3 环与域

3.1 环与域的定义,子环

环：R被称为一个*环(ring)*，如果R是一个非空集合，R上定义了两个二元代数运算，通常称为加法和乘法，记作$a+b$和ab，适合下列条件：
(i)R对于加法成一个交换群.
(ii) （乘法的结合律）对于R中的任意元素a,b,c，有

$$(ab)c = a(bc).$$

(iii)（乘法对加法的分配律）对于R中的任意元素a,b,c，有

$$\begin{aligned} a(b+c) &= ab+ac \\ (a+b)c &= ac+bc \end{aligned}.$$

如果环R对于乘法运算满足交换律，即$ab = ba$，则称G为*交换环(commutative ring)*.

如果环R中有元素e使得$ae = ea = a$，则称e是R的*单位元*，称R是有单位元的环（含幺环），通常把R的关于乘法运算单位元e记为**1**.（R关于加法运算的单位元是**0**）.在有单位元的环R中，对于元素a，如果有R中的元素b使得$ab = ba = 1$则称a为*可逆元(invertible element)*或*单位(unit)*，此时b称为a的逆元，记作a^{-1}，逆元是唯一的.

零因子：环R中的一个元素a称为一个*左（或右）零因子(left(right)zero divisor)*，如果R中有元素$b \neq 0$，使得$ab = 0$(或$ba = 0$).左零因子和右零因子都简称为零因子，**0**是平凡的零因子，其余的零因子是非平凡的，若R没有非平凡的零因子，则称R为*无零因子环* .

整环：有单位元$1(\neq 0)$的无零因子的交换环称为*整环(integral domain)*.

除环：如果环R的所有非零元组成的集合R^*对于乘法构成一个群，即R是有单位元的环且每个非零元都可逆，则R称为*除环(division ring)*.

域：交换的除环称为*域(field)*，即F被称为一个域，如果F是一个有单位元$1(\neq 0)$的交换环，并且它的每一个非零元都可逆.域F有两个代数运算：加法和乘法，F关于加法构成**Abel**群，F的所有非零元组成的集合F^*关于乘法也构成**Abel**群，并且适合乘法对于加法的分配律.

有理数域Q，实数域R，复数域C都是域，当**p**为素数时，模**p**的剩余类环Z_p也是一个域，称为模**p**的剩余类域.一个域中若只有有限个元素，则称它为*有限域(finite field/galois field)*.

子环：如果环R的一个非空子集R_1对于R的加法和乘法也成为一个环，则称R_1是R的一个*子环(subring)*.环R的一个非空子集R_1是子环的充要条件是：R_1对于R的减法和乘法都封闭，即$a,b \in R_1 \Rightarrow a-b, ab \in R_1$.

3.2 环的理想,商环,环的同态与同构

理想：设R是一个环，I是R的一个非空子集.如果I对于减法封闭，即$a \in I, b \in I \Rightarrow a - b \in I$.且$I$具有“吸收性”，即$a \in I, r \in R \Rightarrow ar \in I, ra \in I$.则称$I$为$R$的一个*理想(ideal)*或者*双边理想*.如果I对于减法封闭，并且具有“左(或右)吸收性”，即$a \in I, r \in R \Rightarrow ar \in I$(或$ra \in I$)则称$I$为$R$的一个*左(或右)理想(left(right)ideal)*.

由于理想对减法封闭，所以I是R的加法群的子群.理想是从代数几何中代数簇的研究里抽象得到的代数结构.

单环：显然**0**和R是环R的理想，称为平凡的理想，如果环R只有平凡的理想，则称R为*单环(simple ring)*.

在整数环Z中，一个整数**m**的所有倍数组成的集合mZ是Z的一个理想.在域F的一元多项式环$F[x]$中，一个多项式$f(x)$的所有倍式组成的集合是$F[x]$的一个理想.一般地，设R是一个含幺交换环，$a \in R$，把集合$\{ra|r \in R\}$记作Ra，容易看出Ra是R的一个理想，一列理想I_j的交集$\cap I_j$也是一个理想.

