我们知道在整数环及数域上一元多项式环中都有因子分解定理，

那么在一般的整环中因子分解定理是否成立呢?

本节将就此问题进行简单讨论，

假设本节所涉及的环均为整环，

若 R 是整环，则 U(R)表示 R 的单位群，R^*表示 R 的非零元构成的集合，

$\hat{R}$表示 R 的非零、不可逆元构成的集合，即$\hat{R}=R^*-U(R)$，

一、整除性、不可约元和素元

定义 7.1 设 R 是整环，a，b 属于 R，若存在属于 R 的 c，使得 a=bc，

则称 b 整除 a

或称 b 是 a 的因子，一般地，将其记为 b|a，

如果不存在这样的 c，则称 b 不整除 a，或称 b 不是 a 的因子，记为 b∤a，

若 b|a 和 a|b 同时成立，则称 a 与 b 相伴，记作 a~b，

R 的可逆元及与 a 相伴的元素都是 a 的因子，称这样的因子为 a 的平凡因子，

a 的其他因子(如果有的话)称为 a 的真因子，

整除有如下性质:

命题 7.1 设 R 是整环，若 a，b，c，x，y 属于 R，则下列结论成立:

(1)a|a(整除具有反身性);

(2)如果 a|b 且 b|c，那么 a|c(整除具有传递性);

(3)如果 a|b 且 a|c，那么 a|(xb+yc);

(4)a|b⇔⟨b⟩包含于⟨a⟩;

(5)a~b⇔⟨a⟩=⟨b⟩;

命题 7.2 设 R 是整环 ，a , b , c 属于 R，若 a=bc 且 a≠0，则

(1)当 b~a 时 ，c 是可逆元;

(2)当 b 是可逆元时 ，c~a

(3)若 b 是 a 的真因子 ，则 c 也是 a 的真因子 ，

证: (2)的结论是明显的 ，(3)的结论可以由(1) , (2)得出 ，我们仅需要证明(1)，

若 b~a，则存在属于 R 的 d，使得 b=ad，那么 a=adc，

根据整环的消去律可知 1=dc，即 c 是可逆元 ，

例 7.1 在整环 $Z[\sqrt{-3}]=\{a+b\sqrt{-3}|a,b\in Z\}$中 ，证明 $2\nmid(1\pm\sqrt{-3})$，

证: 若 $2|(1\pm\sqrt{-3})$，则存在属于 $Z[\sqrt{-3}]$的α，使得 $2\alpha=(1\pm\sqrt{-3})$，

但是 $\alpha=\frac{1\pm\sqrt{-3}}{2}$不属于 $Z[\sqrt{-3}]$，矛盾 ，因此 $2\nmid(1\pm\sqrt{-3})$，

例 7.2 在整环 $Z[\sqrt{-3}]=\{a+\sqrt{-3}b|a,b\in Z\}$中 ，求 4 的所有因子 ，

解: 若 $\alpha=a+b\sqrt{-3}$ ，则 $N(\alpha)=a^2+3b^2$，

若令 $4=\alpha\beta$，其中α , β属于 $Z[\sqrt{-3}]$，则 $16=N(\alpha)N(\beta)$，

当 $N(\alpha)=1$, $N(\beta)=16$ 时 ，$\alpha=\pm1$, $B=\frac{4}{\pm\alpha}=\pm4$;

当 $N(\alpha)=2$, $N(\beta)=8$ 时 ，这样的α , β不存在;

当 $N(\alpha)=4$, $N(\beta)=4$ 时 ，$\alpha=\pm2$, $\beta=\frac{4}{\pm2}=\pm2$ 或 $\alpha=\pm(1\pm\sqrt{-3})$, $\beta=\pm2(1\mp\sqrt{-3})$

从而 4 的所有因子为 $\alpha=\pm1,\pm2,\pm(1\pm\sqrt{-3}),\pm4$，

定义 7.2 令 R 是整环 ，a , b 属于 R，若存在属于 R 的 d，使得 d|a , d|b，

则称 d 为 a , b 的公因子 ，

特别地 ，若 d 为 a , b 的公因子 ，并且对于任意 a , b 的公因子 c 有 c|d，

则称 d 为 a , b 的最大公因子 ，记为(a , b)，

若 1 是 a , b 的最大公因子 ，则称 a 与 b 互素 ，

根据定义易知，两个最大公因子相伴，

实际上，还容易验证最大公因子具有如下性质:

(1)$(a,(b,c))\sim((a,b),c)$;

(2)$(ca,cb)\sim c(a,b)$;

