抽象代数-环论 整理

环，子环

1. 环的特征、环元素的左逆和右逆

- 环R是零环当且仅当$0_R = 1_R$，意思是恒等元等于零元.
- 可在环R中定义“整数”，也就是映射$f:\mathbb{Z}\to R$，$n\mapsto n_R$，其中n_R定义为$\underbrace{1_R+\cdots+1_R}_{n个}$（$n\geq 1$），$(-n)_R$定义为$\underbrace{(-1)_R+\cdots+(-1)_R}_{n个}(n\geq 1)$.

  $\mathrm{char}R$: 若$(R,+)$中$\mathrm{ord}_{(R,+)}(1_R)=0$，则定义$\mathrm{char}R=\infty$，其他情况定义$\mathrm{char}R=\mathrm{ord}_{(R,+)}(1_R)$.（即：$\mathrm{char}(R)$用于描述$1_R$作为加法群元素的阶数）

  $\mathrm{char}R$是$(R,+)$中元素阶的上界（且有整除关系）（只需验证$na=0_R\Leftrightarrow n|\mathrm{char}(R)$.）

  $\mathrm{char}R=n$，则$\forall k,l\in\mathbb{Z}$，$k_R=l_R$当且仅当$n\mid(k-l)$；$\forall k\in\mathbb{Z}$，$k_R=0_R$当且仅当$n\mid k$.

  【remark】事实上这暗示了任何环R里都有一个子环$\mathbb{Z}/n\mathbb{Z}$或者是$\mathbb{Z}$（同构意义下），且以后会发现这是1_R生成的子环从而是R的最小子环（因为环必须要包含恒等元）

  【关于特征的一个例题】R是非零交换环且$a^2=a$对任何环中元素都成立，则环R的特征为2.
- 左逆、右逆
  - 若既有左逆，也有右逆，则左逆、右逆均唯一，且左逆=右逆. 此时称该环元素可逆.称环中的乘法可逆元为环的单位. 环的全体单位在环乘法下构成乘法群，称为环的单位群.

- 若为交换环，则： 有单边逆⇒可逆.
- 有左逆无右逆的**例子**：F上无限维线性空间V上的全体线性变换$\mathrm{End}_F(V)$. 考虑φ，φ将基向量e_1送到e_2，e_2送到e_3，e_3送到e_4，$\cdots$，则，显然φ有无限多个左逆. 因此φ没有右逆，否则，φ就既有左逆也有右逆从而可逆了，可逆时逆唯一，这与有无限多个左逆矛盾.
- 这不是偶然，而是必然成立，一般地，若$a \in R$有左逆，则以下等价：
  - a没有右逆
  - a不可逆
  - a是右零因子
  - a有至少2个左逆
  - a有无限多个左逆

  证明：①⇒②由以上事实显然，②⇒③，设a的左逆为u，则$ua = 1$，考虑$1 - au \neq 0$，则$(1-au)a = a - a(ua) = a - a = 0$，又因为$1 - au \neq 0$，所以$a \neq 0$，所以$a$是零因子.

  ③⇒ ④，注意到：若u是一个左逆，则$u + 1 - au \neq u$也会是一个左逆. 具体直接代入验证即可.

  ④⇒ ⑤，这是真正**困难**的问题，假设只有n个不同的左逆元$(n \geq 2)$，所以可对$i \neq k$考虑$x_k + 1 - ax_i$，则这也是左逆，此时$x_k, \cdots, x_k + 1 - ax_n$为均为左逆. 但是已经假设了只有$n$个不同左逆，所以以上必有重复. 分两种情况：

  ①$x_k = x_k + 1 - ax_i$，则此时$1 - ax_i = 0$，所以a既有左逆又有右逆，这与有2个左逆矛盾.

  ②存在$x_j \neq x_i$，使得$x_k + 1 - ax_i = x_k + 1 - ax_j$，则此时$ax_i = ax_j$，同时左乘以（例如）$x_i$可得$x_i = x_j$，这与$x_i \neq x_j$矛盾.

  （这一过程称为Kaplansky定理）

  ⑤⇒ ①，反证法，如果有右逆则此时a是单位，这与有无限多个右逆矛盾.

2. 一些重要概念

- 单位群，$R^\times$. 例如$\mathbb{Z}^\times = \{\pm 1\}$，$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{m} \in \mathbb{Z}/n\mathbb{Z}, (m,n) = 1\}$.

  $\mathrm{End}_F(V)^\times = \mathrm{GL}_F(V)$.
- 除环. 若R中非零元均可逆，也就是$R^\times$的底集就是$R/\{0\}$，则称环R是除环.
- 交换除环称为域.
- 最经典的不是除环，但是是域的例子：Hamilton's quaternion algebra

  $\mathbb{H} = \{a + bi + cj + dk, a, b, c, d \in R\}$，其上的加法为四维实线性空间的加法，乘法按照一些给定的公式来计算.

  这是一个除环，因为$\forall q \in \mathbb{H} - \{0\}$，$q^{-1} = \frac{q^*}{|q|}$，其中$q^*$类似于复共轭，$||$类似于复数模.

  （*）四元数的表示：①标量-矢量表示：$(a, \boldsymbol{u}) \cdot (b, \boldsymbol{v}) = ab - \boldsymbol{u} \cdot \boldsymbol{v} + (a\boldsymbol{u} + b\boldsymbol{v} + \boldsymbol{u} \times \boldsymbol{v})$

  ②矩阵表示. 嵌入$M_2(\mathbb{C})$.

  $$I_2, \quad \mathbf{I} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{J} = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}, \quad \mathbf{K} = \begin{pmatrix} & i \\ i & \end{pmatrix}.$$

  $q \in \mathbb{H}$满足$q^2 = -1 \Leftrightarrow a = 0, b^2 + c^2 + d^2 = 1$.（用四元数的矩阵表示很容易计算）
- 整环：没有非平凡的零因子的环称为整环. 即在整环R中，$ab = 0$给出$a = 0$或$b = 0$.

  交换整环称为整区.

  除环必然是整环，域必然是整区.

  【经典例子】$\mathbb{Z}/n\mathbb{Z}$是整区当且仅当n是素数，事实上这时候是域（有限整区必为域），在域论中叫做p元域，是有限域中最重要的一个例子.
- 有限整环必然是除环，有限除环必然为域（即必然交换），所以有限整环必然是域.（Wedderburn's little theorem）

- Gauss整数环$\mathbb{Z}[i]$是$\mathbb{C}$的子环. 还有类似的子环如$\mathbb{Z}[\sqrt{-5}]$和$\mathbb{Z}[\sqrt{2}]$.

  【注意】$\mathbb{Z}[i]^\times=\{1,-1,i,-i\}\cong C_4$.

  事实上$\mathbb{Z}[i]$是$\mathbb{C}$中由i生成的子环.（$\mathbb{Z}[i]$中元素均为i的整系数多项式，反之任何i的整系数多项式都是$\mathbb{Z}[i]$中元素）
- $R[x]$是一个环，R是$R[x]$的子环.
  - 事实：$R[x]$是交换环、整环、整区当且仅当R是交换环、整环、整区.
- $R[x]^\times=R$中的单位对应的零次多项式（即$R^\times$作为常数多项式）.
- $M_n(R)$是环. $M_n(R)^\times$是那些行列式等于$R^\times$中元素的矩阵.
- 子环的概念. 就是加法子群+子含幺半群.
- R的最小子环是$S=\langle 1_R\rangle$. 这个环，事实上与$\mathbb{Z}$或$\mathbb{Z}/n\mathbb{Z}$同构（作为环），其中n是R的特征
- $\mathbb{Z}$的最小子环是$\mathbb{Z}$，特别地，$\mathbb{Z}$的唯一子环是$\mathbb{Z}$
- $S=\{a+bq:a,b\in\mathbb{R}\}\subset\mathbb{H}$，其中$q^2=-1$是$\mathbb{H}$的子环，$S\cong\mathbb{C}$作为环.
- 任何多个子环的交仍是子环.
- 【子环（外显定义）】X是R的子集，称S是由X生成的子环，如果S是包含X的最小子环，也有显示的表达式：

$$S=\{f(a_1,\cdots,a_n):f\in\mathbb{Z}[x_1,\cdots,x_n],n\geq 0,a_i\in X\}.$$

根据这个外显的定义可以看出，$\mathbb{C}$中由i生成的子环就是$\mathbb{Z}[i]$.

理想，商环

1. 基本概念

- 称I是R的理想，如果I是R的加法子群，而且I对乘法满足左右吸收律.
- 商环，如果I是R的理想，则加法商群R/I在自然的乘法下具有环结构.
- 平凡理想：R总是R的理想，$\{0\}$也总是R的理想，这两个理想是平凡理想.
- 【命题】若I是R的理想且I含有R中的单位元（更一般地，含有R中的单边可逆元），则$I=$整个R.

  这是因为一旦有单边逆，则I将恒等元1_R吸进来，1_R又将整个R吸进来.

  特别地：
  - 若加法子群S既是子环也是理想，则$S=R$
  - 若理想I含有恒等元，则$I=R$
  - 除环只有平凡理想，特别地，域只有平凡理想
  - 【注！】只有平凡理想的环未必是除环，例如$M_n(R)$，我们在作业中证明了$M_n(R)$的理想和R的理想是一个一一对应，特别地，若D是除环，则$M_n(D)$也只有平凡理想，但是当$n\geq 2$时$M_n(D)$必然不再是除环.
  - 但是，有如下命题：
- 【命题】只有平凡理想的非零交换环一定是域，非零交换环是域当且仅当只有平凡理想.

  【证明】设非零交换环R只有平凡理想，只需证明R的所有非零元都可逆. 考虑$a\in R$，$a\neq 0$，考虑a生成的主理想(a)，因为R只有平凡理想且(a)包含非零元素a，从而$(a)=R$，所以存在$x\in R$使得$ax=1$，所以a可逆，所以R是域.
- 【命题】商环的子环和理想.

  R/I的子环，一一对应于R中含I的子环

  R/I的理想，一一对应于R中含I的理想

  【remark】用环同态理解：此处的一一对应对应着商同态的像或商同态的拉回.
- 【例子】高斯整数环$\mathbb{Z}[i]$可以实现为$\mathbb{Z}[x]/(x^2+1)$，所以$\mathbb{Z}[x]$中含有x^2+1的理想一一对应于高斯整数环$\mathbb{Z}[i]$的理想. 因为$\mathbb{Z}[i]$是ED（Euclidean Domain），所以是PID，所以其所有理想都是主理想，因此具有$(a+bi)$的形式，$a,b\in\mathbb{Z}$. 因此，$\mathbb{Z}[x]/(x^2+1)$的理想是$(a+bi)$的商同态拉回. $(a+bi)=(a+b\overline{x})$，商同态拉回后为$(a+bx,x^2+1)$.
- 【例子】$\mathbb{Z}$的理想：$\mathbb{Z}$的加法子群只有$n\mathbb{Z}$，这些都是理想（容易验证），所以这是$\mathbb{Z}$的全部理想.

$\mathbb{Z}/n\mathbb{Z}$的加法子群只有$d\mathbb{Z}/n\mathbb{Z}$，其中d是n的因子. 这些也都是理想，所以这就是$\mathbb{Z}/n\mathbb{Z}$的全部理想.

2. 理想的运算

- 【重要】理想的运算. 设R是环，I, J是R的理想.
  - **交**. 任意多个理想的交仍然是理想. 例如考虑整数环$\mathbb{Z}$，则$\bigcup_{i=1}^{k} m_i\mathbb{Z} = \mathrm{lcm}(m_1, \cdots, m_k)\mathbb{Z}$，仍然是理想.
  - **和**. 任意多个理想的和仍是理想. 例如$\mathbb{Z}$的理想，$\sum_{i=1}^{k} m_i\mathbb{Z} = \gcd(m_1, \cdots, m_k)\mathbb{Z}$，仍然是理想.