生成的理想和主理想：设S是环R的一个非空子集，环R的包含S的所有理想的交称为*由S生成的理想(ideal generated by S)*，记作(S)，如果$S = \{a_1, a_2, \cdots, a_n\}$，则称$(S)$是*有限生成的*，并把$(S)$记作$(a_1, a_2, \cdots, a_n)$.由一个元素$a$生成的理想称作*主理想(principal ideal)*，记作(a).

R是有单位元的交换环，则Ra是由一个元素a生成的理想，因此Ra是主理想，Ra可以记作(a)，特别地，在整数环Z中mZ是主理想，可记作(m).

理想的和与积：若A, B是R的两个非空子集，易验证，如果I, J都是R的理想，则$I + J, IJ$也是R的理想，且有$IJ \subseteq I \cap J \subseteq I + J$.(其中$A + B = \{a + b|a \in A, b \in B\}$，$AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n|a_i \in A, b_i \in B\}$)

理想的互素：在整数环Z中，m, n是整数，$(m, n) = 1$时$(m) + (n) = (1) = Z$，由此抽象出互素的概念：R是有单位元的环，I, J是R的理想，如果$I + J = R$，则称I与J*互素(coprime)*.

互素的性质：
(1)设R是由单位元的交换环，I, J是R的理想，I与J互素，则$IJ = I \cap J$.
(2)设R是由单位元的交换环，I, J, K是R的理想，如果I和J都与K互素，则IJ与K互素.

商环：设R是一个环，I是R的一个理想，则I是R的加法群的子群.由于R的加法群是一个**Abel**群，因此I是正规子群，从而有商群R/I，它的元素是陪集$r + I$，定义$(r_1 + I)(r_2 + I) = (r_1r_2 + I)$，可以验证这个乘法是定义良好的，且满足结合律和左右分配律，因此R/I是一个环，称为R对于I的*商环(quotient ring)*，商环R/I中的元素$r + I$称为模I的*剩余类(residue class)*.

商环的性质：
(1)如果环R有单位元**1**，则商环R/I有单位元**1+I**.
(2)如果环R是交换环，则商环R/I也是交换环.

环的同态：设R和R'是两个环，如果存在R到R'的一个映射σ，使得对于R中任意两个元素a, b，满足$\sigma(a + b) = \sigma(a) + \sigma(b)$,$\sigma(ab) = \sigma(a)\sigma(b)$.则称$\sigma$是$R$到$R'$的一个*同态映射*，简称为*同态(homomorphism)*.(若环R, R'有单位元$1, 1'$，还要求$\sigma(1) = 1'$).

同态的性质：
(1)σ把R的单位元e映成R'的单位元e'.
(2)对于任意$a\in R$，σ把G中a的逆元a^{-1}映成R'中$\sigma(a)$的逆元$\sigma(a)^{-1}$，即$\sigma(a^{-1})$=$\sigma(a)^{-1}$.
(3)R的加法子群H在σ下的像$\sigma(H)$是R'的加法子群.
(4)R在σ下的像$Im\sigma$是R'的子群，称$Im\sigma$为同态σ的像***(image)***.$Im\sigma$不仅是R'的加法群的子群，而且是环R'的一个子环.

同态的核：设σ是环R到环R'的一个同态，则R'的单位元e'的原像集称为σ的核***(Kernel)***，记作$Ker\sigma$，$Ker\sigma=\{a\in G|\sigma(a)=e'\}$.由定义易知$Ker\sigma$是环$R$的加法群一个子群，也是环$R$的一个理想.

