Lemma：域中没有素元．域中没有不可约元．

Proof：设 $(R,+,\cdot,0_R,1_R)$ 是域．

$\because R$ 是域 $\quad\therefore R$ 是整环

对 $\forall\, p\in R$，

若 $p=0_R$，则 p 不是素元，也不是不可约元．

若 $p\neq 0_R$，则 $p\in R\setminus\{0_R\}$ $\quad\because R$ 是域 $\quad\therefore R$ 是除环

$\therefore R^\times = R\setminus\{0_R\}$ $\quad\therefore p\in R^\times$

$\therefore p$ 不是素元，也不是不可约元．

$\therefore$ 域中没有素元，也没有不可约元． $\square$

思考：整环中存在素元的充要条件是什么？

整环中存在不可约元的充要条件是什么？

Lemma：R 是唯一分解环，对 $\forall\, r,s\in R\setminus\{0_R\}$，有：$\gcd(r,s)\in R\setminus\{0_R\}$，$\operatorname{lcm}(r,s)\in R\setminus\{0_R\}$．

Proof：$\because r,s\in R\setminus\{0_R\}$ $\quad\therefore \exists\, n\in\mathbb{Z}_{\geq 0}$ 和不可约元 $p_1,\cdots,p_n\in R$，s.t.

$r\sim\prod\limits_{i=1}^{n}p_i^{a_i}$，$s\sim\prod\limits_{i=1}^{n}p_i^{b_i}$，其中对 $\forall\, i=1,\cdots,n$，有 $a_i,b_i\in\mathbb{Z}_{\geq 0}$ 且 a_i,b_i 不同时为 0

$\therefore \gcd(r,s)\sim\prod\limits_{i=1}^{n}p_i^{\min\{a_i,b_i\}}$，$\cancel{\operatorname{lcm}\sim\prod\limits_{i=1}^{n}p_i^{\max\{a_i,b_i\}}}$ $\operatorname{lcm}(r,s)\sim\prod\limits_{i=1}^{n}p_i^{\max\{a_i,b_i\}}$

$\therefore \exists\,\lambda\in R^\times$，s.t. $\gcd(r,s)=\lambda\prod\limits_{i=1}^{n}p_i^{\min\{a_i,b_i\}}\in R$

$\exists\,\mu\in R^\times$，s.t. $\operatorname{lcm}(r,s)=\mu\prod\limits_{i=1}^{n}p_i^{\max\{a_i,b_i\}}\in R$

对 $\forall i=1,\cdots,n$ ，$\because p_i \in R$ 是不可约元 $\therefore p_i \neq 0_R$

$\therefore p_i^{\min\{a_i, b_i\}} \in R$ 且 $p_i^{\min\{a_i, b_i\}} \neq 0_R$

$p_i^{\max\{a_i, b_i\}} \in R$ 且 $p_i^{\max\{a_i, b_i\}} \neq 0_R$

$\therefore \prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}} \neq 0_R$ ，$\prod_{i=1}^{n} p_i^{\max\{a_i, b_i\}} \neq 0_R$

$\because \lambda, \mu \in R^{\times}$ ，R 是非零环 ，$\therefore \lambda, \mu \in R \setminus \{0_R\}$

$\therefore \lambda \prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}} \neq 0_R$ ，$\mu \prod_{i=1}^{n} p_i^{\max\{a_i, b_i\}} \neq 0_R$

$\therefore \gcd(r, s) \in R \setminus \{0_R\}$ ，$\operatorname{lcm}(r, s) \in R \setminus \{0_R\}$. $\square$

Lemma：R是整环，$p\in R$，p是R的素元，则p是不可约元.

Proof：$\because$ p是R的素元 $\therefore p\in R$，$p\neq 0_R$，$p\notin R^\times$

对$\forall a\in R$，若$a\mid p$，则有：

$\because a\mid p$ $\therefore \exists d\in R$，s.t. $p=da$ $\quad\therefore p=ad$

$\cancel{\therefore p=ad=1_R\cdot(ad)}$ $\quad\equiv\ \because ad=p=1_R\cdot p$ $\quad\therefore p\mid ad$

$\because a\in R$，$d\in R$，$p\mid ad$，p是素元 $\quad\therefore p\mid a$或$p\mid d$

若$p\mid a$，则有$a\mid p$且$p\mid a$ $\quad\therefore a\sim p$

若$p\mid d$，则有：$\because a\in R$且$p=ad$ $\quad\therefore d\mid p$

$\because p\mid d$且$d\mid p$ $\quad\therefore p\sim d$ $\quad\therefore \exists r\in R^\times$，s.t. $p=rd$

$\therefore ad=p=rd$.