    （这里的等式用bezout引理即可得到）
  - **积**. 任意多个理想的积仍是理想. 在此之前先讨论什么是理想的积.

    $$IJ = \{\sum_{i=1}^{n} x_i y_i : x_i \in I, y_i \in J, n \geq 0\}.$$

    如果不补充有限和，那么这将不是加法子群从而不是理想.

    立刻可以验证有结合律，同时理想还具有加乘分配率：

    $$I(JK) = (IJ)K, \quad I(J+K) = IJ + IK, \quad (I+J)K = IK + JK.$$

    $\prod_{i=1}^{k} m_i\mathbb{Z} = (m_1 \cdots m_k)\mathbb{Z}$.

    观察，是不是总是有$IJ \subset I \cap J$？答案是肯定的.（看定义，然后由吸收律显然）
  - **互素**：称I, J互素，如果$I + J = R$.
    - 若理想I和理想$J_1, \cdots, J_k$都互素，则I和$J_1 \cdots J_k$互素.
    - 若R是交换环，$I_1, \cdots, I_n$两两互素，则它们的积与交一样：$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.
- 由子集X生成的理想：含R的子集X的最小理想. 也有外延定义：

  $$(X) = \{\sum_{i=1}^{n} r_i x_i s_i : r_i, s_i \in \mathbb{R}, x_i \in X, n \geq 0\}.$$

  $$(x) = \{\sum_{i=1}^{n} r_i x s_i : r_i, s_i \in \mathbb{R}, n \geq 0\}.$$

  比较复杂.
- 通常在交换环中考虑由子集生成的理想.

  $$(x) = Rx (x\text{的}R\text{“倍数”}), \quad (x_1, \cdots, x_n) = Rx_1 + \cdots + Rx_n.$$

  称一个元素生成的理想为**主理想**.
- 【命题】若R是交换环，则$a \in R^\times$当且仅当$(a) = R$. 这一事实与后面讨论UFD时的事实“主理想与相伴类一一对应”有关.
- 【例子】用主理想表示两个平凡理想：(0_R)和(1_R).
- 【例子】域F上一元多项式环：$F[x]$
  - 断言：域F上一元多项式环的理想都是主理想. 设I是$F[x]$的理想，则存在$F[x]$中次数最低的首1多项式$f(x)$，对$F[x]$中的任何元素$g(x)$，存在唯一的$q(x) \in F[x]$使得$g(x) = q(x)f(x) + r(x)$，其中$\deg r < \deg f$. 因为f是$F[x]$中次数最低的首1多项式，所以$r = 0$，所以$g(x) = q(x)f(x)$，所以 $I = F[x]f(x) = (f(x))$.
  - 关于域上的一元多项式环，有以下常用引理，在此复习：
    - $f, g \in F[x]$，则$\deg(fg) = \deg f + \deg g$. 由此可知$F[x]$是整区，从而$F[x]$有分式域，一般记为$\mathrm{Frac}(F[x]) := F(x)$，该域通常称为$F$上的有理函数域.
    - 给定$F[x]$中的两个多项式f, g，其中$g \neq 0$，则存在$q(x), r(x) \in F[x]$，使得$\deg r < \deg g$且 $f(x) = q(x)g(x) + r(x)$.
- 【重要的计算公式】交换环中理想的运算（只要考虑整数的情形就不难想明白）：

$$(x)=0\Leftrightarrow x=0,\quad (x)=R\Leftrightarrow x\in R^{\times},$$
$$(x)(y)=(xy),\quad (x_1,\cdots,x_n)(y_1,\cdots,y_n)=(x_iy_j)_{1\le i\le n,1\le j,n},$$
$$(x_1,\cdots,x_n)+(y_1,\cdots,y_n)=(x_1,\cdots,x_n,y_1,\cdots,y_n).$$

- 【一个例子】$\mathbb{Z}[\sqrt{-5}]$的数论.

  $\mathcal{P}=(2,1+\sqrt{-5})=(2,1-\sqrt{-5})$.

  $q_1=(3,1+\sqrt{-5})$，$q_2=(3,1-\sqrt{-5})$.

  可以验证这些不是主理想.（取范数可注意到事实：$2,3,1\pm\sqrt{-5}$均不能写成两个非单位元的乘积），所以在当时称为ideal number

  研究它需要用到一个函数N，特别是它的乘性，由此可知$\mathbb{Z}[\sqrt{-5}]$的单位元只有±1，等等.

环同态

1. 基本概念

- 环同态的定义：保加，保乘，保恒等元.（是加法群同态且是含幺半群同态）

  【remark】保恒等元不能去掉. 由保乘法并不能直接推出$f(1_R)=1_S$，例如，假设$f(a)=0_R$ for all $a\in R$，则显然也满足保乘，但是并不保恒等元.

- 嵌入同态：S是R的子环，$i:S\to R$，$a\mapsto a$是一个单同态.
- 商同态：I是R的理想，$\pi:R\mapsto R/i,a\mapsto \overline{a}$是一个满同态.
- 【定理】环同态基本定理. $f:R\to S$是环同态. 定义$\ker f=\{x\in R:f(x)=0_S\}=f^{-1}(0_S)$（与$f$作为加法群同态的核的底集相同）
  - $\ker f$不仅是R的加法子群，还是R的理想.
  - $\mathrm{Im}f$是R的子环.
  - 同态基本定理：f诱导环同构$\overline{f}:R/\ker f\to \mathrm{Im}f$，$\overline{x}\mapsto f(x)$. 即$R/\ker f\cong \mathrm{Im}f$作为环.
- $\mathrm{Hom}_{\mathrm{Grp}}(G_1,G_2)\neq\varnothing$，因为总是有平凡群同态. 但是这个结论对于环并不成立，这主要是因为环同态把恒等元映射为恒等元，但是在不同的环里面恒等元作为加法群元素的阶可能是完全不一样的. 有一些$\mathrm{Hom}_{\mathrm{Grp}}(G_1,G_2)$是只有平凡群同态的，而平凡群同态通常都不可能还是环同态.例如：

  如果要考虑$\mathbb{Z}/2\mathbb{Z}$到$\mathbb{Z}/3\mathbb{Z}$是否有环同态，则先考虑是否有加法群同态，即$\mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/3\mathbb{Z})$.

  假设存在f是环同态，因为$f(\overline{0})=\overline{0}$，但是$f(\overline{0})=f(\overline{1}+\overline{1})=f(\overline{1})+f(\overline{1})=\overline{0}$，所以$\mathrm{ord}_{(\mathbb{Z}/3\mathbb{Z},+)}(f(\overline{1}))\mid 2$，所以$f(\overline{1})=\overline{0}$，这与$f$是环同态矛盾.

  根据上面的推导过程可以看出f只能是平凡群同态，这就导致不可能是环同态

2. 典型的例子

- 【例】用同态基本定理证明，R中$\langle 1_R\rangle$只能是$\mathbb{Z}$或者$\mathbb{Z}/n\mathbb{Z}$.

  注意$\langle 1_R\rangle$可以实现为同态$f:\mathbb{Z}\to\mathbb{R}$，$n\mapsto n_R$的像. 而$\ker f=\begin{cases}0,\mathrm{char}R=\infty,\\ n\mathbb{Z},\mathrm{char}R=n,\end{cases}$，所以根据同态基本定理可知$\langle 1_R\rangle\cong\mathbb{Z}$或$\langle 1_R\rangle\cong\mathbb{Z}/n\mathbb{Z}$.

- 【例】域上的一元多项式环$F[x]$. 其上的**赋值同态**.

  考虑$a\in F$，以及a处的**赋值映射**$\phi:F[x]\to F,f(x)\mapsto f(a)$. 则，这是一个环同态且是满同态（这是因为$\forall c\in F,\phi(c)=c$，其中第一个$c$指的是$F[x]$中常数多项式$c$）

  而$\ker\phi=\{f(x)\in F[x]:f(a)=0\}=\{f(x)\in F[x]:(x-a)\mid f(x)\}=(x-a)F[x]=(x-a)$.

  （$x-a$生成的主理想）

  根据同态基本定理：

  $$F[x]/(x-a)\cong F,\quad \forall a\in F.$$

- 【例】$\varphi:\mathbb{R}[x]\to\mathbb{C}$，$f(x)\mapsto f(i)$.

$\mathrm{Im}\varphi = \mathbb{C}$,
$\ker\varphi = \{f(x)\in\mathbb{R}[x] : f(i)=0\} = \{f(x)\in\mathbb{R}[x] : (x-i)(x+i) \mid f(x)\} = (x^2+1)f(x) = (x^2+1)$（$x^2+1$生成的主理想）

由同态基本定理，$\mathbb{R}[x]/(x^2+1)=\mathbb{C}$，这是从$\mathbb{R}[x]$造出$\mathbb{C}$的方法.

- 【例】一般情况：$F[x]/(f(x))$. $f(x)=a_0+a_1x+\cdots+a_nx^n, n\geq 1, a_n\neq 0$.

  $\forall g(x)\in F[x]$，用$f(x)$除$g(x)$，则$\exists! q(x)$使得$g(x)=f(x)q(x)+r(x)$，所以$\overline{g(x)}=\overline{r(x)}$. 且$\deg r\leq n-1$.

  事实上：商环元素和次数小于$n-1$的余式是一一对应.

  观察 F可以看成$F[x]/(f(x))$的子环，这是因为$F\to F[x]\to F[x]/(f(x))$是一个单同态，商环中的$\overline{c}$相当于F元素嵌入.

  记$\overline{x}=\alpha$（$x\in F[x]$在商同态下的像），则商环元素$\overline{g(x)}$形如：

  $$r_0+r_1\alpha+\cdots+r_{n-1}\alpha^{n-1}$$

  其中r_i实际上是$\overline{r}_i$，但是我们已经将它看成子环F中的元素，因此将\bar 去掉了.

  而$0=\overline{0}=\overline{f(\alpha)}=a_0+a_1\alpha+\cdots+a_n\alpha^n$. 因此可以认为$F[x]/(f(x))$是在$F$上增加了一个数字$\alpha$，这个数字满足的条件是$a_0+a_1\alpha+\cdots+a_n\alpha^n=0$.

  【remark】以上是域扩张的基本想法.

  【remark】$F[x]/(f(x))$是域，当且仅当$f(x)$是$F[x]$中不可约多项式.

  $$\begin{aligned}(F[x]/(f(x)))^\times &= \{\overline{g(x)}\in F[x]/(f(x)), \exists\overline{q(x)}\in F[x]/(f(x)), \mathrm{s.t.}\overline{g(x)q(x)}=\overline{1}\}\\ &= \{\overline{g(x)}\in F[x]/(f(x)), \exists p(x),q(x)\in F[x], \mathrm{s.t.} g(x)q(x)+f(x)p(x)=1\}\\ &= \{\overline{g(x)}\in F[x]/(f(x)) : \gcd(g(x),f(x))=1\}\end{aligned}$$

  $(F[x]/f(x))^\times = F[x]/(f(x))-\{0\}$当且仅当$f(x)$是$F[x]$中不可约多项式.

  若$\gcd f\geq 2$且$f(x)$是$F[x]$中不可约多项式，则方程$f(x)=0$在F上没有根，但是在更大的域$\widetilde{F}=F[x]/(f(x))$上有根$\alpha$，其中$\alpha=\overline{x}$.

  【remark】我们得到了两个结果：$\mathbb{Z}/p\mathbb{Z}$是域当且仅当p是素数，$F[x]/(f(x))$是域当且仅当$f(x)$是不可约多项式，事实上这两个结果可以用极大理想的语言统一. 即：群同态φ的像是域$\Leftrightarrow$ φ的核是极大理想，特别地，R/I是域$\Leftrightarrow$ I是极大理想.

- 【例】$f: R\to S$是环同态，则f诱导了环同态$\widetilde{f}: R[x]\to S[x]$.

  例如$\pi: \mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$诱导了$\mathbb{Z}[x]\to\mathbb{Z}/n\mathbb{Z}[x]$ 满.

