Lemma: R是唯一分解环，$r\in R$且$r\neq 0_R$，则$\exists\, n\in\mathbb{Z}_{\geqslant 0}$和不可约元$p_1,\cdots,p_n\in R$，s.t. $r\sim p_1^{a_1}\cdots p_n^{a_n}$（其中$p_1,\cdots,p_n$彼此不同，$a_1,\cdots,a_n\in\mathbb{Z}_{\geqslant 0}$）

对$\forall\, d\in R$且$d\neq 0_R$，有：

$$d\mid r \iff d\sim p_1^{e_1}\cdots p_n^{e_n}$$，其中$e_1,\cdots,e_n\in\mathbb{Z}_{\geqslant 0}$，$e_1\leqslant a_1,\cdots,e_n\leqslant a_n$.

Proof: ($\Leftarrow$): $\because d\sim p_1^{e_1}\cdots p_n^{e_n}$，其中$e_1,\cdots,e_n\in\mathbb{Z}_{\geqslant 0}$，$e_1\leqslant a_1,\cdots,e_n\leqslant a_n$

$\therefore \exists\,\lambda\in R^\times$，s.t. $d=\lambda p_1^{e_1}\cdots p_n^{e_n}$

$\because e_1,\cdots,e_n\in\mathbb{Z}_{\geqslant 0}$，$a_1,\cdots,a_n\in\mathbb{Z}_{\geqslant 0}$，$e_1\leqslant a_1,\cdots,e_n\leqslant a_n$

$\therefore a_1-e_1\in\mathbb{Z}_{\geqslant 0},\cdots,a_n-e_n\in\mathbb{Z}_{\geqslant 0}$　$\therefore p_1^{a_1-e_1}\cdots p_n^{a_n-e_n}\in R$

$\because r\sim p_1^{a_1}\cdots p_n^{a_n}$　$\therefore \exists\,\mu\in R^\times$，s.t. $r=\mu p_1^{a_1}\cdots p_n^{a_n}$

$\because \lambda^{-1}\mu p_1^{a_1-e_1}\cdots p_n^{a_n-e_n}\in R$，且

$$\left(\lambda^{-1}\mu p_1^{a_1-e_1}\cdots p_n^{a_n-e_n}\right)\cdot d=\left(\lambda^{-1}\mu p_1^{a_1-e_1}\cdots p_n^{a_n-e_n}\right)\left(\lambda p_1^{e_1}\cdots p_n^{e_n}\right)$$

$$=\mu p_1^{a_1}\cdots p_n^{a_n}=r$$

$\therefore d\mid r$

($\Rightarrow$): $\because r\in R$，$d\in R$，$d\mid r$　$\therefore \exists\, k\in R$，s.t. $r=kd$.

假设$k=0_R$，则有：$r=kd=0_R\cdot d=0_R$　矛盾.　$\therefore k\neq 0_R$　$\therefore k\in R\setminus\{0_R\}$.

$\because R$是唯一分解环，$k\in R\setminus\{0_R\}$，$d\in R\setminus\{0_R\}$.　$\alpha_1,\cdots,\alpha_s$彼此不同，$\beta_1,\cdots,\beta_t$彼此不同

$\therefore \exists\, s,t\in\mathbb{Z}_{\geqslant 0}$和不可约元$\alpha_1,\cdots,\alpha_s\in R$，$\beta_1,\cdots,\beta_t\in R$，s.t.

$k\sim\alpha_1^{b_1}\cdots\alpha_s^{b_s}$，$d\sim\beta_1^{c_1}\cdots\beta_t^{c_t}$（其中$b_1,\cdots,b_s,c_1,\cdots,c_t\in\mathbb{Z}_{\geqslant 0}$）

$\therefore \exists\,\gamma,\delta\in R^\times$，s.t. $k=\gamma\alpha_1^{b_1}\cdots\alpha_s^{b_s}$，$d=\delta\beta_1^{c_1}\cdots\beta_t^{c_t}$.

$\therefore r=kd=\gamma\delta\alpha_1^{b_1}\cdots\alpha_s^{b_s}\beta_1^{c_1}\cdots\beta_t^{c_t}$　$\therefore r\sim\alpha_1^{b_1}\cdots\alpha_s^{b_s}\beta_1^{c_1}\cdots\beta_t^{c_t}$

$\because r \sim p_1^{a_1} \cdots p_n^{a_n}$ ，其中 $a_1, \cdots, a_n \in \mathbb{Z}_{\geq 0}$

$r \sim \alpha_1^{b_1} \cdots \alpha_s^{b_s} \beta_1^{c_1} \cdots \beta_t^{c_t}$ ，其中 $b_1, \cdots, b_s$ ， $c_1, \cdots, c_t \in \mathbb{Z}_{\geq 0}$