假设$d=0_R$，则有：$p=ad=a\cdot 0_R=0_R$. 矛盾. $\quad\therefore d\neq 0_R$

$\because a\in R$，$r\in R^\times$，$d\in R$，$d\neq 0_R$，$ad=rd$ $\quad\therefore a=r$

$\therefore a=r=r\cdot 1_R$，$r\in R^\times$ $\quad\therefore a\sim 1_R$

$\therefore a\sim p$或$a\sim 1_R$ $\quad\therefore p$是不可约元. $\square$

定义（唯一分解环，唯一析因整环，UFD）R是整环，若对$\forall r\in R$且$r\neq 0_R$，以下两个条件都成立：

① $\exists n\in\mathbb{Z}_{\geq 0}$和不可约元$p_1,\cdots,p_n\in R$，s.t. $r\sim p_1\cdots p_n$（若$n=0$，则$r\sim 1_R$）

② 若还有不可约元$q_1,\cdots,q_m\in R$，s.t. $r\sim q_1\cdots q_m$，则有$m=n$，且$\exists\sigma\in \mathfrak{S}_n$，s.t. 对$\forall i=1,\cdots,n$，都有$p_i\sim q_{\sigma(i)}$

则称R是唯一分解环，也称R是唯一析因整环.

定义(唯一分解环，唯一析因整环，另一种表述) R 是整环，若对 $\forall r\in R$ 且 $r\neq 0_R$，以下两个条件都成立：

① $\exists n\in\mathbb{Z}_{\geqslant 0}$ 和不可约元 $p_1,\cdots,p_n\in R$，s.t. $r\sim p_1\cdots p_n$ (若 $n=0$，则 $r\sim 1_R$)

② 若还 $\exists m\in\mathbb{Z}_{\geqslant 0}$ 和不可约元 $q_1,\cdots,q_m\in R$，s.t. $r\sim q_1\cdots q_m$，则有 $m=n$，

且 $\exists\sigma\in\mathfrak{S}_n$，s.t. 对 $\forall i=1,\cdots,n$，都有 $p_i\sim q_{\sigma(i)}$

则称 R 是唯一分解环，也称 R 是唯一析因整环.

Lemma：域是唯一分解环

Proof：设 $(R,+,\cdot,0_R,1_R)$ 是域.

$\because R$ 是域 $\quad\therefore R$ 是整环.

对 $\forall r\in R$ 且 $r\neq 0_R$，$\because R$ 是域 $\quad\therefore R$ 是除环 $\quad\therefore R^\times=R\setminus\{0_R\}$

$\therefore r\in R^\times \quad \because r=r\cdot 1_R$，$r\in R^\times \quad\therefore r\sim 1_R$

$\therefore\exists n=0$ 和不可约元 $p_1,\cdots,p_n\in R$，s.t. $r\sim p_1\cdots p_n$. 条件①满足.

若还 $\exists m\in\mathbb{Z}_{\geqslant 0}$ 和不可约元 $q_1,\cdots,q_m\in R$，s.t. $r\sim q_1\cdots q_m$，则有：

$\because R$ 是域 $\quad\therefore R$ 中没有不可约元 $\quad\therefore m=0 \quad\therefore r\sim 1_R \quad\therefore m=0=n$

条件②满足

$\therefore R$ 是唯一分解环.

$\therefore$ 域是唯一分解环. $\square$

定义（唯一分解环中的最大公因数和最小公倍数）R是唯一分解环

对$\forall\ r,s\in R\setminus\{0_R\}$，$\exists\ n\in\mathbb{Z}_{\geq 0}$和不可约元$p_1,\cdots,p_n\in R$，s.t.

$$r\sim\prod_{i=1}^{n}p_i^{a_i}\qquad s\sim\prod_{i=1}^{n}p_i^{b_i}$$

对$\forall\ i=1,\cdots,n$，有：$a_i,b_i\in\mathbb{Z}_{\geq 0}$

且a_i,b_i不同时为0

（如果某个不可约元$p_i\in R$只出现在r的分解式中，则令$b_i=0$即可.

如果某个不可约元$p_i\in R$只出现在s的分解式中，则令$a_i=0$即可.）

定义r和s的最大公因数为：

$$\gcd(r,s)\sim\prod_{i=1}^{n}p_i^{\min\{a_i,b_i\}}\qquad(\gcd(r,s)\in R)$$

定义r和s的最小公倍数为：

$$\operatorname{lcm}(r,s)\sim\prod_{i=1}^{n}p_i^{\max\{a_i,b_i\}}\qquad(\operatorname{lcm}(r,s)\in R)$$

$\gcd(r,s)$和$\operatorname{lcm}(r,s)$实际上是R对$\sim$的一个等价类

定义（唯一分解环中的互素）R是唯一分解环，$r_1,\cdots,r_n\in R\setminus\{0_R\}$，

若$\gcd(r_1,\cdots,r_n)\sim 1_R$，则称$r_1,\cdots,r_n$互素.