  这里$\ker\widetilde{\pi}=(n)$. 从而由同态基本定理$\mathbb{Z}[x]/(n)\cong\mathbb{Z}/n\mathbb{Z}[x]$.

3. 一些稍复杂的例子

- **命题** R是环，I,J为理想且$I\subset J$，则：

  $$R/J=(R/I)/(J/I).$$

  【证明】 $f: R/I\to R/J$，$a+I=\overline{a}\mapsto\overline{a}=a+J$.

  则$\mathrm{Im}f=R/J$，$\ker f=J/I$. 根据同态基本定理，$R/J\cong(R/I)/(J/I)$.

  【推论】$R/(I+J)\cong(R/I)/(I+J)/I$.

- 【例】计算$\mathbb{Z}[x]/(x-m,n)$.

  $\mathbb{Z}[x]/(x-m,n)=\mathbb{Z}[x]/(x-m)+(n)=(\mathbb{Z}[x]/(x-m))/((x-m)+(n))/(x-m)$.

  注意有同构：$\mathbb{Z}[x]/(x-m)\cong\mathbb{Z}$，考虑$(x-m)+(n)/(x-m)$在同构下的像，则有
  $(x-m)+(n)/(x-m)\sim n\mathbb{Z}$.

所以有$\mathbb{Z}[x]/(x-m,n)\cong\mathbb{Z}/n\mathbb{Z}$.

或者用另一个计算方向：$\mathbb{Z}[x]/(x-m)+(n)=(\mathbb{Z}[x]/(n))/(x-m)+(n))/(n)$，注意$\mathbb{Z}[x]/(n)\cong\mathbb{Z}/n\mathbb{Z}[x]$（用赋值同态的同态基本定理），再考虑$(x-m)+(n)/(n)$在该同构下的像，其像为$(x-\overline{m})$，所以有：

$\mathbb{Z}[x]/(x-m,n)\cong\mathbb{Z}/n\mathbb{Z}[x]/(x-\overline{m})\cong\mathbb{Z}/n\mathbb{Z}$.

【remark】除了分步商以外，也可直接考虑环同态$\mathbb{Z}[x]\to\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$，$f(x)\mapsto\overline{f(m)}$的同态基本定理.

- 【例】计算$\mathbb{Z}[i]/(2-i)$.

  $\mathbb{Z}[i]=\mathbb{Z}[x]/(x^2+1)$（考虑$\mathbb{Z}[x]\to\mathbb{C}\to\mathbb{Z}[i]$的赋值同态），所以
  $\mathbb{Z}[i]=\mathbb{Z}[x]/(x^2+1)/(\overline{2-x})=\mathbb{Z}[x]/(x^2+1)/\overline{(2-x)}=\mathbb{Z}[x]/(x^2+1)/(2-x)+(x^2+1)/(x^2+1)$

  上面等于$\mathbb{Z}[x]/(x^2+1)/(2-x,^2+1)/(x^2+1)\cong\mathbb{Z}[x]/(2-x)/(2-x,x^2+1)/(2-x)$，因为$\mathbb{Z}[x]/(2-x)\cong\mathbb{Z}$（赋值同态诱导的同构），而$(2-x,x^2+1)/(2-x)$在同构映射下的像为$5\mathbb{Z}$

  所以$\mathbb{Z}[i]/(2-i)\cong\mathbb{Z}/5\mathbb{Z}$作为环.

  【remark】还有一个比较初等的做法. 先忘掉乘法结构，把该群看成加法子群的商群，则有：

  $\mathbb{Z}[i]=\{a+ib:a,b\in\mathbb{Z}\}\cong\mathbb{Z}\oplus\mathbb{Z}$，此时$(2-i)$在该同构下的像为

  $$(2-i)=\{(2-i)(a+bi):a,b\in\mathbb{Z}\}=\{2a+b+(2b-a)i:a,b\in\mathbb{Z}\}=\{a\begin{pmatrix}2\\-1\end{pmatrix}+b\begin{pmatrix}1\\2\end{pmatrix}:a,b\in\mathbb{Z}\}$$

  考虑矩阵$\begin{pmatrix}2&1\\-1&2\end{pmatrix}$，其不变因子为$D_1=1$，$D_2=5$，所以$(2-i)\cong\mathbb{Z}\oplus5\mathbb{Z}$作为群，于是
  $\mathbb{Z}[i]/(2-i)\cong(\mathbb{Z}\oplus\mathbb{Z})/(\mathbb{Z}\oplus5\mathbb{Z})\cong\mathbb{Z}/5\mathbb{Z}$.

  另一方面，考虑Gauss整数环中的恒等元在同构下的像$(1,0)\in\mathbb{Z}\oplus\mathbb{Z}$，这也是5阶加法子群的生成元，所以这不仅是一群同构，还是一环同构.

- 【例】计算$\mathbb{Z}[i]/(5)$.

  $\mathbb{Z}[i]=\mathbb{Z}[x]/(x^2+1)$，$(5)$在该同构映射下的像为
  $(\overline{5})=\{\overline{5f(x)}:f(x)\in\mathbb{Z}[x]\}=\overline{(5)}=(5)+(x^2+1)/(x^2+1)$.

  更换商的顺序：

  $$\mathbb{Z}[i]/(5)\cong\mathbb{Z}[x]/(x^2+1)/((5)+(x^2+1))/(x^2+1)\cong\mathbb{Z}[x]/(5)/((x^2+1)+(5))/(5)$$

  注意$\mathbb{Z}[x]/(5)\cong\mathbb{F}_5[x]$（考虑前面系数模5的同态），于是$((x^2+1)+(5))/(5)$在该同态下的像为

  $$\overline{x^2+1}=x^2+\overline{1}=x^2-\overline{4}=(x-\overline{2})(x+\overline{2}).$$

  于是$\mathbb{Z}[i]/(5)\cong\mathbb{F}_5[x]/((x-\overline{3})(x-\overline{2}))=\mathbb{F}_5[x]/((x-\overline{3}))((x-\overline{2}))$

  因为$x-\overline{3}$和$x-\overline{2}$是$\mathbb{F}_5[x]$中互素多项式，由中国剩余定理：

  $$\mathbb{F}_5[x]/((x-\overline{3}))((x-\overline{2}))\cong\mathbb{F}_5[x]/(x-\overline{3})\times\mathbb{F}_5[x]/(x-\overline{2})\cong\mathbb{F}_5\times\mathbb{F}_5.$$

  这不是域. 事实上，$\mathbb{Z}[i]$是ED从而是PID，后面会证明，如果p是$\mathbb{Z}[i]$不可约元，则$\mathbb{Z}[i]/(p)$必然是域. 而5是模4余1的奇素数，它在Gauss整数环中是可约的.

- 【例】来自Artin的几个例子：$\mathbb{F}_5[x]/(x^2-\overline{3})$是域，因为可以证明$(x^2-\overline{3})$是$\mathbb{F}_5$上不可约多项式.

  $\mathbb{F}_{11}[x]/(x^2-\overline{3})\cong\mathbb{F}_{11}\times\mathbb{F}_{11}$，其主要原因是$x^2-\overline{3}$在$\mathbb{F}_{11}[x]$可约，所以不是域.

- 【例】 计算在$\mathbb{Z}/12\mathbb{Z}$中添加2的逆元得到的域.

  即$\mathbb{Z}/12\mathbb{Z}[x]/(2x-1)$. 此时$\mathbb{Z}/12\mathbb{Z}$可以看成是这个域的子环，将这个域中的$\overline{x}$记作$\alpha$，则$\alpha$满足$\alpha=2^{-1}$.

  我们来计算这个环. $\mathbb{Z}/12\mathbb{Z}[x]=\mathbb{Z}[x]/(12)$，$(2x-1)$作为$\mathbb{Z}/12\mathbb{Z}[x]$的理想在此同构下的像为$(\overline{2x-1})$，因为$(\overline{2x-1})=\overline{(2x-1)}=(2x-1)+(12)/(12)=(2x-1,12)/12$，所以：

  $$\mathbb{Z}/12\mathbb{Z}[x]/(2x-1)\cong(\mathbb{Z}[x]/(12))/((2x-1,12)/(12))\cong\mathbb{Z}[x]/(2x-1,12)\cong\mathbb{Z}[x]/(2x-1,3)$$
  $$\cong(\mathbb{Z}[x]/(3))/((2x-1,3)/(3))\cong\mathbb{F}_3[x]/(2x-1)=\mathbb{F}_3[x]/(x+1)\cong\mathbb{F}_3.$$

- 【例*】$\mathbb{R}\times\mathbb{R}$添加$(2,0)$的逆元.

  注意$\mathbb{R}[x]/(x^2-1)=\mathbb{R}[x]/(x-1)(x+1)\cong\mathbb{R}\times\mathbb{R}$（by 中国剩余定理）

  $(2,0)$在该同构下的像为$x+1$：

$$\begin{array}{ccc}\mathbb{R}[x]/(x^2-1)=\mathbb{R}[x]/(x-1)\times\mathbb{R}[x]/(x+1)\cong\mathbb{R}\times\mathbb{R}\\ x+1\qquad\qquad(x+1,0)\qquad\qquad(2,0)\end{array}$$

  所以，该环为：

$$\mathbb{R}[x][y]/(x^2-1)/((x+1)y-1)=\mathbb{R}[x,y]/(x^2-1)/((x+1)y-1)$$
$$=\mathbb{R}[x,y]/(x^2-1)/((x+1)y-1,x^2-1)/(x^2-1)=\mathbb{R}[x,y]/((x+1)y-1,x^2-1)\cong\mathbb{R}.$$

环的直积，中国剩余定理

1. 环的外直积和内直积

- **环的外直积**：R_1,R_2是环，在$R_1\times R_2$底集上定义加法和乘法，加法是分量相加，乘法是分量相乘，则该集合在这两种运算下是环，零元是$(0_{R_1},0_{R_2})$，恒等元是$(1_{R_1},1_{R_2})$.
- $R_1'=\{(a_1,0_{R_2}):a_1\in R_1\}$，$R_2'=\{(0_{R_1},a_2):a_2\in R_2\}$，这两个都是$R_1\times R_2$的理想.
- **幂等元**：$a\in R$，$a^2=a$，称a是幂等元.
- $e_1=(1_{R_1},0_{R_2})$，$e_2=(0_{R_1},1_{R_2})$是环$R_1\times R_2$的幂等元.
- **环的中心** $Z(R)$.
- e_1,e_2是环$R_1\times R_2$的中心元，事实上这是$R_1\times R_2$的两个**中心幂等元**.
- $R_1'=(e_1)$，$R_2'=(e_2)$.
- **环的内直积**：设R是环，I,J是环的理想，且$R=I\oplus J$作为加法子群，则以下自动成立：
  - $\exists!e\in I,f\in J$，使得$1=e+f$（这是显然的）
  - e,f是R的中心幂等元（直接验证，用唯一分解性以及$1=e+f$）
  - $ef=fe=0$（$ef,fe\in I\cap J$），更一般地，$\forall x\in I,y\in J$，$xy=yx=0$.
  - $I=(e),J=(f)$（定义验证）
  - I,J关于R的加法和乘法都是环，恒等元分别是e,f（注：这并不意味着I是R的子环！因为I和J都不含有R的恒等元）
  - 有环同构$I\times J\cong R$，$(a,b)\mapsto a+b$，我们称R是I和J的内直积. 注意，内直积关系仅仅需要满足$I\oplus J=R$作为加法子群成立即可.

【remark】虽然$R_1\to R_1\times R_2,a_1\mapsto(a_1,0)$不是环同态（因为像是$R_1'$，但是$R_1'$不是后者的子环），但是，$R_1\times R_2\to R_1$有投影环同态$\mathscr{P}_1$，且$\ker\mathscr{P}_1=R_2'$.