$\therefore$ $t \leq n$ ，且 $\exists \sigma \in \mathfrak{S}_n$ ， s.t. 对 $\forall i = 1, \cdots, t$ ，都有 $\beta_i \sim p_{\sigma(i)}$ 且 $c_i \leq a_{\sigma(i)}$ （如果 $\alpha_1, \cdots, \alpha_s$ 中没有与 $p_{\sigma(i)}$ 相伴的元，则 $c_i = a_{\sigma(i)}$ ）

$\therefore \beta_1^{c_1} \cdots \beta_t^{c_t} \sim p_{\sigma(1)}^{c_1} \cdots p_{\sigma(t)}^{c_t}$ $\therefore \alpha \sim p_{\sigma(1)}^{c_1} \cdots p_{\sigma(t)}^{c_t}$ ，其中 $t \in \mathbb{Z}_{\geq 0}$ 且 $t \leq n$

$\therefore \alpha \sim p_{\sigma(1)}^{c_1} \cdots p_{\sigma(t)}^{c_t}$ ， $t \in \mathbb{Z}_{\geq 0}$ 且 $t \leq n$ ， $c_1 \leq a_{\sigma(1)}$ ， $\cdots$ ， $c_t \leq a_{\sigma(t)}$ □

Lemma：R 是唯一分解环， $\lambda, a, b \in R \setminus \{0_R\}$ ， $\gcd(\lambda, a) \sim 1_R$ ，则有： $\gcd(\lambda, ab) \sim \gcd(\lambda, b)$

Proof：$\because R$ 是唯一分解环， $\lambda, a, b \in R \setminus \{0_R\}$ ，

$\therefore \exists n \in \mathbb{Z}_{\geq 0}$ 和不可约元 $p_1, \cdots, p_n \in R$ （$p_1, \cdots, p_n$ 彼此不同）， s.t.

$\lambda \sim \prod_{i=1}^{n} p_i^{c_i}$ （对 $\forall i = 1, \cdots, n$ ，有： $c_i \in \mathbb{Z}_{\geq 0}$ ）

$a \sim \prod_{i=1}^{n} p_i^{a_i}$ （对 $\forall i = 1, \cdots, n$ ，有： $a_i \in \mathbb{Z}_{\geq 0}$ ）

$b \sim \prod_{i=1}^{n} p_i^{b_i}$ （对 $\forall i = 1, \cdots, n$ ，有： $b_i \in \mathbb{Z}_{\geq 0}$ ）

（对 $\forall i = 1, \cdots, n$ ， a_i, b_i, c_i 不同时为 0 ，如果某个 p_i 只出现在 a 的分解式中，则 $b_i = c_i = 0$ 即可）

$\therefore \gcd(\lambda, a) \sim \prod_{i=1}^{n} p_i^{\min\{c_i, a_i\}}$ $\because \gcd(\lambda, a) \sim 1_R$

$\therefore \prod_{i=1}^{n} p_i^{\min\{c_i, a_i\}} \sim 1_R$ $\therefore \prod_{i=1}^{n} p_i^{\min\{c_i, a_i\}} \sim \prod_{i=1}^{n} p_i^{0}$

$\therefore$ 对 $\forall i = 1, \cdots, n$ ，有： $\min\{c_i, a_i\} = 0$

(如果某个 $\min\{c_i, a_i\} \in \mathbb{Z}_{\geq 1}$，则 $p_i \sim 1_R$ ∴ 事 $p_i \in R^\times$ 矛盾.)

$\because ab \sim \prod_{i=1}^{n} p_i^{a_i+b_i}$

$\therefore \gcd(\lambda, ab) \sim \prod_{i=1}^{n} p_i^{\min\{c_i, a_i+b_i\}}$, $\gcd(\lambda, b) \sim \prod_{i=1}^{n} p_i^{\min\{c_i, b_i\}}$

对 $\forall i=1, \cdots, n$.

若 $\min\{c_i, a_i\} = c_i$，则 $c_i = 0$. ∴ $\min\{c_i, a_i+b_i\} = \min\{0, a_i+b_i\} = 0$

$\min\{c_i, b_i\} = \min\{0, b_i\} = 0$ ∴ $\min\{c_i, a_i+b_i\} = 0 = \min\{c_i, b_i\}$

若 $\min\{c_i, a_i\} = a_i$，则 $a_i = 0$ ∴ $\min\{c_i, a_i+b_i\} = \min\{c_i, 0+b_i\} = \min\{c_i, b_i\}$

∴ 对 $\forall i=1, \cdots, n$，有：$\min\{c_i, a_i+b_i\} = \min\{c_i, b_i\}$

$\therefore \prod_{i=1}^{n} p_i^{\min\{c_i, a_i+b_i\}} = \prod_{i=1}^{n} p_i^{\min\{c_i, b_i\}}$ ∴ $\gcd(\lambda, ab) \sim \gcd(\lambda, b)$ □

Lemma：R 是唯一分解环，$\lambda, a, b \in R \setminus \{0_R\}$，$\gcd(\lambda, a) \sim 1_R$，$\lambda \mid ab$，则有：$\lambda \mid b$

Proof：∵ R 是唯一分解环，$\lambda, a, b \in R \setminus \{0_R\}$

∴ $\exists n \in \mathbb{Z}_{\geq 0}$ 和不可约元 $p_1, \cdots, p_n \in R$（$p_1, \cdots, p_n$ 彼此不同），s.t.