(3)$(a,b)\sim 1,(a,c)\sim 1\Rightarrow(a,bc)\sim 1$,

两个元素的最大公因子的定义及性质可以推广到有限个元素上，

例 7.3 在高斯整环 Z[i]中，求 $1+i$ 和 3 的公因子和最大公因子，

解: 若$\alpha=a+bi$ 是 $1+i$ 的因子，则 $N(\alpha)|N(1+i)$，即$(\alpha^2+b^2)|2$,

因而 $N(\alpha)=2$ 或 1，$\alpha=\pm(1\pm i)$或± 1 或$\pm i$，显然，$1+i$ 仅有平凡因子，

若$\alpha=a+bi$ 是 3 的因子，则 $N(\alpha)|N(3)$，即$(a^2+b^2)|9$,

因而 $N(\alpha)=1$ 或 3 或 9，显然，$N(\alpha)\neq 3$,

当 $N(\alpha)=1$ 时，$\alpha=\pm 1$ 或$\pm i$，当 $N(\alpha)=9$ 时，$\alpha=\pm 3$ 或$\pm 3i$,

所以，3 只有平凡因子: $\pm 1,\pm i,\pm 3,\pm 3i$,

因此，$\pm 1,\pm i$ 是 $1+i$ 和 3 的公因子，这些公因子彼此相伴，

因而它们也是 $1+i$ 和 3 的最大公因子，

定义 7.3 设 R 是整环，a 属于$\hat{R}$，若 a 只有平凡因子，则称 a 是 R 的不可约元，

若 a 有非平凡因子，则称 a 是 R 的可约元，

定义 7.4 设 R 是整环，p 属于$\hat{R}$，

若从 $p|ab$ 能够推出 $p|a$ 或 $p|b$，则称 p 是 R 的素元

命题 7.3 设 R 是整环，a，b 属于 R 且 a~b，

若 a 是 R 的不可约元(或素元)，则 b 是 R 的不可约元(或素元)，

证: 由 a~b 可知，存在可逆元 u，使得 b=au，又由 a 属于$\widehat{R}$可知 b 属于$\widehat{R}$，

若 c 是 b 的因子，则 c 是 a 的因子，

因为 a 只有平凡因子，所以 c 是可逆元或 c 与 a 相伴，从而，c 与 b 相伴，

也就是说，c 是 b 的平凡因子，b 是不可约元，

若 b|cd，则 a|cd，

因为 a 是素元，所以 a|c 或 a|d，而 $a=bu^{-1}$，因此，b|c 或 b|d，即 b 是素元

在讨论因子分解问题时，我们认为相伴的两个元素是一样的

素元的概念也可以用理想的语言表述为:

命题 7.4 若 R 是整环，p 属于 R，则当且仅当⟨p⟩是非零素理想时，p 是素元

证: 若 p 是素元，则 p 属于$\widehat{R}$，从而⟨p⟩是 R 的非零真理想，

若令 ab 属于⟨p⟩，则 p|ab，从而 p|a 或 p|b，

因此 a 属于⟨p⟩或 b 属于⟨p⟩，即⟨p⟩是素理想，

反之，若⟨p⟩是非零素理想，则 p 属于$\widehat{R}$，

若令 p|ab，则 ab 属于⟨p⟩，

因为⟨p⟩是素理想，所以 a 属于⟨p⟩或 b 属于⟨p⟩，进而 p|a 或 p|b，于是 p 是素元

命题 7.5 令 R 是整环，则 R 中素元一定是不可约元，

证: 若令 p 是素元，则⟨p⟩是非零素理想，

若 a 是 p 的因子，则存在属于 R 的 b，使得 p=ab，从而 ab 属于⟨p⟩，

又因为⟨p⟩是素理想，

所以 a 属于⟨p⟩或 b 属于⟨p⟩，那么 p|a 或 p|b，即 a~p 或 b~p，

再由命题 7.2 可知，a 是 p 的平凡因子，即 p 是不可约元，

例 7.4 在整数环 Z 中，素元和不可约元的概念是等价的

证: 因为 n 与−n 相伴，所以根据命题 7.3 的结论，不妨设 n 是正整数，

若 n 是不可约元，则 n 一定是素数，

由本章例 5.5 可知，⟨n⟩是非零素理想，再由命题 7.4 可知，n 是素元，

反之，由命题 7.5 即可得证，

例 7.5 设 F 是数域，在一元多项式环 F[x]中，不可约元就是不可约多项式，

例 7.6 在整环 $Z[\sqrt{-3}]=\{a+\sqrt{-3}b|a,b\in Z\}$中，证明 2 是不可约元，但不是素元

证: 首先，2 不是可逆元，

因为若 2 是可逆元，则存在属于 $Z[\sqrt{-3}]$的α，使得 $1=2\alpha$，则 $1=4N(\alpha)$，矛盾，

所以，2 不是可逆元，

其次，考察 2 的因子，令 $2=\alpha\beta$，α，β属于 $Z[\sqrt{-3}]$，则 $4=N(2)=N(\alpha)N(\beta)$，

若 $N(\alpha)=1$，则$\alpha=\pm1$，α是可逆元;