2. 外直积的泛性质，中国剩余定理

- **外直积的泛性质**：任取一个环S，若S到$R_1,\cdots,R_n$分别有环同态$f_1,\cdots,f_n$，则$\exists!$环同态φ：$S\to R_1\times\cdots\times R_n$，使得$f_i=\mathscr{P}_i\circ\varphi$. 更确切地，$\varphi$由公式$s\mapsto(f_1(s),\cdots,f_n(s))$给出.

  【remark】也就是说，如果有S到一堆环的同态，存在一个S到这堆环的外直积的同态，使得以上那些同态都是从这个同态中长出来的，而且这是唯一的.

- **中国剩余定理**

  R是**交换环**，$I_1,\cdots,I_n$是R的两两互素的理想，则$I_1\cdots I_n$仍然是R的理想，且有环同构：

$$R/I_1\cdots I_n\cong(R/I_1)\times\cdots\times(R/I_n).$$

【证明】

- 考虑商同态$\pi_i:R\to R/I_i$，则由外直积的泛性质可知存在唯一的一个环同态$\varphi:R\to(R/I_1)\times\cdots\times(R/I_n)$，使得其公式为$a\mapsto(\pi_1(a),\cdots,\pi_n(a))=(\overline{a},\cdots,\overline{a})$.

所以$\ker\varphi=I_1\cap I_2\cap\cdots\cap I_n=I_1I_2\cdots I_n$，因为理想互素.

- 断言φ是满射.

  两两互素$\Rightarrow I_1$与$I_2\cdots I_n$互素$\Rightarrow I_1+I_2\cdots I_n=R\Rightarrow\exists\, a_1\in I_1$，$b_1\in I_2\cdots I_n$使得$a_1+b_1=1$，所以$\pi_1(b_1)=\overline{b_1}=\overline{1}=\pi_1(1)$.

  $b_1\in I_2\cdots I_n=I_2\cap\cdots\cap I_n\Rightarrow\pi_2(b_1)=\overline{0}$，$\cdots$，$\pi_n(b_1)=\overline{0}\Rightarrow\varphi(b_1)=(\overline{1},\overline{0},\cdots,\overline{0})$.

  同理存在$b_i\in R_i$，$2\le i\le n$，使得$\varphi(b_i)=(\overline{0},\cdots,\overline{1},\cdots,\overline{0})$. 这就证明了所有的中心幂等元都有原像，因此：

  $\forall(\overline{x_1},\cdots,\overline{x_n})\in R/I_1\times\cdots\times R/I_n$，

$$\begin{aligned}&\varphi(x_1b_1+\cdots+x_nb_n)=\varphi(x_1)\varphi(b_1)+\cdots+\varphi(x_n)\varphi(b_n)\\&=(\overline{x}_1,\cdots,\overline{x}_1)(\overline{1},\overline{0},\cdots,\overline{0})+\cdots+(\overline{x}_n,\cdots,\overline{x}_n)(\overline{0},\overline{0},\cdots,\overline{1})\\&=(\overline{x}_1,\cdots,\overline{x}_n)\end{aligned}$$

这就证明了这是满射，所以由同态基本定理得到环同构.□

- 【例】$n=p_1^{e_1}\cdots p_s^{e_s}$，$\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}/p_1^{e_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_s^{e_s}\mathbb{Z}$.

  引理：$(R_1\times R_2)^\times=R_1^\times\times R_2^\times$.

  由此可以证明$(m,n)=1\Rightarrow\varphi(mn)=\varphi(m)\varphi(n)$.

  还常用在多项式中，前面也已经应用过了.

分式域

1. 分式域（泛性质）

如果不说，这部分都认为R是**整区**

- 分式域：
  - R是整区，在集合$R\times(R-\{0\})=\{(a,b):a,b\in R,b\ne0\}$定义二元关系

    $\sim$: $(a,b)\sim(c,d)\Leftrightarrow ad=bc$

    则$\sim$是一个等价关系.
  - 记$\sim$定义的等价类为$\frac{a}{b}$，记$R\times(R-\{0\})$关于$\sim$的商集为：

$$\mathcal{F}=\{\frac{a}{b}:a,b\in R,b\ne0\}.$$

    定义$\mathcal{F}$上的加法和乘法后，可以验证这是良定义的（需要用到R是整区的条件，因为计算结果中为分母相乘，整区保证了分母相乘仍$\ne0$.）

    且$\mathcal{F}$在以上两个运算下成为域，其零元为$\frac{0}{1}$，恒等元为$\frac{1}{1}$.
  - 称$\mathcal{F}$是整区R的分式域.
- 【例】$\mathrm{Frac}(\mathbb{Z}):=\mathbb{Q}$.
- **分式域的泛性质**：R是整区，F是R的分式域，则有：
  - 映射$i:R\to F$，$a\mapsto\frac{a}{1}$是单同态，所以R是F的子环.
  - 若K是域，$f:R\to K$是单同态，则存在唯一的单同态$g:F\to K$，使得$f=g\circ i$，且g的定义式为$\frac{a}{b}\mapsto f(a)f(b)^{-1}$.
  - 若$\forall k\in K$，$\exists a,b\in R$，$b\ne0$，使得$k=\frac{f(a)}{f(b)}:=f(a)f(b)^{-1}$（事实上这就是$g$的定义式，所以就是在说$g$是满同态），则$g$是同构.
- 【例】$\mathrm{Frac}(F)=F$.

  证明：用分式域的泛性质：$id:F\to F$，所以存在唯一的g是单同态$g:\mathrm{Frac}(F)\to F$，使得$id=g\circ i$. 而$\forall x\in F$，x可以被g映到，所以g是满射从而g是同构.
- 【例】$\mathbb{Z}[i]$的分式域为$\mathbb{Q}[i]$.

- 【例】某个域作为环的特征为0，则它必有一个与$\mathbb{Q}$作为环同构的子域（类似于若某个环的特征为0，则它必有一个与$\mathbb{Z}$作为环同构的子环）

  证明：考虑F的特征是0，则有同态$f:\mathbb{Z}\to F$，$n\mapsto n_F$必然是单同态，根据分式域的泛性质，存在g是单同态$\mathbb{Q}\to F$，使得$f=g\circ i$，因为g是单同态，所以$\mathbb{Q}\cong \mathrm{Im}g$，所以$F$有一个与$\mathbb{Q}$同构的子域.

2. Hilbert零点定理介绍*

- 【例 **Hilbert's weak Nullstellensatz**】

  n元多项式环$\mathbb{C}[x_1,\cdots,x_n]$的极大理想与$\mathbb{C}^n$中的$n$维向量之间存在一一对应.

  更确切地说，对任何$\mathbb{C}^n$中的向量$a=(a_1,\cdots,a_n)$，可以考虑赋值同态：

  $$\varphi_a:\mathbb{C}[x_1,\cdots,x_n]\to\mathbb{C},\quad f(x_1,\cdots,x_n)\mapsto f(a_1,\cdots,a_n).$$

  其中$\ker\varphi_a=(x_1-a_1,\cdots,x_n-a_n)$，这就是$\mathbb{C}[x_1,\cdots,x_n]$的极大理想.

  【证明】对任何$a\in\mathbb{C}^n$，φ_a是满射，所以$\ker\varphi_a$是$\mathbb{C}[x_1,\cdots,x_n]$的极大理想. 下面验证$\ker\varphi_a=(x_1-a_1,\cdots,x_n-a_n)$. 首先考虑$a=0$向量的情形，则$f(0)=0$当且仅当$f$的常数项$=0$，所以$f$中出现的每个单项式必然被$x_1,\cdots,x_n$中至少一个整除. 因此$f$可写成$x_1,\cdots,x_n$的$\mathbb{C}[x_1,\cdots,x_n]$系数线性组合，因此$\ker\varphi_0\subset(x_1,\cdots,x_n)$，另一方面，任何$x_1,\cdots,x_n$的多项式系数线性组合在0处取值必然得0，所以$\ker\varphi_0\supset(x_1,\cdots,x_n)$，综上所述$\ker\varphi_0=(x_1,\cdots,x_n)$.

  对于$a\neq0$的情形，作变量替换$x_i=y_i+a$可说明$\ker\varphi_a=(y_1,\cdots,y_n)$.

  真正困难的是证明所有$\mathbb{C}[x_1,\cdots,x_n]$的极大理想都是某个$a$对应的$\ker\varphi_a$. 将会在《交换代数》课程中证明□

UFD

1. 整区R中元素的整除，相伴，不可约元，素元

- 整区中的整除：
  - R是整区，$a,b\in R$，若存在$c\in R$，使得$a=bc$，则称b是a的因子或b整除a，记为$b\mid a$.
  - 换句话说，若$(a)\subset(b)$，则称$b\mid a$.
  - 整除关系是传递的
  - 单位元整除所有的环元素，因为单位元u生成的主理想是整个环.
- 相伴：称a,b相伴，如果$(a)=(b)$，这当且仅当存在$u\in R^\times$使得$a=ub$，当且仅当a和b互相整除.
- 相伴是一个等价关系，相伴类和主理想一一对应.

  a的相伴类是$aR^\times$，0的相伴类是单点集，1的相伴类是$R^\times$

  对应的理想分别是：$(a),(0),(1)$，后两种是平凡的情况，一般不研究.
- 不可约元：设$a\in R$，$a\neq0$，$a\neq R^\times$，从而(a)非平凡.

  若不存在b,c非单位，使得$a=bc$，则称a不可约.
- 【命题】a不可约$\Leftrightarrow$ 不存在R的主理想(b)使得$(a)\subsetneq(b)\subsetneq R$.
- 【命题】相伴两元素的可约性一样.（因为可约可以完全被其主理想刻画）
- 【例】$\mathbb{Z}$中元素不可约当且仅当是素数，$F[x]$中元素不可约当且仅当是不可约多项式.
- 【例】$\mathbb{C}[x]$中，根据代数基本定理，$\mathbb{C}[x]$中元素不可约当且仅当它是线性多项式$x-\alpha_i$所在的相伴类. $\mathbb{R}[x]$中，有两类不可约元，分别为线性多项式$x-a$和满足b^2-4c的二次多项式x^2+bx+c（所在的相伴类）.
- 【定义】素元：a非零非单位，若a满足$a|bc\Rightarrow a|b$或$a|c$，则称a是素元.
  - a素$\Leftrightarrow$($bc\in(a)\Rightarrow b\in(a)$ or $c\in(a)$.)
  - a素且$a|b_1\cdots b_n$，则$\exists b_i$，使得$a|b_i$.（对n用数学归纳法）
- 【命题】相伴两元素的素性一样.（因为素可以完全被其生成的主理想刻画）
- 【命题】整区中素元必然不可约.

2. UFD的概念，素性条件和因子链条件，最大公因子和最小公倍子

- UFD：设R是整区，若满足对任何$a\in R$且非零非单位，a都可以分解为有限个不可约元的乘积，且分解在不计次序和相伴的意义下是唯一的，则称R是一个**唯一分解整区**.
- 【例】$\mathbb{Z}$是UFD（算术基本定理），$F[x]$是UFD.
- 【例】以后会证明若R是UFD则$R[x]$是UFD，从而$R[x,y]$也是UFD（因为$R[x,y]=R[x][y]$），归纳可知$R[x_1,\cdots,x_n]$也是UFD
- 【例】环$\bigcup_{k\geq 0}\mathbb{Z}[x^{1/2k}]$不是UFD，假设$x$存在有限分解，则其必然具有某种形式，但是可以发现其中的因子都是可约的，从而与有限不可约分解的存在性矛盾.
- 【例】$\mathbb{Z}[\sqrt{-5}]$不是UFD. 虽然可以证明分解总是存在的，（要用到范数N的乘性和"单调性"）但是分解不唯一，如$6=2\times 3=(1+\sqrt{-5})(1-\sqrt{-5})$，而$2,3,1+\sqrt{-5},1-\sqrt{-5}$都不可约且不相伴（用范数$N$说明），所以这不是UFD.
- **定义（素性条件）** R是整区，其不可约元均是素元，则称整区R满足素性条件.
- 【例】$\mathbb{Z}[\sqrt{-5}]$不满足素性条件，因为2是不可约元且$2|(1+\sqrt{-5})(1-\sqrt{-5})$，但$2\nmid(1+\sqrt{-5})$，且$2\nmid(1-\sqrt{-5})$，所以$2$不是素元.
- **定义（因子链条件）** R是整区，若R**没有**无限长主理想真升链：

  $$(a_1)\subsetneq(a_2)\subsetneq\cdots\subsetneq(a_i)\subsetneq(a_{i+1})\subsetneq\cdots$$

  或，等价地，R**中主理想升链必稳定**，即若有

  $$(a_1)\subseteq(a_2)\subseteq\cdots(\text{不要求真包含})$$

  可推出$\exists n\geq 1$使得$(a_n)=(a_{n+1})=(a_{n+2})=\cdots$

  则称R适合因子链条件或R满足ACCP（Ascending Chain Condition of Principal ideals，主理想升链必稳定）

  【remark】**主理想升链必稳定**和**没有无限长主理想真升链**是同一件事的两种说法.

