环与模　Richard. E. Brochure.

基本概念：

(定义1) 环公理 (Ring axioms.)

集合 R 与运算 $\cdot, \times : R\times R \to R$，若满足以下公理则称为环 (Ring)

(1) R 对 $+$ 构成交换群 (Abelian grop)

(2) R 对 $\cdot$ 构成半群 (semigroup)

(3) 分配律：$(r_1+r_2)r = r_1r + r_2r$

$r(r_1+r_2) = rr_1 + rr_2$

应当将 R 的所有性质与群 G 类比. 首先，G 描述的是对称性. Cayley 定理说明了 G 是具有某结构的集合上，所有保持该结构的映射. 称为对称性 (Symetry). 对环也应定义一个作用：

(定义2) R-作用，R-模 (R-action R-module)

交换群 X 的左 R-作用 $R\times X \to X$，$r(x) \longmapsto r(x)$ 满足：

$r_1(r_2(x)) = (r_1r_2)x$，$(r_1+r_2)x = r_1x + r_2x$，$1_R(x) = x$.

也被称为左 R-模. X 并非一个任意集合，是因为难以对映射定义自然的加法.

对群 G，若要如下论述以证明 Cayley 定理.

G 在具有右 G-作用的集合 G 上的左作用，是该集合的对称性.

这里 G 在 G 上的左右作用是 G 中乘法. gx / xg. 上述元非是结合律.

类似地对环 R，有：

R 在具有右 R-模结构的交换群 R 上的左作用是对称性.

同时，可以将群的同态与环的同态进行类比.

(定义3) 理想 (ideals).

环 R 的理想 I 是 R 的子集，满足：

(1) $\forall a, b \in I$，$a+b \in I$.　　(2) $\forall a\in I, r\in R$，$ra \in I$.

正规子群是群同态的核，而理想相应地是环同态的核

元素 a 生成的理想是容易定义的，即 $\langle a\rangle := \{ar : r\in R\}$. 这显然是包含 a 的最小理想，称为 a 的主理想 (Principle ideal)

唯一分解性 (Unique factorization).

整数 $\mathbb{Z}$ 对 $+$ 与 $\cdot$ 构成环. 在 $\mathbb{Z}$ 中, 重要的数论性质是, 每个 $x\in\mathbb{Z}$ 都能"精确到单位"地写成素数的乘积.

(定义1) 整环 (Integer domain)

称 R 为整环, 若 R 为有单位元的, 无零因子 (zero divisers), 交换环.

即不存在 $a,b\neq 0$, 而 $ab=0$.

记环 R 中可逆元素的集合为 $R^\times$. "精确到单位"是因为可以在乘积表达式中无限加入 $R^\times$ 中元素对.

定义等价关系 $a\sim b$: $\exists r\in R^\times$, $ar=b$. 下面的所有 R 中元素 a 应理解为 $R/\sim$ 中元素, $R/\sim$ 没有自然的加法结构. 因而下面将只谈及乘法.

(定义2) $p\in R$ 称为素元 (prime), 当且仅当 $p\mid ab \Leftrightarrow p\mid a$ 或 $p\mid b$

$p\in R$ 称为不可约元 (irreducable). 当且仅当 $a\mid p \Leftrightarrow a=1$ 或 p

所有的素元显然都是不可约元. 因为对素元 p 若 $a\mid p$, 则 $\exists k$, $ka=p$. 即有 $p\mid ka$, 则 $p\mid k$ 或 $p\mid a$. 前者说明 $a=1$, 后者说明 $a=p$.

前面定义了主理想, 整除可以方便地用主理想刻画: $a\mid b \Leftrightarrow \langle b\rangle \subseteq \langle a\rangle$

若一个环的所有理想都是主理想, 则称为主理想环 (Principle ideal domain, PID)

(命题3) 在主理想环上, 不可约元都是素元.

证: 在PID中, 若 p 不可约, 则不存在理想 $\langle p\rangle \subset I$, 且 $p\in I$.

若 $p\mid ab$, 但 $p\nmid a$ 且 $p\nmid b$, 则说明 $p\in(ab)$ 但 $p\notin(a)$, $p\notin(b)$ 故存在 a_{r_1}, b_{r_2} 使得 $p=a_{r_1}b_{r_2}$. 这导致 $p\in\langle a_{r_1}\rangle$. 只能有 $a_{r_1}=1$ 或 $a_{r_1}=p$, 都导致矛盾.

(定理4) 主理想环都是唯一分解环.

证: 存在性: 若 a_0 不可分, 存在无穷的递降链 $\{a_k\}_{k\geq 0}\in R$, $a_{k+1}\mid a_k$, 且 $\frac{a_k}{a_{k+1}}\neq 1$.

考虑理想 $I_k=\langle a_k\rangle$, $I_k\subset I_{k+1}$. 则 $\bigcup_{k=0}^{\infty} I_k$ 也是理想. 由PID性质, 它是由某元素 b 生成的理想. $b\in\bigcup_{k=0}^{\infty} I_k$, 知 $\exists N$, 使 $b\in I_N$. 于是有 $\bigcup_{k=0}^{\infty} I_k\subset I_N$, 矛盾. (一个主理想环, 不能有无限上升理想链).

唯一性：若 $a = a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_m$，利用(命题3)，$a_1$ 为素元，

知必有 b_k，使 $a_1 | b_k$. 由 b_k 不可约性知 $a_1 = b_k$.

$a_2, a_3 \cdots$ 同理.

一般而言，在 $F[X]$ 环或 $\mathbb{Z}$ 上，唯一分解性的证明方式是带余除法. 这是一个更强的要求：