若 $N(\alpha)=2$，则这样的α不存在;

若 $N(\alpha)=4$，则 $N(\beta)=1$，即β是可逆元，从而 2 与α相伴，

综上，2 仅有平凡因子，所以 2 是不可约元，

注意到，$2|(1+\sqrt{-3})(1-\sqrt{-3})$，但 $2\nmid(1+\sqrt{-3})$，这说明 2 不是素元，

二、唯一分解整环

定义 7.5 设 R 是整环，若对属于$\hat{R}$的任意 a 满足以下两个条件:

(1)存在不可约元 $p_1,p_2,\cdots,p_m$，使得 $a=p_1p_2\cdots p_m$;

(2)如果还有不可约元 $q_1,q_2,\cdots,q_n$，使得 $a=q_1q_2\cdots q_n$，那么 $m=n$，

并且经过适当调整 q_i 的顺序之后，有 p_i 与 q_i 相伴，$i=1,2,\cdots,m$，

则称 R 是唯一分解整环，当然$\hat{R}$中任意元素 a 在 R 中有唯一分解，

在整数环 Z 中，

若 $n\neq 0, \pm 1$，则 n 可以唯一地表示成不可约元的乘积，因此 Z 是唯一分解整环

令 F 是数域，在一元多项式环 F[x]中，

若 $\deg f(x)\geqslant 1$，则 f(x)可以唯一地表示成不可约多项式的乘积，

根据例 7.5 可知，F[x]中的不可约多项式实际上是 F[x]中的不可约元，

因此，F[x]是唯一分解整环，

为了研究唯一分解整环的判定问题，我们先证明如下引理，

引理 7.1 设 R 是唯一分解整环，a 属于$\hat{R}$，

令 $a=p_1p_2\cdots p_m$, 其中 $p_1, p_2, \cdots, p_m$ 是 R 的不可约元，

若 b 是 a 的真因子，则 b 与 $p_1, p_2, \cdots, p_m$ 中某些因子的乘积相伴，

证: 因为 b 是 a 的真因子，所以 b 属于$\hat{R}$，

若令 a=bc，则由命题 7.2 可知，c 是 a 的真因子，

从而 c 属于$\hat{R}$，那么 b, c 在 R 中有唯一分解，

若设 $b=q_1q_2\cdots q_k, c=r_1r_2\cdots r_l$, 其中 $q_1, q_2, \cdots, q_k, r_1, r_2, \cdots, r_l$，是不可约元，

则 $a=q_1q_2\cdots q_kr_1r_2\cdots r_l$

再由 R 中元素分解的唯一性可知，每个 q_i 与某个 p_j 相伴，

因此 b 与 $p_1, p_2, \cdots, p_m$ 中某些因子的乘积相伴，

由引理 7.1 知道，唯一分解整环的非零不可逆元素的真因子个数是有限的(不考虑相伴的因素)，

推论 7.1 令 R 是唯一分解整环，$b, p_1, p_2, \cdots, p_m$ 是 R 的不可约元，

若 $b|p_1p_2\cdots p_m$，则存在 p_i，使得 $b\sim p_i$

定理 7.1 若 R 是整环，则当且仅当 R 满足下面两个条件时，R 是唯一分解整环

(1)若 R 中的元素列 $a_1, a_2, \cdots, a_n, \cdots$，满足 $a_{i+i}|a_i, i=1, 2, \cdots$，

则存在某个 n，使得 $a_n \sim a_{n+1} \sim a_{n+2} \sim \cdots$，这里“~”表示元素相伴;

(2)R 中的不可约元是素元，

证: 若 R 是唯一分解整环，则 R 中每个非零元素的真因子个数是有限的

(可逆元的真因子个数为零)，

所以不可能出现满足 a_{i+1} 是 $a_i (i=1, 2, \cdots)$ 的真因子的无穷元素列 $a_1, a_2, \cdots, a_n, \cdots$