Lemma（既约分式）R为唯一分解环，$h\in \mathrm{Frac}(R)\setminus\{0_{\mathrm{Frac}(R)}\}$，则存在

$f,g\in R$，s.t. $g\neq 0_R$且f和g互素，且$h=\dfrac{f}{g}$.

（这般分式$\dfrac{f}{g}$称为既约分式）

Proof：$\because h\in\mathrm{Frac}(R)$　$\therefore\exists\ \alpha\in R$且$\beta\in R$且$\beta\neq 0_R$，s.t. $h=\dfrac{\alpha}{\beta}$

$\because h\neq 0_{\mathrm{Frac}(R)}$　$\therefore\alpha\neq 0_R$　$\therefore\alpha,\beta\in R\setminus\{0_R\}$

$\because R$是唯一分解环，$\alpha, \beta \in R\backslash\{0_R\}$

$\therefore \exists n \in \mathbb{Z}_{\geqslant 0}$ 和不可约元 $p_1, \cdots, p_n \in R$，s.t.

$\alpha \sim \prod_{i=1}^{n} p_i^{a_i}$，$\beta \sim \prod_{i=1}^{n} p_i^{b_i}$，对$\forall i=1,\cdots,n$，有：$a_i, b_i \in \mathbb{Z}_{\geqslant 0}$ 且 a_i, b_i 不同时为0.

$\therefore \gcd(\alpha, \beta) \sim \prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}}$

$\because \alpha \sim \prod_{i=1}^{n} p_i^{a_i}$ $\quad \therefore \exists \lambda \in R^{\times}$，s.t. $\alpha = \lambda \prod_{i=1}^{n} p_i^{a_i}$

$\because \beta \sim \prod_{i=1}^{n} p_i^{b_i}$ $\quad \therefore \exists \mu \in R^{\times}$，s.t. $\beta = \mu \prod_{i=1}^{n} p_i^{b_i}$

$\because \gcd(\alpha, \beta) \sim \prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}}$ $\quad \therefore \exists \gamma \in R^{\times}$，s.t. $\gcd(\alpha, \beta) = \gamma \prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}}$

$$\therefore h = \frac{\alpha}{\beta} = \frac{\lambda \prod_{i=1}^{n} p_i^{a_i}}{\mu \prod_{i=1}^{n} p_i^{b_i}} = \frac{\lambda \prod_{i=1}^{n} p_i^{a_i - \min\{a_i, b_i\}} \cdot \prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}}}{\mu \prod_{i=1}^{n} p_i^{b_i - \min\{a_i, b_i\}} \cdot \prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}}}$$

$$= \frac{\lambda \gamma^{-1} \prod_{i=1}^{n} p_i^{a_i - \min\{a_i, b_i\}} \gamma \prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}}}{\mu \gamma^{-1} \prod_{i=1}^{n} p_i^{b_i - \min\{a_i, b_i\}} \gamma \prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}}} = \frac{\lambda \gamma^{-1} \prod_{i=1}^{n} p_i^{a_i - \min\{a_i, b_i\}} \cdot \gcd(\alpha, \beta)}{\mu \gamma^{-1} \prod_{i=1}^{n} p_i^{b_i - \min\{a_i, b_i\}} \cdot \gcd(\alpha, \beta)}$$

$$= \frac{\lambda \prod_{i=1}^{n} p_i^{a_i - \min\{a_i, b_i\}}}{\mu \prod_{i=1}^{n} p_i^{b_i - \min\{a_i, b_i\}}}$$

令 $f = \lambda \prod_{i=1}^{n} p_i^{a_i - \min\{a_i, b_i\}}$，$g = \mu \prod_{i=1}^{n} p_i^{b_i - \min\{a_i, b_i\}}$ $\quad \therefore f, g \in R\backslash\{0_R\}$

$\because \lambda, \mu \in R^{\times}$ $\quad \therefore f \sim \prod_{i=1}^{n} p_i^{a_i - \min\{a_i, b_i\}}$，$g \sim \prod_{i=1}^{n} p_i^{b_i - \min\{a_i, b_i\}}$

$\therefore \gcd(f, g) \sim \prod_{i=1}^{n} p_i^{\min\{a_i - \min\{a_i, b_i\},\ b_i - \min\{a_i, b_i\}\}} = \prod_{i=1}^{n} p_i^{0} = \prod_{i=1}^{n} 1_R = 1_R$

$\therefore$ f和g互素

$\therefore$ $f, g \in R \setminus \{0_R\}$，$f$和$g$互素，$h = \dfrac{f}{g}$ $\square$