→R'，使得$f(a+b)=f(a)+f(b), f(a \cdot b)=f(a) \cdot f(b)$，则<R',+,·>是环。

1.5 理想、商环

1.5.1 理想

（1）I是R的非空子集，如果任意的$x, y \in I, r \in R$，有$x-y \in I, x \cdot r \in I, r \cdot x \in I$，称I是R的一个理想。

（2）$<I,+>$是$<R,+>$的子群

（3）每个环R都有R和$\{0_R\}$这两个平凡理想，非平凡理想叫做真理想

（4）I_1，I_2都是R的理想，定义

$$I_1 \cdot I_2=\left\{\sum_{k=1}^{n} r_{1k} \cdot r_{2k} \mid r_{1k} \in I_1, r_{2k} \in I_2, 1 \leqslant k \leqslant n, n=1,2,\cdots\right\}$$

$$I_1+I_2=\{r_1+r_2 \mid r_1 \in I_1, r_2 \in I_2\}$$

他们都是R的理想。

（5）在R中，元素x,y模I同余，当且仅当$x-y \in I$。

（6）R中的模I同余关系是等价关系，元素x所在的等价类$[x]=\{y|y \in R，x-y \in I\}=\{x+i|x \in I\}=x+I$。

1.5.2 商环

（1）I是R的理想，$R/I=\{x+I|x \in R\}$关于理想加法、理想乘法构成环，称为R模I的商环。

零元：0_R+I；负元：（−x）+ I；单位元：1_R+I

（2）如果R的理想I中有R的可逆元，该理想必是平凡理想

（3）域F只有$\{0_F\}$和F两个理想，没有真理想

1.5.3 主理想

（1）R是交换环，R中元素a生成的理想$(a) = \{a \cdot r | r \in R\}$叫做主理想

（2）交换环R的子集$S = \{r_1, \ldots, r_k\} \subseteq R$，则$(r_1, r_2, \ldots, r_k) = \{r_1 \cdot t_1 + \ldots + r_k \cdot t_k | t_i \in R\}$是R的理想，是S生成的理想

（3）如果R的所有理想都是主理想，称R是主理想环。

（4）$<\mathbf{Z},+,\cdot>$是主理想环

1.6 多项式

1.6.1 环上的多项式

（1）环上的多项式定义为$P(x) = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n, a_n \neq 0_R, n \geq 0$

（2）环上的所有多项式记为$R[x]$，$< R[x], +, \cdot >$是整环

1.6.2 域上的多项式

（1）域上的多项式可以做带余除法，其商和余式是唯一确定的

（2）$F[x]$是主理想环

1.6.3 域上的多项式商环

（1）F[x]的理想都是$P = (P(x))$的形式

（2）$F[x]/P = \{f(x) + P | f(x) \in F[x]\} = \{b_0 + b_1 x + \ldots + b_{n-1} x^{n-1} + P|, b_i \in F\}$

【举例】写出$Z_2[x]/(x^2+x+1)$的加法表和乘法表

1.7 环同态定理

（1）ϕ是R_1到R_2的同态映射，0_{R_2}是R_2的零元，Ker φ＝$\{r | r \in R_1$，$\varphi(r)=0_{R_2}\}$，称为φ的同态核

（2）Ker φ是R_2的理想

（3）R_1的任意商环都是R_1的同态像，若φ是R_1到R_2的满同态映射，则$R_1/\text{Ker}\ \varphi \cong R_2$

（4）φ是R_1到R_2的同态映射，则

① S_1是R_1的子环，则$\varphi(S_1)$是R_2的子环，特别，$\varphi(R_1)$是R_2的子环

② S_1是R_1的理想，则$\varphi(S_1)$是$\varphi(R_1)$的理想

③　S_2是$\varphi(R_1)$的子环，则$\varphi^{-1}(S_2)$是R_1的子环

④　S_2是$\varphi(R_1)$的理想，则$\varphi^{-1}(S_2)$是R_1的理想，且$R_1/\phi^{-1}(S_2) \cong \phi(R_1)/S_2$

（5）I_1，I_2是R的两个理想，$I_2 \subseteq I_1$，则I_1/I_2是R/I_2的理想且$\frac{R/I_2}{I_1/I_2} \cong R/I_1$