因此(1)成立，

下面证明条件(2)成立，

设属于 R 的 c 是不可约元，欲证 c 是素元，仅需证从 c|ab，能得到 c|a 或 c|b，

我们分几种情形讨论，

情形 1，若 a=0 或 b=0，则 c|a 或 c|b，

情形 2，若 a 是可逆元或 b 是可逆元，则 c|b 或 c|a，

情形 3，若 a, b 属于$\hat{R}$，则 a, b 在 R 中有唯一分解，

若令 $a=p_1p_2\cdots p_m, b=q_1q_2\cdots q_n$，其中 $p_1, p_2, \cdots, p_m, q_1, q_2, \cdots, q_n$ 是不可约元，

则 $c|p_1p_2\cdots p_mq_1q_2\cdots q_n$,

根据推论 7.1 可知，存在某个 $p_i (i=1, 2, \cdots, m)$ 或某个 $q_i (j=1, 2, \cdots, n)$，

使得 $c \sim p_i$ 或者 $c \sim q_j$, 于是 c|a 或 c|b，

综上，c 是素元，

反之，若整环 R 满足条件(1)和(2)，我们来证明 R 是唯一分解整环，

首先说明对属于$\hat{R}$的任意元素 a，都有不可约元 p，使得 p|a，

如果 a 是不可约元，则取 p=a，若 a 是可约元，则 a 有真因子

设 a_1 是 a 的真因子，如果 a_1 是不可约元，则取 $p=a_1$，否则，a_1 有真因子，

设 a_2 是 a_1 的真因子，……，继续这个过程，

则有一个元素列 $a, a_1, a_2, \cdots$，满足 $a_1|a, a_{i+1}|a_i, i=1, 2, \cdots$，

至此，由条件(1)，这个元素列一定终止于某个 a_n, 并且 a_n 是不可约元，$a_n|a$，

进而，我们说明分解式的存在性，

令 p_1 是不可约元且 $a=p_1b$，令 p_2 是不可约元且 $b=p_2c$，

对元素 c 重复上面的过程，有 $c=p_3d, a=p_1p_2p_3d, \cdots$，

再由(1)，此过程也不可能无限进行下去，它必定终止于有限步，

即存在 $a=p_1p_2\cdots p_n$，其中 $p_1, p_2, \cdots, p_n$ 是不可约元，

最后，我们指出分解式的唯一性，

令 $a=p_1p_2\cdots p_n=q_1q_2\cdots q_m$，这里每个 p_i, q_j 都是不可约元，

进而由条件(2)，p_i, q_j 都是素元，

不妨设 $n\leqslant m$，因为 p_1 是素元，所以由 $p_1|q_1q_2\cdots q_m$ 可知，存在 q_j 使得 $p_1|q_j$，

因此，不妨假设 $p_1|q_1$，由于 p_1, q_1 都是不可约元，所以，$p_1\sim q_1$，

于是存在属于 U(R)的 u_1，使得 $p_1=u_1q_1$，由整环的消去律得 $u_1p_2\cdots p_n=q_2\cdots q_m$，

又由命题 7.3，u_1p_2 是不可约元，那么类似地有，$u_1p_2\sim q_2$，

进而，存在属于 U(R)的 u_2，使得 $u_1p_2=u_2q_2$，

再由整环的消去律得 $u_2p_3\cdots p_n=q_3\cdots q_m$，

继续这个过程，……，

若 $n<m$，则存在属于 U(R)的 u_n 使得 $u_n=q_{n+1}\cdots q_m$，从而 q_{n+1} 是可逆元，矛盾，

所以，一定有 $n=m$，并且 $p_i\sim q_i, 1\leqslant i\leqslant n=m$

注意，利用定理 7.1 可以断定整环 $Z[\sqrt{-3}]$不是唯一分解整环，

但有一类非常重要的环: 主理想整环确是唯一分解整环，

引理 7.2 在主理想整环 R 中，不可约元与素元是等价的，

证: 由命题 7.5 可知，素元一定是不可约元，

因此，我们仅需证明 R 中的不可约元是素元，

令 p 是不可约元，如果$\langle p\rangle$是极大理想，则由本章定理 5.3 可知，$\langle p\rangle$是素理想

那么再由命题 7.4 可知，p 是素元，

为此，下面我们证明$\langle p\rangle$是极大理想，

假设存在 R 的一个理想 $I=\langle a\rangle$满足$\langle p\rangle$包含于$\langle a\rangle$，则 $a|p$，

但是 p 是不可约元，所以 a 是可逆元或 $a\sim p$，

若 a 是可逆元，则 I=R，若 $a\sim p$，则$\langle a\rangle=\langle p\rangle$，这就是说，$\langle p\rangle$是极大理想