单同态与满同态：设σ是环R到环R'的一个同态，如果σ是满射，则称σ是**满同态*(surjective homomorphism)***，如果σ是单射，则称σ是**单同态*(injective homomorphism)***或**嵌入*(embedding)***.σ是满同态当且仅当$Im\sigma=R'$，σ是单同态当且仅当$Ker\sigma=\{e\}$

设I是环R的一个理想，令

$$\pi : R\to R/I$$

$$r\longmapsto r+I,$$

则π是环R到商环R/I的一个满同态，保持加法和乘法运算.如果环R有单位元**1**则$\pi(1)=1+I$，且$Ker\pi=I$.称π为**自然同态*(natural homomorphism)***.商环是环R在自然同态下的像，理想I是自然同态的核$Ker\pi$.

环同态基本定理：设σ是群G到G'的一个同态，则同态像同构于商环$R/Ker\sigma$，即$R/Ker\sigma\cong Im\sigma$.

证明：由于σ也是环**R**的加法群到**R'**的加法群的一个同态，因此根据群同态基本定理得$R/Ker\sigma$与**Im**σ同构，它的一个同构映射为

$$\varphi : R/Ker\sigma\to Im\sigma$$

$$r+Ker\sigma\longmapsto\sigma(r),$$

只需证明φ保持乘法：$\varphi(r_1+Ker\sigma)(r_2+Ker\sigma)=\varphi(r_1r_2+Ker\sigma)=\sigma(r_1r_2)=\sigma(r_1)\sigma(r_2)=\varphi(r_1+Ker\sigma)\varphi(r_2+Ker\sigma)$.因此$\varphi$是$R/Ker\sigma$到$Im\sigma$的一个同构映射，从而$R/Ker\sigma$与$Im\sigma$的同构.

环的同构：若同态σ是双射，则称R与R'是**同构的*(isomorphic)***，记作$R\cong R'$，σ是R到R'的一个**同构映射**，简称为**同构*(isomorphism)***.

类似于群的第一、第二同构定理，有环的第一、第二同构定理如下：

第一同构定理：设R是群，H是R的子环，I是R的理想，则**(1)**$I+H$是R的子环**(2)**$I\cap H$是H的理想，且有环同构$H/I\cap H\cong I+H/I$.

第二同构定理：设R是环，I,J都是R的理想，且$I\subseteq J$，则J/I是R/I的理想，且有环同构$(R/I)/(J/I)\cong R/J$.

环同态基本定理反映了环R的每一个同态像都同构于R对于同态核的商群，又同态核是R的理想，因此掌握了群R的所有理想，就掌握了R的所有同态像，从而可以了解环R的结构，反之亦然.这就是理想在研究环的结构中起着十分重要的作用的缘故.

3.3 素理想与极大理想,环的直和

在上一节中我们已经定义了理想的互素：R是有单位元的环，I, J是R的理想，如果$I+J=R$，则称I与J互素.这是根据Z中的互素满足$(m,n)=1$时$(m)+(n)=Z$，抽象得到的互素的概念.类似的抽象出根据整数环可以抽象出如下定义：

素理想：若R的一个理想$P \neq R$，使得对任意的$a,b \in R, ab \in P \Rightarrow a \in P$或$b \in P$，则称$P$为$R$的一个***素理想(prime ideal)***.

极大理想：若R的一个理想$M \neq R$，使得对任意的理想$I \subseteq R$，若$M \subseteq I$，则$I=M$或$I=R$，则称M为R的一个***极大理想(maximal ideal)***.

设R是一个有单位元的交换环，$P \subseteq R$是R的一个理想，则P是R的素理想当且仅当R/P是整环.

设R是一个有单位元的交换环，$M \subseteq R$是R的一个理想，则M是R的极大理想当且仅当R/M是域.(极大理想的定义是由域的性质引出，由域都是整环，可以得到极大理想一定是素理想，反之不成立，如$Z[x]/(x)$是整环但不是域，从而(x)是$Z[x]$的一个素理想，但不是极大理想.)

谱：设R是含单位元$1(\neq 0)$的交换环，则R的所有素理想组成的集合称为R的***谱(spectrum)***，简称为$SpecR$.