  【remark】ACC$\Leftrightarrow$理想升链必稳定$\Leftrightarrow$ 环中理想都有限生成.

  满足ACC条件的环称为诺特环（**Noetherian ring**）.
- **例** $\mathbb{Z}$，$F[x]$适合因子链条件.（因为在$\mathbb{Z}$中若有$(0)\subsetneq(m_1)\subsetneq(m_2)$，则$|m_1|>|m_2|$；在$F[x]$中若$(0)\subsetneq(f_1(x))\subsetneq(f_2(x))$，则$\deg f_1(x)>\deg f_2(x)$）
- **例** $\mathbb{Z}[x,x^{1/2},\cdots,x^{1/2^k},\cdots]$不适合因子链条件，因为$(x)\subsetneq(x^{1/2})\subsetneq(x^{1/4})\subsetneq\cdots$是一个无限长主理想真升链.
- **例** $\mathbb{Z}[\sqrt{-5}]$适合ACCP，因为若$(0)\subsetneq(a)\subsetneq(b)$，则$0<N(a)<N(b)$.

  【remark】$\mathbb{Z}[\sqrt{-5}]$不是UFD的原因是不可约分解存在但不唯一，环$\bigcup_{k\geq 1}\mathbb{Z}[x^{1/2^k}]$不是UFD的原因是不可约分解不存在，这提示我们素性条件可能与不可约分解唯一性有关，而ACCP条件可能与不可约分解的存在性有关.事实上有以下四个命题：
- 【命题】若整区R适合ACCP，则对于R中非零非单位元a，a可以分解为**有限个**不可约元的乘积.

  【证明】若a不可约，则不用证明，若a可约，则存在非零非单位元b,c使得$a=bc$，因此$0\subsetneq(a)\subset(b)$，注意c非单位，所以a，b不相伴，因此$0\subsetneq(a)\subsetneq(b)$. 对非零非单位$b$重复以上论证可知存在$d$非零非单位，而且$(b)\subsetneq(d)$，一直做下去就得到一条无限主理想真升链，这与ACCP条件是矛盾的.□
- 【命题】若整区R适合素性条件，$a\in R$，$a\neq 0$，$a\notin R^\times$，且有分解

  $$a=p_1p_2\cdots p_r=q_1q_2\cdots q_s.$$

  其中p_i,q_j不可约，则：

  $r=s$且存在$\sigma\in S_r$使得$p_i\sim q_{\sigma(i)}$，$1\leq i\leq r$.

【证明】研究p_1，对于p_1有：$p_1 \mid p_1 \cdots p_r = q_1 \cdots q_s$，因为$p_1$不可约，而且$R_1$满足素性条件，所以$p_1$是素元，根据素元性质的推广可知$\exists j, 1 \leq j \leq s$，使得$p_1 \mid q_j$，不妨假设$p_1 \mid q_1$，使得$q_1 = u_1 p_1$，$u_1 \in R$，$q_1$不可约，$p_1$不可约（特别地$p \notin R^\times$），所以$u_1 \in R^\times$，所以$p_1 \sim q_1$，代入前面的分解式，再用到整区的乘法消去律可得$a = p_2 \cdots p_r = u_1 q_2 \cdots q_s$. 对$p_2$做同样的论证，又得$\exists u_2 \in R^\times$，使得$a = p_3 \cdots p_r = u_1 u_2 q_3 \cdots q_s$，如果$r < s$，则到某一步时有$1 = u_1 u_2 \cdots u_r q_{r+1} \cdots q_s$，故$q_{r+1} \cdots q_s \in R^\times$，这与$q_{r+1}, \cdots, q_s$不可约矛盾，若$r > s$，则到某一步就得到$p_{s+1} \cdots p_r = u_1 \cdots u_s$，又矛盾.□

- 【命题】UFD适合因子链条件.

  【引理】（用来描述UFD的唯一分解性）R为UFD，$a \in R$，$a \neq 0$，$a \notin R^\times$，且$a = p_1 \cdots p_r$，其中p_i不可约，则：

  - a的任何因子与$F = \{p_{i1} p_{i2} \cdots p_{is} : 1 \leq i_1 < i_2 < \cdots < i_s \leq r, \quad s \geq 0\}$中的某一个元素相伴.（当$s = 0$时默认是恒等元）
  - 因此，R含有(a)的主理想只有有限个（注意上面的F是一个有限集合）

  【引理的证明】设b是a的因子，则存在$c \in R$使得$a = bc$，分情况讨论：

  ①$b \in R^\times$，则$b \sim 1$，此时取$s = 0$即可.

  ②$c \in R^\times$，则$a \sim b$，此时取$p_1 \cdots p_r = a \in F$即可.

  ③$b, c \notin R^\times$，由$a \neq 0$可知$b, c \neq 0$，对b, c作不可约分解$b = q_1 \cdots q_s$，$c = q_{s+1} \cdots q_t$，其中$q_1, \cdots q_t \notin R^\times$且非零，代入可知$a = q_1 \cdots q_t = p_1 \cdots p_r$，根据**UFD中不可约分解**的唯一性可知$t = r$而且存在$\sigma \in S_r$，使得$q_i \sim p_{\sigma(i)}$，特别地，$b = q_1 \cdots q_s \sim p_{\sigma(1)} \cdots p_{\sigma(s)} \in F$.

  【Remark】依赖于UFD分解的唯一性.

  若(b)是含(a)的主理想，则$b|a$，根据上面已经证明的，b与F中某个成员相伴，也就是b就是F中某个元素生成的主理想，注意F是有限集合，所以主理想只有有限个.

  □

  【命题的证明】反证：R是UFD，假设R不适合ACCP，则存在无限主理想真升链$0 \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$，对于非零非单位元$a_1$，$(a_i), i \geq 2$都是包含$(a_1)$的主理想且它们互不相同，因为这是无限的，所以和引理矛盾.

  □

  【命题】UFD适合素性条件.

  证明：显然.

  以上四个命题加起来可以证明定理.□

- 最大公因子和最小公倍子：R是整区，$a, b \in R$，$d, m \in R$：
  - 若$d \mid a$，$d \mid b$，且$(d' \mid a, d' \mid b \Rightarrow d' \mid d)$，则称$a$是$a, b$的最大公因子.
  - 若$a \mid m$，$b \mid m$，且$(a \mid m', b \mid m' \Rightarrow m \mid m')$，则称$m$是$a, b$的最大公因子.

【remark】若d_1, d_2都是最大公因子，则d_1, d_2相伴，因此若最大公因子存在，则它在相伴意义上唯一，将这样的相伴类记为$\gcd(a, b)$，同样lcm也有唯一性，从而$\mathrm{lcm}(a, b)$.

【警告】整区元素未必都有最大公因子，例如$\mathbb{Z}[\sqrt{-5}]$中$2(1 + \sqrt{-5})$和6没有最大公因子.

【命题】UFD中元素有gcd和lcm.（UFD满足GCD条件）

设R是UFD，$a, b \neq 0$，且$a = \mu p_1^{e_1} \cdots p_k^{e_k}$，$b = \nu p_1^{f_1} \cdots p_k^{f_k}$，其中$p_1, \cdots, p_k$是**互不相伴**的**不可约**元，$e_i, f_i \geq 0$，$u, \nu \in R^\times$（注意：这样的分解必然存在，不妨取两者的不可约分解，然后把其中相伴的差的中心元补在前面，最后将互不相伴的所有东西搜罗起来，因此只要求≥ 0）则a, b的gcd和lcm都存在，且可以用这个公式计算：

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} \cdots p_k^{\min(e_k, f_k)},$$
$$\mathrm{lcd}(a, b) = p_1^{\max(e_1, f_1)} \cdots p_k^{\max(e_k, f_k)}.$$

【证明】显示地写下a, b的因子的形式即可得到以上公式.

【定理】设R是整区，则以下等价：

- R是UFD
- R满足ACCP和素性条件
- R满足ACCP和GCD条件（GCD条件：R中任何两个元素的最大公因子都存在，若存在，则自动唯一）

【证明】只有最后一个条件推出素性条件需要证明. 证明可以参考复旦大学《抽象代数学》P102 引理5.5

【命题，lcm的理想刻画】 设R是整区（不需要是UFD），则$m=\mathrm{lcm}(a,b)$当且仅当$(a)\cap(b)=(m)$.

PID，ED

1. PID

- UFD里Bezout等式是不是还成立.

  为了研究这个问题，先看看最大公因子的概念用理想的语言是如何叙述的.

  UFD满足GCD条件，也就是，R中任何两个元素的最大公因子都是存在的（而且可以用一个公式计算出来，见前面）

  $d\mid a,d\mid b$当且仅当$(a)\subseteq(d)$，$(b)\subseteq(d)$，这当且仅当$(a,b)\subseteq(d)$.

  $d=\gcd(a,b)$当且仅当$(a,b)\subseteq(d)$，且如果$(a,b)\subseteq(d')$，则$(d)\subseteq(d')$. 即：$\gcd(a,b)$相伴类对应的主理想是“距离”a,b生成的理想(a,b)“最近”的主理想. 但是这并不能说明$\gcd(a,b)$对应的主理想就等于a,b生成的理想(a,b).

  而Bezout的成立却当且仅当$(a,b)=(d)$！这是因为：

  $$(a,b)=(d)\Leftrightarrow(d)\subseteq(a,b)\Leftrightarrow d\in(a,b)\Leftrightarrow\exists x,y\in R,d=ax+by.$$

  【Remark】注意，事实上$(a,b)=(d)$成立当且仅当(a,b)是一个主理想（若是主理想，则根据(d)是距离它最近的主理想可知(d)就是(a,b)）. 我们将这样的性质提取出来，就得到PID的概念

- 【命题】设R为UFD，$d=\gcd(a,b)$，则以下条件等价：
  - Bezout等式.
  - $(a,b)=(d)$.
  - (a,b)是主理想.
- 【例】 UFD中，(a,b)不总是主理想，例如$\mathbb{Z}[x]$，$(2,x)\neq(1)=\mathbb{Z}[x]$.
- **PID**：若整区R的所有理想都是主理想，则称R是**主理想整区**（PID，Principal Ideal Domain）
- 【命题】PID是UFD.
- 【命题】PID是UFD.

  【证明】验证PID满足因子链条件（事实上只需要验证ACC条件）和素性条件.

  ①验证ACC条件. 若PID有理想升链$I_1\subseteq I_2\subseteq\cdots\subseteq I_n\subseteq\cdots$，考虑$\bigcup_{n\geq1}I_n$，则这是一个理想（容易验证:这$J=\bigcup_{n\geq1}I_n$，如果$u,v\in J$，则存在$m,n$使得$u\in I_m$，$v\in I_n$，不妨$m\geq n$，则有$u,v\in I_m$. 因为$I_m$是理想，所以$u+v\in I_m$且$ru\in I_m$对任何$r\in R$.从而$u+v,ru\in J$，故$J$是理想 ）. 因为$R$是PID，所以$\bigcup_{n\geq1}I_n$是主理想，所以$\bigcup_{n\geq1}I_n=(a)$，其中$a\in R$，所以，$a\in\bigcup_{n\geq1}I_n$，所以存在$i\geq1$，使得$a\in I_i$，所以$(a)\subset I_i$，所以$\bigcup_{n\geq1}I_n=I_i$，因此理想升链稳定.