定理 7.2 主理想整环 R 是唯一分解整环 ，

证: 我们只需验证 R 满足定理 7.1 中的条件(1)和(2)，

又根据引理 7.2 可知 ，条件(2)已经满足 ，下面证明条件(1)成立 ，

为此 ，若任取元素列 $a_1, a_2, a_3, \cdots, a_n \cdots$，其中 $a_{i+1} | a_i, i=1, 2, \cdots$，

则存在对应的主理想列$\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \langle a_3\rangle \subseteq \cdots \subseteq \langle a_n\rangle \subseteq \cdots$

现在, 令 $N = \bigcup_{i\in I} \langle a_i\rangle$, 则 N 是环 R 的理想

由于 R 是主理想整环 ，因此 ，不妨令 $N=\langle a\rangle$，那么存在 n，使得$\langle a\rangle$包含于$\langle a_n\rangle$，

而$\langle a_n\rangle$是包含于$\langle a\rangle$的 ，所以$\langle a\rangle=\langle a_n\rangle$，

从而对属于 Z^+的任意 k 有$\langle a\rangle=\langle a_n\rangle \subseteq \langle a_{n+k}\rangle \subseteq \langle a\rangle$，$\langle a_n\rangle=\langle a_{n+k}\rangle$，即条件(1)满足 ，

定义 7.6 设 R 是整环 ，若 R 中的每一个非零元 a 都对应一个非负整数$\delta(a)$，

并且 R 中任意元素 b 都可以写作 $b=aq+r$，q，r 属于 R，$r=0$ 或$\delta(r)<\delta(a)$，

则称 R 是欧几里得整环 ，简称欧氏环 ，

若在整数环 Z 中 ，令$\delta(a)=|a|$(a 属于 Z)，

在数域 F 上的一元多项式环 F[x]中 ，令$\delta(f(x))=\deg f(x)$ (f(x)属于 F[x])，

则可知 Z 和 F[x]都是欧氏环 ，

例 7.7 证明高斯整环 Z[i]是欧氏环 ，

证: 事实上 ，对属于 Z[i]的$\alpha=a+bi$，可令$\delta(x)=a^2+b^2$，即$\delta(\alpha)=N(\alpha)$，

因此 ，对任意$\alpha=a+bi$，$\beta=c+di$，为求 q，r 使得$\alpha=\beta q+r$，

可以考虑: $\alpha\beta^{-1}=s+ti$，其中 $s=\frac{ac+bd}{c^2+d^2}=\frac{ac+bd}{\delta(\beta)}$，$t=\frac{bc-ad}{\delta(\beta)}$

然后再取 s'，t'属于 Z，使得$|s-s'|\leqslant\frac{1}{2}$，$|t-t'|\leqslant\frac{1}{2}$，

那么若令 $q=s'+t'i$，$r=\alpha-\beta q$，则有 q，r 属于 Z[i]，而且$\alpha=\beta q+r$，

现在 ，我们只需证明 $r=0$ 或$\delta(r)<\delta(\beta)$，但若 $r=0$，则结论已成立 ，

若 $r\neq 0$，则$\delta(r)=\delta(\alpha-\beta q)=\delta(\beta(\alpha\beta^{1}-q))=\delta(\beta)\delta(\alpha\beta^{-1}-q)$

$=\delta(\beta)\delta(s-s'+ti-t'i)=\delta(\beta)[(s-s')^2+(t-t')^2]$

$\leqslant\delta(\beta)\left[\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2\right]<\delta(\beta)$，即 Z[i]是欧氏环 ，

定理 7.3 欧氏环是主理想整环，

证: 设 R 是欧氏环，I 是 R 的任意一个理想，若 I={0}，则 I=⟨0⟩是主理想;

若 I≠{0}，则由欧氏环的定义，对 I 的每一个非零元 a 都有一个非负整数δ(a)，

从而存在非负整数的子集合{δ(a)|a∈I，a≠0}，

于是存在属于 I 的非零元 b 使得δ(b)=min{δ(a)|a∈I，a≠0}，

进而，对属于 I 的任意 c，有 c=bq+r，r=0 或δ(r)＜δ(b)，

那么由属于 I 的 r=c−b 及 b 的取法可知，r=0，即 c=bq，c 属于⟨b⟩，I=⟨b⟩，

于是，I 是 R 的主理想，

现在，我们已经知道: 欧氏环是主理想整环，主理想整环是唯一分解整环，

但是，它们的逆命题都不成立，

例如，Z[x]是唯一分解整环，但不是主理想整环，

还有$\left\{a+\frac{b}{2}\left(1+\sqrt{-19}\right)\middle|\, a,b\in Z\right\}$是主理想整环，但不是欧氏环，