环的直和：设$R_1, R_2, \cdots, R_n$都是环，作$R_1, R_2, \cdots, R_n$加法群的直和$R_1 \bigoplus R_2 \bigoplus \cdots \bigoplus R_n$，定义乘法如下：$(a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) = (a_1b_1, a_2b_2, \cdots, a_nb_n)$，这个乘法满足结合律和左右分配律，因此$R_1 \bigoplus R_2 \bigoplus \cdots \bigoplus R_n$是一个环，称为$R_1, R_2, \cdots, R_n$的直和.它的零元是$(0,0,\cdots,0)$，如果每个环都有单位元$1_i$，它的单位元是$(1_1, 1_2, \cdots, 1_n)$，如果每个环都是交换环，则$R_1 \bigoplus R_2 \bigoplus \cdots \bigoplus R_n$也是交换环.

同余：设I是环R的一个理想，对于$a,b \in R$，如果$a-b \in I$，则称a,b模***I*同余*(a is congruent to b modulo I)***，记作$a = b \pmod I$.同余关系具有反身性，对称性和传递性，因此是一个等价关系.容易看出a的等价类$\bar{a}=a+I$从而R对于模I同余的商集就是商环R/I.

引理：设R是有单位元$1(\neq 0)$的环，它的理想$I_1, I_2, \cdots, I_s$两两互素，则$R/I_1 \cap I_2 \cap \cdots \cap I_s \cong R/I_1 \bigoplus R/I_2 \bigoplus \cdots \bigoplus R/I_s$.
证明：构建映射

$$\sigma : R \to R/I_1 \cap I_2 \cap \cdots \cap I_s$$

$$x \longmapsto (x+I_1, x+I_2, \cdots, x+I_s),$$

验证σ是环R到环$R/I_1 \bigoplus R/I_2 \bigoplus \cdots \bigoplus R/I_s$的一个同态，结合环同态基本定理可以得到$R/I_1 \cap I_2 \cap \cdots \cap I_s \cong Im\sigma$.由$I_s$两两互素证明$\sigma$是满射，从而原结论成立.

中国剩余定理：设**R**是有单位元$1(\neq 0)$的环，理想$I_1, I_2, \cdots, I_s$两两互素，则对于任意的**s**个元素$b_1, b_2, \cdots b_s \in R$，同余方程组$x = b_j \pmod I)_j (\forall j = 1, 2, \cdots s)$在$R$内必有解，且如果**a,c**为两个解，则$a = c \pmod{I_1 \cap I_2 \cap \cdots \cap I_s}$.(由$\sigma$是满射可以得到该同余方程组有解，由同余关系的对称性和传递性可得到解在模**I**意义下唯一)

推论：设R是有单位元$1(\neq 0)$的环，它的理想$I_1, I_2, \cdots, I_s$两两互素，且$I_1 \cap I_2 \cap \cdots \cap I_s = (0)$，
则有$R \cong R/I_1 \bigoplus R/I_2 \bigoplus \cdots \bigoplus R/I_s$.

3.4 唯一分解整环,主理想整环,Euclid整环

我们已经知道，整数环**Z**的结构：每一个正整数可以唯一地分解成有限多个素数的乘积(不考虑排列顺序)，域F上的一元多项式环$F[x]$的结构：每一个次数大于0的多项式都可以分解成有限多个不可约多项式的乘积，且在相伴意义下分解唯一.**Z**和$F[x]$都是整环，自然地，将这个结论抽象到一般的整环中.

因子与倍元：设R是一个整环，对于任意取定的$a,b\in R$，如果存在$c\in R$，使得$a=bc$，则称b整除a，记作$b|a$，此时称b是a的*因子(factor/divisor)*，a是b的*倍元(multiple)*.整除关系具有反身性和传递性，没有对称性但有相伴性见下文.

u是R的单位(即可逆元)当且仅当$u|1$，即$(u)=R$，R单位u是R的每一个元素a的因子，因为$a=u(u^{-1}a)$.

相伴：$b|a\Leftrightarrow(b)\supseteq(a)$，如果$b|a,a|b$则称$a$与$b$*相伴(associate)*，记作$a\sim b$，相伴是一个等价关系.$a\sim b\Leftrightarrow(a)=(b)\Leftrightarrow R$的单位$u$使得$a=bu$.