  ②验证素性条件. 设R是PID，设p是R的不可约元，且$p\mid ab$，要证明$p\mid a$或者$p\mid b$.

  R是PID，考虑(p,a)，则(p,a)是主理想，显然$(p)\subset(p,a)\subset R$，而因为p是不可约元，所以$(p,a)=(p)$或者$(p,a)=R$.

  同理可知$(p,b)=(p)$或者$(p,b)=R$.

  - 若$(p,a)=(p)$，则$a\in(p)$，所以$p\mid a$，
  - 若$(p,b)=(p)$，则$b\in(p)$，所以$p\mid b$，
  - 如果$(p,a)=R$且$(p,b)=R$，我们要说明这是不可能的. 因为$(p,a)=(p)+(a)=R$且$(p,b)=(p)+(b)=R$，所以(p)和(a)、(b)都互素，所以(p)和$(a)(b)=(ab)$互素，因此$(p)+(ab)=R$. 由$p\mid(ab)$可知$ab\in(p)$，所以$(p)+(ab)=(p,ab)=(p)=R$，所以p是单位，但是这与p不可约矛盾.

□

- 【命题】PID适合Bezout等式.

  【证明】此时根据定义可知$(a,b)=(d)$，其中$d=\gcd(a,b)$. 这当且仅当$d\in(a,b)$，也就是存在$x,y\in R$使得$d=xa+yb$.

- 【例】
  - (1) 若R是UFD，p是R的不可约元，则$R/(p)$是整区.
  - (2) 若R是PID，p是R的不可约元，则$R/(p)$是域.

  【证明】
  - (1) 这几乎是显然的. 因为R是UFD，所以R适合素性条件，所以p是素元. 在$R/(p)$中若有$\overline{a}\cdot\overline{b}=\overline{0}$，则有$\overline{ab}=\overline{0}$即$ab\in(p)$. 因为$p$是素元，所以$ab\in(p)\Rightarrow a\in(p)$或$b\in(p)$，从而$\overline{a}=0$或$\overline{b}=0$，由整区的定义可知$R/(p)$是整区.□
  - (2) 只需证明$\forall a\in R$且$a\notin(p)$，$\overline{a}\in(R/(p))^\times$，即存在$b\in R$使得$\overline{a}\overline{b}=\overline{1}$. 考虑理想$(a,p)$，因为$R$是PID，所以存在$r\in R$使得$(a,p)=(r)$. 因为$(p)\subset(a,p)=(r)\subset R$，注意$p$是不可约元，根据不可约元的理想刻画可知$(r)=(p)$或$(r)=R$. 若$(r)=(p)$，则$a\in(p)$，这与$a\notin(p)$矛盾，所以只能是$(r)=R$即$r$是单位，也即$(a,p)=(r)=(1)$，所以存在$x,q\in R$，使得$ab+pq=1$，考虑上式在商同态下的像即得$\overline{a}\overline{b}=\overline{1}$，这就证明了$R/(p)$是域.□

    【注】这对于一般的UFD不成立（一般的UFD只能得到$R/(p)$是整区），例如$\mathbb{Z}[x]/(x^2+1)$，x^2+1是$\mathbb{Z}[x]$中不可约元且$\mathbb{Z}[x]$是UFD，但是$\mathbb{Z}[x]/(x^2+1)=\mathbb{Z}[i]$不是域.□

2. ED

- 【定义】ED

  R为整区，在$R-\{0\}$上定义函数$f:R-\{0\}\to\mathbb{N}=\{0,1,\cdots\}$，满足若$a,b\in R$，$b\neq0$，则存在$q,r\in R$，使得有带余除法：

  $$a=bq+r.$$

  其中，$r=0$或者$f(r)<f(b)$.

  则称f是R上一个Euclid赋值或者Euclid函数，若整区R至少有一个Euclid赋值，则称R是一个Euclid整区.（ED，Euclidean Domain）

  【remark】一般抠掉零元

  【remark】用来衡量带余除法中余式小于除式

  【remark】本质的要求是取值能比大小，而且有下界（后面的证明中有体现），取成$\mathbb{N}$是一种方便的取法.

- 【例】回顾整数的带余除法可知$|\cdot|:\mathbb{Z}-\{0\}\to\mathbb{N}$的一个Euclid函数，所以$\mathbb{Z}$是ED.

  回顾域上一元多项式环$F[x]$的带余除法，可知，$\deg:F[x]-\{0\}\to\mathbb{N}$是一个Euclid函数，所以$F[x]$是ED.

- 【命题】ED是PID.

  【证明】设R是ED，f是其上一个Euclid函数，设I是R的一个理想，要证明它是主理想.
  - $I=0$，则$I=(0)$，不用证明.
  - $I\neq0$，因为f是有下界的，所以，只需要取出$b\in I-\{0\}$，使得$f(b)=\min_{x\in I,x\neq0}f(x)$. 下证明$I$就是$(b)$，这只需要证明$I\subset(b)$.

    任取$a\in I$，存在$q,r\in R$，使得$a=bq+r$，其中$r=0$或者$f(r)<f(b)$.

    观察$a\in I$，$b\in I$，所以$r=a-bq\in I$. 若$r\neq0$，则$f(r)<f(b)$，这与b的选取矛盾. 所以$r=0$，这说明$a=bq\in(b)$，所以$I\subset(b)$，故$I=(b)$，即I是主理想.□

  【remark】这事实上说明ED的所有理想都是主理想，而且该主理想的生成元可以通过欧氏赋值取值最小这一条件找到.

- Gauss整数环$\mathbb{Z}[i]$. 事实上这是$\mathbb{Z}[\sqrt{-1}]$，即在整数环中添加$\sqrt{-1}$.

- **重要定理** $\mathbb{Z}[i]$是ED.

  【证明】此证明的关键是找到欧氏赋值，对于二次代数整数环来说非常重要的一个函数就是N函数.

  $$N:\mathbb{Z}[i]-\{0\}\to\mathbb{N},\quad m+ni\mapsto m^2+n^2.$$

  一些基本的观察：N是满足乘性的，事实上，这是gauss整数作为$\mathbb{C}$中的元素的模长，因此当然是满足乘性的.

- 为了研究Gauss整数环是ED，我们首先将$\mathbb{Z}[i]$延拓为分式域$\mathbb{Q}[i]$，在分式域上也有一个N的对应的延拓，即$\forall q_1+q_2i\in\mathbb{Q}[i]$，定义$N(q_1+q_2i)=q_1^2+q_2^2$.

  则乘性仍然是满足的.

- 证明N是一个欧氏赋值，即$\forall a,b\in\mathbb{Q}[i]$，$b\neq 0$，存在$q,r\in\mathbb{Z}[i]$，使得

  $$a=bq+r,\quad r=0\quad or\quad N(r)<N(b).$$

  也就是在$\mathbb{Q}[i]$中有：

  $$\frac{a}{b}=q+\frac{r}{b},\quad N(\frac{a}{b}-q)<1.$$

- 这只需要一个断言：$\forall x=q_1+q_2i\in\mathbb{Q}[i]$，存在$y=m_1+m_2i\in\mathbb{Z}[i]$，使得：

  $$N(x-y)=(q_1-m_1)^2+(q_2-m_2)^2<1.$$

  断言的证明：令m_1,m_2分别是离q_1,q_2最近的整数，则$|q_1-m_1|\leq\frac{1}{2}$，$|q_2-m_2|\leq\frac{1}{2}$.

  所以

  $$N(x-y)\leq\frac{1}{4}+\frac{1}{4}=\frac{1}{2}<1.$$

- 一旦有了断言，设$a,b\in\mathbb{Z}[i]$，$b\neq 0$，则$\frac{a}{b}\in\mathbb{Q}[i]$，生成存在$q\in\mathbb{Z}[i]$，使得$N(\frac{a}{b}-q)<1$.

  令$r=a-bq\in\mathbb{Z}[i]$，则$N(r)=N(a-bq)=N(b(\frac{a}{b}-q))=N(b)N(\frac{a}{b}-q)<N(b)$.

  注意$b\neq 0$，所以$N(b)>0$.

【remark】在$\mathbb{Z}[\sqrt{2}]$上定义范数$N(m_1+m_2\sqrt{2})=|m_1^2-2m_2^2|$，然后完全仿照上面的步骤可以证明$\mathbb{Z}[\sqrt{2}]$，

- 【定理】Fermat's theorem on sums of two squares

  p是奇素数，则

  $$\exists m,n\in\mathbb{Z},p=m^2+n^2\quad\Leftrightarrow\quad p\equiv 1\mod 4.$$

  【证明】对任何整数n，若$n=2k$是偶数，则$n^2=4k^2\equiv 0\mod 4$，若$n=2k+1$是奇数，则$n^2=4k^2+4k+1\equiv\mod 4$. 因此对任何$m,n\in\mathbb{Z}$，$m^2+n^2\equiv 0,1,2\mod 4$，若还有$m^2+n^2$是奇素数，那么它必然模4余1. 反过来的方向参见一句话证明□

- 观察：若素数p在$\mathbb{Z}[i]$中可约，则其分解必然是$p=(m+ni)(m-ni),n\neq 0$（待定系数，再根据p素），此时$p=m^2+n^2$，所以此时它必然是模4余1的. 因此p在$\mathbb{Z}[i]$中不可约当且仅当p是模4余3的素数.

- 【定理】$\mathbb{Z}[i]$中的不可约元在不计相伴的意义下（$\mathbb{Z}[i]^\times=\{\pm 1,\pm i\}$）有：

  - $1+i$（来自于偶素数2的不可约分解，2是一个可约的素数）
  - $m\pm ni$，其中$0<m<n$，$m^2+n^2=p\equiv 1\mod 4$. 规定m,n的大小关系是保证相伴类不重复，例如$m+ni$和$n-mi$实际上是同一相伴等价类的.
  - p，$p\equiv 3\mod 4$.

- 【例子】2可约，3不可约，5可约，7不可约，11不可约，13可约，17可约，19不可约.

- 【例子】$6+7i$在$\mathbb{Z}[i]$中的不可约分解?

  【解】注意不可约元的模方只能是$4n+3$素数的平方或者$4n+1$素数或者偶素数2.

  $N(6+7i)=85=17\times 5$，对应一个模为17的不可约元和一个模为5的不可约元的乘积（两者都是$4n+1$素数）

$(1+4i)(1+2i)=-7+6i$，补充一个单位元$-i$可得不可约分解$6+7i=(4-i)(1+2i)$.

3. 以下证明R是UFD给出$R[x]$是UFD这一大定理

- 【大定理】R是UFD $\Rightarrow R[x]$是UFD.
- 基本策略：考虑$R[x]$与$F[x]$以及$R/(p)[x]$的联系，$F=\mathrm{Frac}(R)$是分式域，p是R的不可约元.
- 注意以下事实：
  - 若p是R的不可约元，则$R/(p)$是整区.
  - $F[x]$都是ED，从而使PID，UFD，所以对任何$f\in R[x]$，f作为$F[x]$中的元素有不可约分解.
  - $F[x]$中任何一个多项式$f(x)$都与$R[x]$中的某个多项式$g(x)$在$F[x]$中相伴（**通分**即可）
- 【引理】（整区上一元多项式环的性质）R是整区
  - $\forall f(x),g(x)\in R[x]$，有$\deg f(x)g(x)=\deg f(x)+\deg g(x)$.