真因子与平凡因子：如果$b|a$但$a\nmid b$(即b是a的因子但b不是a的相伴元)，则称b是a的*真因子(proper factor)*.不难看出，若u是单位则u没有真因子.对R中的给定元素a，R的所有单位和a的任一相伴元都称为a的*平凡因子(trivial factor)*，a的其他因子(如果还有的话)称为a的非平凡因子.

可约：设$a\in R$，$a\neq 0$，且a不是单位，若a只有平凡因子，则称a是*不可约的(irreducible)*，否则称a是*可约的(reducible)*.

素元：设$a\in R$，$a\neq 0$，且a不是单位，如果从$a|bc$可以推出$a|b$或$a|c$，则称a是一个*素元(prime element)*

在整环R中，素元一定是不可约元，反之不成立.(如整环$Z[\sqrt{-5}]$中3和$2\pm\sqrt{-5}$都是不可约元，但都不是素元)

在整环R中，a为素元当且仅当(a)为非零素理想.由此可以得到如果元素a生成的理想(a)为非零极大理想，则a为素元，进而a为不可约元.

最大公因子：设$a,b\in R$，如果存在$c\in R$，使得$c|a,c|b$，则称c是a和b的*公因子(common divisor)*.a,b的一个公因子d被称为*最大公因子(greatest common divisor)*，如果$c|a,c|b$可以推出$c|d$，d也记作$gcd(a,b)$.

引理：在整环R中，如果每一对元素都有最大公因子，则对任意$a,b,c\in R$，有$(ca,cb)\sim c(a,b)$.

唯一分解整环：整环R满足下列两个条件,：
(1)R中的每一个非零且非单位的元素a可以分解成有限多个不可约元的乘积:$a=p_1p_2\cdots p_s$;
(2)上述分解在相伴意义下是唯一的，即如果a有两个分解式$a=p_1p_2\cdots p_s=q_1q_2\cdots q_l$，则$t=s$，并且可以将$q_j$的下标适当改写可使得$p_i\sim q_i,i=1,2,\cdots s$.
则称R是一个*唯一因子分解整环(unique factorization domain)*或*Gauss整环(Gauss domain)*

下面探讨怎样的整环是唯一分解整环，首先研究唯一分解整环的性质.

唯一分解整环的性质：
(1)设R是唯一因子分解整环，则
(1)R的每一对元素都有最大公因子;
(2)R的每一个不可约元都是素元;
(3)因子链条件***(divisor chain condition)***成立，即如果$a_1, a_2, a_3, \cdots$中，每一个a_i都是a_{i-1}的真因子，则这个序列是有限序列.

唯一因子分解整环的判定：整环R如果满足下列两个条件，则R是唯一因子分解整环：
(1)因子链条件;
(2)每一个不可约都是素元.(可换为"每一对元素都有最大公因子".因为由**(2)**可以推出R的每一个不可约元都是素元)

主理想整环：整数环**Z**和一元多项式环$F[x]$的每一个理想都是主理想，由此抽象出主理想整环的概念.一个整环R称为***主理想整环(principal ideal domain)***，如果R的每个理想都是主理想，记作PID.

主理想整环的性质：
(1)主理想整环中不可约元**p**生成的理想(**p**)一定是极大理想.则R是唯一因子分解整环.
(2)主理想整环一定是唯一因子分解整环.

Euclid整环：整数环**Z**和一元多项式环**F[x]**都有带余除法，由此抽象出**Euclid**整环的概念.一个整环**R**称为***Euclid整环(Euclidean domain)***，如果存在R^*到自然数集N的一个映射δ，使得对任意$a, b \in R$且$b \neq 0$，都有$h, r \in R$满足$a = hb + r, r = 0$或$r \neq 0$且$\delta(r) < \delta(b)$.

Euclid整环都是主理想整环.