    规定$\deg 0=-\infty$，$-\infty+\alpha=-\infty$ for all $\alpha\in\mathbb{N}\cup\{-\infty\}$.
  - $R[x]$是整区（根据前一题的结论）
  - $R[x]^\times=R^\times$
  - $a\in R$，则a是R的**不可约元**当且仅当a作为$R[x]$中的元素是**不可约元**.

  【证明】都比较显然，第三个和第四个需要考虑次数的关系.
- 【例】对于整区上的多项式环$R[x]^\times$，有$R^\times=R[x]^\times$.

  但是对于一般情况，也就是如果$R\subset S$，R是S的子环，则有$R^\times\subset S^\times$，但是一般没有$R^\times=S^\times$. 更准确地说：

  $$R^\times\subset R\cap S^\times\subset S^\times.$$

  而这两个包含关系都可以不相等.

  ① 第二个包含关系：即S中的单位不必落在R中，例如$\mathbb{Q}$中非零元均为单位，$\mathbb{Z}$是$\mathbb{Q}$的子环，而$\frac{1}{2}\in\mathbb{Q}^\times$不在$\mathbb{Z}$中.

  ② 第一个包含关系：即便S的单位在R中，它在R中也不必可逆. 例如$2\in\mathbb{Q}^\times$，$2\in\mathbb{Z}$，但是$2\notin\mathbb{Z}^\times$.
- 【例】对于整区上的多项式环$R[x]$，有：R中元素不可约，当且仅当它作为$R[x]$中的元素也不可约.

  但是对于一般情况，也就是S是整区，R是S的子环从而也是整区，这一般不成立，更准确地：
  - S的不可约元若在R中，它有可能可约，也有可能不可约.

    例如$\mathbb{Z}[i]$是整区，$\mathbb{Z}$是$\mathbb{Z}[i]$的子环，3是$\mathbb{Z}[i]$中不可约元，也是$\mathbb{Z}$中不可约元.

    $S=\mathbb{Z}\cup\frac{\mathbb{Z}}{2}\cup\frac{\mathbb{Z}}{4}\cup\cdots$是整区，$\mathbb{Z}$是其子环，$6$是$S$中不可约元，这是因为，$3$在$S$中不可约，$2\in S^\times$，所以$6$与$3$在$S$中相伴，所以$6$在$S$中不可约，但是$6$在$\mathbb{Z}$中是可约的.
  - R的不可约元在S中，有可能可约，也有可能不可约，还有可能是单位.

    例如$\mathbb{Z}[i]$是整区，$\mathbb{Z}$是$\mathbb{Z}[i]$的子环，2在$\mathbb{Z}$中不可约但是在$\mathbb{Z}[i]$中可约，3在$\mathbb{Z}$中不可约，在$\mathbb{Z}[i]$中也不可约

    $\mathbb{Z}$是$\mathbb{Q}$的子环，2在$\mathbb{Z}$中不可约，但是在$\mathbb{Q}$中是单位.
- 【引理】**（考虑UFD中的不可约元）**R是UFD
  - $R[x]-0-R[x]^\times=R[x]-0-R^\times=(R-0-R^\times)\bigsqcup(R[x]-R)$.（UFD中不可约元的分类）

    【remark】注意到R中不可约元与$R[x]$中次数为0不可约元一致，所以只需要看次数大于1的不可约元是哪些，这需要用到UFD上一元多项式环f的容量$C(f)$的概念.
  - $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$，$a_n\neq 0$，$\deg f=n\geq 1$，则$f$是不可约元的一个必要条件是$C(f)=1$.
- 【定义】$C(f)$：R是UFD，$f\in R[x]$，且$f(x)\neq 0$，称

  $$C(f):=\gcd(a_0,a_1,\cdots,a_n)\in R$$

  为f的容量. 若$C(f)=1$，则称f为$R[x]$上本原多项式（primitive polynomial）

【remark】$C(f)$的良定义性：$C(f)$在不计相伴下是良定义的，因为gcd是一个相伴等价类.

- 【例】两个关于R和$R[x]$的例子.

  R是整区.

  - (1) 若$R[x]$是PID，则R是域.
  - (2) 若$R[x]$是UFD，则R也是UFD.

  【证明】

  - (1) 对任何$a\in R-0$，考虑它作为$R[x]$中的元素，在$R[x]$中考虑(a,x)，因为$R[x]$是PID，所以存在$b\in R[x]$使得$(a,x)=(b)$.

    断言x是$R[x]$中的不可约元. 否则存在$f(x),g(x)\in R[x]$非单位，使得$x=f(x)g(x)$. 根据整区上一元多项式环的性质可知$1=\deg x=\deg f(x)+\deg g(x)$，不妨$\deg f(x)=1$，$\deg g(x)=0$，$f(x)=cx+d$，$g(x)=e$，其中$c,d,e\in R[x]$，$c,e\neq 0$，于是$x=cex+de$，因为$R$是整区，所以$d=0$，$ce=1$. 所以$e\in R^\times$，根据引理可知$R^\times=R[x]^\times$从而$g(x)\in R[x]^\times$，这与$f(x),g(x)$非单位矛盾.

    一旦证明了**断言**，$(x)\subset(a,x)=(b)\subset R$，由$x$不可约知$(b)=(x)$或$(b)=(R)$，若$(b)=(x)$则$a\in(x)$，所以$\deg a\geq 1$，这与$a\in R-0$矛盾，所以$(b)=R$. 所以$(a,x)=(1)$，所以存在$p(x),q(x)\in R[x]$，使得：

    $$xp(x)+aq(x)=1.$$

    因为$xp(x)$不提供常数项，又结合次数的考虑容易看出：

    $$ar=1.$$

    其中$r\in R$且r是$q(x)$的常数项，由整区可知是$a\in R^\times$，所以R是域.

  - (2) 仍然是用整区上一元多项式环的性质. 设$I_1\subset I_2\subset\cdots I_n\subset\cdots$是$R$中一个（不必严格的）主理想升链，则这也是$R[x]$中的一个主理想升链. 因为$R[x]$是UFD，所以$R[x]$适合因子链条件，所以这个主理想升链稳定. 而以上论述对R中任何一个主理想升链都是成立的，所以R中任何一个主理想升链都稳定，所以R适合因子链条件.

    设$a\mid bc$在R中，则将a,b,c看成$R[x]$中元素就有$a\mid bc$在$R[x]$中，因为$R[x]$是UFD，所以适合塑性条件，所以存在$a\mid b$或$a\mid c$在$R[x]$中. 于是存在$p(x)\in R[x]$使得$b=ap(x)$或者存在$q(x)\in R[x]$使得$c=aq(x)$. 考虑次数可知若存在，则$\deg p(x)=0$，$\deg q(x)=0$，于是存在$p\in R$或者$q\in R$，使得$b=ap$或$c=aq$，于是有$a\mid b$或$a\mid c$在R中. 以上论述中，我们通过$a\mid bc$推出了$a\mid b$或$a\mid c$在R中，所以R适合素性条件.

    综上所述，R适合素性条件和因子链条件，所以R是UFD.□

- 【定理】（次数>1多项式什么时候不可约）R是UFD，$f(x)\in R[x]$，$\deg f(x)\geq 1$，则以下等价：
  - $f(x)$是$R[x]$中不可约多项式
  - $f(x)$是$R[x]$中本原多项式且$f(x)$作为$F[x]$中元素是不可约多项式，其中$F=\mathrm{Frac}R$.
- 【引理】R是UFD，F是R的分式域$\mathrm{Frac}R$，则：
  - 对任何$f(x)\in R[x]-0$，$a\in R-0$，有$C(af)=aC(f)$（显然）
  - 对任何$f(x)\in R[x]-0$，存在$R[x]$中本原多项式$g(x)$使得$f(x)=C(f)g(x)$.（显然）
  - 对任何$f(x)\in F[x]-0$，存在$c\in F^\times$，以及$R[x]$中本原多项式$g(x)$，使得$f(x)=cg(x)$.

    （首先$f(x)$和$R[x]$中某个多项式$f_1(x)$在$F[x]$中相伴，而对$f_1(x)$存在$g(x)$是$R[x]$中本原多项式使得$f_1(x)=C(f_1)g(x)$，合并系数即可）
  - 若$f(x)=cg(x)$，其中$f(x),g(x)\in R[x]-0$且$g(x)$本原，$c\in F^\times$，则$c=C(f)\in R$.

    （$c\in F^\times$，即存在$a,b\in R-0$使得$c=\frac{a}{b}$，对$bf(x)=ag(x)$在$R[x]$中成立两边取C，再用到g本源得$c=C(f)\in R$.）
- 【引理】（Gauss引理） 设R是UFD，则$R[x]$中的两个本原多项式的乘积仍然是本原多项式.

- 【例】Gauss引理的证明，可以考虑$R/(p)[x]$. 这种证明方法留作练习题.
- 【证明】这里用另一种方法证明Gauss引理.

  $f(x)=\sum_{i=0}^{m}a_ix^i$和$g(x)=\sum_{j=0}^{n}b_jx^j$是$R[x]$中两个本原多项式，$h(x)=f(x)g(x)=\sum_{k=0}^{m+n}c_kx^k$. 要证明$h(x)$本原，只需证明对任何$R$的不可约元$p$，存在$k$，使得$p\nmid c_k$.

  $f(x),g(x)$本原给出存在i_0,j_0，p整除$a_m,a_{m-1},\cdots,a_{i_0+1}$，也整除$b_n,b_{n-1},\cdots,b_{j_0+1}$，但$p\nmid a_{i_0}$，$p\nmid b_{j_0}$

  令$k_0=i_0+j_0$，设$h(x)$中x^{k_0}的系数为c_{k_0}，则有$c_{k_0}=\sum_{i+j=k_0}a_ib_j$.

  当$i>i_0$时，因为$p\mid a_i$，所以$p\mid a_ib_j$

  当$j>j_0$时，因为$p\mid b_j$，所以$p\mid a_ib_j$

  当$i=i_0,j=j_0$时，因为$p\nmid a_{i_0}$且$p\nmid b_{j_0}$，所以$p\nmid a_{i_0}b_{j_0}$（因为p不可约，所以p素）

- 【定理的证明】
  - ①f在$R[x]$不可约$\Rightarrow$ f本原，且在$F[x]$中不可约.

    【证明】本原已经证明（本原是不可约的必要条件），下面证明f在$F[x]$中不可约（反证法）. 设$f(x)=g(x)h(x)$在$F[x]$中，其中$g(x),h(x)$ 非单位. 因为$F[x]^\times=F^\times$，所以$\deg g(x)\geq 1$，$\deg h(x)\geq 1$.

    对于$g(x)$和$h(x)$，根据引理，存在$c_g,c_h\in F^\times$，使得$g(x)=c_gg_1(x)$，$h(x)=c_hh_1(x)$，其中$g_1(x),g_2(x)\in R[x]$本原，代入分解式可得

    $$f(x)=c_gc_hg_1(x)h_1(x).$$

    因为g_1,h_1在$R[x]$都本原，R是UFD，根据Gauss引理，g_1h_1在$R[x]$也本原. 又因为$f(x)\in R[x]$，$c_gc_h\in F^\times$，根据引理可知$c_gc_h=c(f)\in R$，从而得到了$R[x]$中的分解式：

    $$f(x)=c(f)g_1(x)h_1(x).$$

    注意$\deg g_1(x)=\deg g(x)\geq 1$，$\deg h_1(x)=\deg h(x)\geq 1$，所以$g_1(x),h_1(x)\notin R[x]^\times$，这与$f(x)$不可约矛盾.□
  - ②f本原且在$F[x]$不可约$\Rightarrow$ 在$R[x]$不可约.

    【证明】（反证）设f本原且在$F[x]$不可约，假设f在$R[x]$可约，则存在$g(x),h(x)\in R[x]-R[x]^\times$，使得$f(x)=g(x)h(x)$. 分两种情况：

    $(i)\deg g=0$（或$\deg h=0$），$g(x)=b\in R$，因为$R[x]^\times=R^\times$，所以$b\notin R^\times$. 所以$f(x)=bh(x)$，所以$c(f)=bc(h)$，这说明$c(f)\notin R^\times$，这与f本原矛盾.

    $(ii)\deg g,\deg h\geq 1$，则$f(x)=g(x)h(x)$在$F[x]$中也成立，这与$f(x)$在$F[x]$中不可约矛盾.□

  【remark】这个定理完全解决了$R[x]$（R是UFD）的不可约元问题，$R[x]$（R是UFD）的不可约元有两种：

  ①R的不可约元（前面关于整区的引理），②$f(x)$本原且在$F[x]$中不可约（刚刚证的定理）

- 【主定理的证明】

  存在性：$f(x)\in R[x]-0-R[x]^\times$，分为两种，$\deg f(x)=0$和$\deg f(x)\geq 1$.
  - $\deg f(x)=0$，则$f(x)=a\in R-0-R^\times$，因为R是UFD，所以a有不可约分解. 注意事实：R中元素不可约，当且仅当它作为$R[x]$中的元素也不可约，所以这也会是$R[x]$的不可约分解.
  - $\deg f(x)\geq 1$，因为$f(x)\in R[x]\subset F[x]$，取$f(x)$在$F[x]$中的不可约分解

    $$f(x)=p_1(x)\cdots p_r(x)$$

这些$p_i(x)$为$F[x]$中不可约多项式，根据前面的引理，存在$c_i \in F^\times$，使得$p_i(x) = c_i q_i(x)$，其中$q_i(x) \in R[x]$本原，代入原来的分解式有$f(x) = \underbrace{c_1 \cdots c_r}_{\in F^\times} \underbrace{q_1(x) \cdots q_r(x)}_{\text{Gauss's Lemma}\to\text{本原}}$，因为$f(x) \in R[x]$，所以根据前面的引理可知，$c_1 \cdots c_r = c(f) \in R$，因为$R$是UFD，所以$c(f)$有不可约分解$c(f) = a_1 \cdots a_s$在$R$中，代入可得

$$f(x) = a_1 \cdots a_s q_1(x) \cdots q_r(x)$$

注意a_i不可约在R中，所以a_i不可约在$R[x]$中. 另外，$q_i(x)$在$R[x]$本原且与$F[x]$中不可约元$p_i(x)$相伴，于是$q_i(x)$本原且在$F[x]$不可约，于是上述就是$f(x)$的不可约分解.□

唯一性：也分两种情况.

- $\deg f(x) = 0$，则$f(x) = a \in R - 0 - R^\times$，设$a = a_1 \cdots a_r$在$R[x]$中是不可约分解，从而根据阶数可知$\deg a_1 = \cdots = \deg a_r = 0$，所以$a_1, \cdots, a_r \in R - 0$不可约. 如果还有$a = b_1 \cdots b_s$，同样也有$\deg b_1 = \cdots = \deg b_s = 0$，所以$b_1, \cdots, b_s \in R - 0$不可约，这样得到了$a \in R$在$R$中的两种不可约分解：

  $$a = a_1 \cdots a_r = b_1 \cdots b_s.$$

  因为R是UFD，所以$r = s$且$a_1, \cdots, a_r$和$b_1, \cdots, b_r$适当调换顺序之后有$a_i \sim b_i$， 所以在$R[x]$中也有$a_i \sim b_i$，这就证明了不可约分解的唯一性.

- $\deg f(x) \geq 1$，设在$R[x]$中有两种不同的不可约分解：

  $$f(x) = a_1 \cdots a_r p_1(x) \cdots p_t(x),$$
  $$f(x) = b_1 \cdots b_s q_1(x) \cdots q_l(x).$$

  其中p_i, q_i不可约从而本原.

  分别在两个式子中计算可得$c(f) = a_1 \cdots a_r = b_1 \cdots b_s$，根据$R$是UFD，$a_i, b_j$不可约可知$r = s$，且适当调换顺序后又$a_i \sim b_i$.

  因为$R[x]$是整区，所以将$c(f)$从两侧消掉可得

  $$p_1(x) \cdots p_t(x) = q_1(x) \cdots q_l(x)$$

  将以上式子看成$F[x]$中等式，因为p_i, q_i在$R[x]$不可约，所以它们在$F[x]$中不可约，因为$F[x]$是ED从而是UFD，所以根据唯一性可知适当调整顺序后就有$p_i = c_i q_i$，其中$c_i \in F^\times$. 因为q_i本原，$p_i \in R[x]$，所以$c_i = c(q_i) \in R$. 又因为q_i是本原多项式，所以$c(q_i) \in R^\times$（相伴等价类），所以$p_i \sim q_i$在$R[x]$中.这就证明了以上两种分解不计相伴下相同.□

- 【定理】（UFD的Eisenstein判别法） R是UFD，F是R的分式域，

  $$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$$

  且$\deg f = n \geq 2$，则若存在R的不可约元p，使得$p \nmid a_n$，$p \mid a_i\ (0 \leq i \leq n-1)$，$p^2 \nmid a_0$，则$f(x)$是$F[x]$中不可约多项式.

素理想和极大理想

只讨论**交换环**R的素理想和极大理想.

- 【定义】素理想的定义可以类比素元.
  - 素元（理想刻画）：R是**整区**，称$p \in R$是R的素元，如果

    $$ab \in (p) \Rightarrow a \in (p) \quad \text{或} \quad b \in (p).$$

  - 素理想：R是**交换环**，I是R的真理想（即I是R的理想且I不是R），称I是R的素理想，如果：

$$ab \in I \Rightarrow a \in I \quad 或 \quad b \in I.$$

- 素理想的商环刻画：从“得到的商环是什么样子”来描述素理想.
  - R是交换环，I是R的素理想 $\Leftrightarrow$ R/I是整区（显然，在R/I中$\overline{a}\overline{b}=\overline{0}$给出$\overline{a}=\overline{0}$或$\overline{b}=\overline{0}$ $\Leftrightarrow$ 在R中有$ab \in I$给出$a \in I$或$b \in I$）
  - 推论：0理想是R的素理想，当且仅当R是整区.
- 【引理】主理想什么时候是素理想？答：在整区中，大致有：“素元生成的主理想是素理想”

  若R是整区，$a \in R$，则(a)是R的素理想当且仅当$a=0$或a是素元.

  【证明】由素元的理想刻画立刻得.□
- 【例】R是交换环，P是R的真理想，则P是R的素理想，当且仅当：若有两个理想I,J满足$IJ \subset P$，则必有$I \subset P$或$J \subset P$.

  【证明】必要性：用反证法，假设$I \not\subset P$且$J \not\subset P$，则存在$a \in I$，$b \in J$，但$a,b \notin P$. 因为$IJ \subset P$，所以$ab \in P$，又因为P是素理想，所以$a \in P$或$b \in P$，和前面的讨论矛盾.

  充分性：如果$ab \in P$，取$I=(a)$，$J=(b)$，则$IJ=(a)(b)=(ab) \subset P$（$ab \in P \Rightarrow (ab) \subset P$），所以$(a) \subset P$或$(b) \subset P$（由条件），所以$a \in P$或$b \in P$.

  □
- 【定义】极大理想的定义类比不可约元
  - 不可约元的理想刻画：R**整区**，p（非零非单位）是R的不可约元当且仅当(p)和R之间不能再非平凡地插入某个主理想，或者，若有$(p) \subset (a) \subset R$，则有$(p)=(a)$或$(a)=R$.
  - 极大理想：R是**交换环**，I是R的真理想，称I是R的极大理想，如果I和R之间不能再非平凡地插入某个理想，或者，若有J是R的理想，适合$I \subset J \subset R$，则有 $I=J$或$J=R$.
- 极大理想的商环刻画
  - R是交换环，I是R的极大理想，当且仅当R/I是域（显然，I是R的极大理想，翻译过来就是，$\forall a \in R-I$，$I+(a)=R$，即$\forall a \in R-I$，存在$x \in I$以及$b \in R$，使得$ab+x=1$. 再翻译过来就是，$\forall \overline{a} \in R/I$，$\overline{a} \neq \overline{0}$，存在$\overline{b} \in R/I$，使得$\overline{a}\overline{b}=\overline{1}$. 也就是$R/I-0=(R/I)^{\times}$.）
  - 推论，**极大理想**$\Rightarrow$ R/I是域$\Rightarrow$ R/I是整区$\Rightarrow$ **素理想**
- 【例】域F的真理想只有0，所以F的素理想、极大理想都只有0.
- 【命题】R是PID但不是域
  - 【回顾1】 R是PID，p是R的不可约元，则$R/(p)$是域.
  - 【回顾2】 PID 的所有理想形如(a)，回顾刚才的命题，主理想是素理想当且仅当$a=0$或a是素元.
  - 【回顾3】 PID是UFD，满足素性条件（不可约元等价于素元）
  - 【回顾4】R是交换环，则极大理想$\Rightarrow$素理想
  - 【结论1】R的素理想只有$0,(p)$，其中p是R的不可约元（根据回顾2、3）
  - 【结论2】R的极大理想只有(p)（根据$R/(0)=R$不是域可知0不是极大理想，再根据回顾1、4结合结论1）
- 【例】
  - $\mathbb{Z}$的素理想只有$0,p\mathbb{Z}$，极大理想只有$p\mathbb{Z}$.
  - $F[x]$的素理想只有$0,(p(x))$，极大理想只有$(p(x))$，其中$(p(x))$是$F[x]$上不可约多项式.
- 【例】 UFD 情况较为复杂，一般只有：若p是不可约元，则(0)和(p)都是R的素理想.（根据素性条件）
- 【例】(2)是$\mathbb{Z}[x]$的素理想，但不是极大理想.

  【证明】因为$\mathbb{Z}[x]$是UFD，2是$\mathbb{Z}[x]$不可约元（根据2是$\mathbb{Z}$的不可约元），所以(2)是$\mathbb{Z}[x]$的素理想.

  为什么不是极大理想？用极大理想的商环刻画，因为$\mathbb{Z}[x]/(2)=\mathbb{F}_2[x]$，不是域.□
- 【例】 $(x-m,p)$是$\mathbb{Z}[x]$的极大理想（其中m是整数，p是素数）

  【证明】$\mathbb{Z}[x]/(x-m,p)=\mathbb{Z}[x]/(x-m)/(x-m,p)/(x-m)=\mathbb{Z}/p\mathbb{Z}=\mathbb{F}_p$，是域.□
- 【例】$(x^2+x+1,2)$是$\mathbb{Z}[x]$的极大理想

  【证明】$\mathbb{Z}[x]/(x^2+x+1,2)=\mathbb{Z}[x]/(2)/(x^2+x+1,2)/(2)=\mathbb{F}_2[x]/(x^2+x+\overline{1})$

$x^2+x+\overline{1}$在$\mathbb{F}_2[x]$中是不可约的，二次（当然还有三次）多项式是不是可约可以看对应的多项式方程有没有根，在这里显然是没有的：$0^2+0+1=1$，$1^2+1+1=1$.

所以这是一个域□

- 【例】$\mathbb{Z}[\sqrt{-5}]$，(2)不是素理想，$(2,1+\sqrt{-5})$是极大理想.

  【证明】注意这不是UFD，2是不可约元但是2不是素元.（$2\mid(1+\sqrt{-5})(1-\sqrt{-5})$但是不整除任何一个）

  下面证$(2,1+\sqrt{-5})$是极大理想.

  $\mathbb{Z}[\sqrt{-5}]/(2,1+\sqrt{-5})=(\mathbb{Z}[x]/(x^2+5))/((2,1+x,x^2+5)/(x^2+5))=\mathbb{Z}[x]/(2,1+x,x^2+5)$

  注意$x^2+5\subset(2,1+x)$，这是因为$x^2+5=2\times3+(1+x)(x-1)$，所以
  $(2,1+x,x^2+5)=(2,1+x)$.

  所以上式$=\mathbb{Z}[x]/(2,1+x)=\mathbb{F}_2$，是域.□