$\lambda \sim \prod_{i=1}^{n} p_i^{c_i}$ （对 $\forall i=1, \cdots, n$，有：$c_i \in \mathbb{Z}_{\geq 0}$）.

$a \sim \prod_{i=1}^{n} p_i^{a_i}$ （对 $\forall i=1, \cdots, n$，有：$a_i \in \mathbb{Z}_{\geq 0}$）

$b \sim \prod_{i=1}^{n} p_i^{b_i}$ （对 $\forall i=1, \cdots, n$，有：$b_i \in \mathbb{Z}_{\geq 0}$）（对 $\forall i=1, \cdots, n$，a_i, b_i, c_i 不同时为 0）

∴ $ab \sim \prod_{i=1}^{n} p_i^{a_i+b_i}$ ∵ $\lambda \mid ab$ ∴ 对 $\forall i=1, \cdots, n$，有：$c_i \leq a_i+b_i$

∵ $\gcd(\lambda, a) \sim \prod_{i=1}^{n} p_i^{\min\{c_i, a_i\}}$ ∴ $\prod_{i=1}^{n} p_i^{\min\{c_i, a_i\}} \sim \prod_{i=1}^{n} p_i^{0}$

$\therefore$ 对 $\forall i=1,\cdots,n$，有：$\min\{c_i,a_i\}=0$

（若某个 $\min\{c_i,a_i\}\in\mathbb{Z}_{\geq 1}$，则 $p_i\sim 1_R$ $\therefore p_i\in R^\times$ 矛盾）

对 $\forall i=1,\cdots,n$，

若 $\min\{c_i,a_i\}=c_i$，则 $c_i=0$ $\therefore$ $c_i=0\leq b_i$

若 $\min\{c_i,a_i\}=a_i$，则 $a_i=0$ $\therefore$ $c_i\leq a_i+b_i=0+b_i=b_i$

$\therefore$ 对 $\forall i=1,\cdots,n$，有：$c_i\leq b_i$ $\therefore a\mid b$. □

Lemma（既约分式的极小性）R 为唯一分解环，$h\in \mathrm{Frac}(R)\setminus\{0_{\mathrm{Frac}(R)}\}$，已经证明了存在 $f,g\in R$，s.t. $g\neq 0_R$ 且 f 和 g 互素，且 $h=\frac{f}{g}$.

若 $f_1,g_1\in R$ 也满足 $g_1\neq 0_R$ 且 $h=\frac{f_1}{g_1}$，则 $f\mid f_1$ 且 $g\mid g_1$

Proof: $\because f,g,f_1,g_1\in R$ 且 $\frac{f}{g}=h=\frac{f_1}{g_1}$

$\therefore fg_1=f_1g$ $\because f_1g=g_1f$ $\therefore f\mid gf_1$

假设 $f=0_R$，则有：$h=\frac{f}{g}=\frac{0_R}{g}=0_{\mathrm{Frac}(R)}$ 矛盾. $\therefore f\neq 0_R$ $\therefore f\in R\setminus\{0_R\}$

假设 $f_1=0_R$，则有：$h=\frac{f_1}{g_1}=\frac{0_R}{g_1}=0_{\mathrm{Frac}(R)}$ 矛盾. $\therefore f_1\neq 0_R$ $\therefore f_1\in R\setminus\{0_R\}$

$\because f,g,f_1\in R\setminus\{0_R\}$. $\gcd(f,g)\sim 1_R$，$f\mid gf_1$ $\therefore f\mid f_1$

$\because fg_1=f_1g$ $\therefore g\mid fg_1$

$\because g,f,g_1\in R\setminus\{0_R\}$，$\gcd(g,f)\sim 1_R$，$g\mid fg_1$ $\therefore g\mid g_1$

$\therefore f\mid f_1$ 且 $g\mid g_1$ □

Lemma (既约分式的唯一性) R 是唯一分解环，$h \in Frac(R) \setminus \{0_{Frac(R)}\}$，已经证明了存在 $f, g \in R$, s.t. $g \neq 0_R$ 且 f 和 g 互素，且 $h = \frac{f}{g}$.

若还存在 $f_1, g_1 \in R$, s.t. $g_1 \neq 0_R$ 且 f_1 和 g_1 互素，且 $h = \frac{f_1}{g_1}$

则有：$f \sim f_1$ 且 $g \sim g_1$.

Proof: 由上一引理：$f | f_1$ 且 $g | g_1$

$\because f_1, g_1 \in R$, $g_1 \neq 0_R$, f_1 和 g_1 互素，$h = \frac{f_1}{g_1}$

$f, g \in R$, $g \neq 0_R$, $h = \frac{f}{g}$ $\therefore f_1 | f$ 且 $g_1 | g$

$\because f \in R, f_1 \in R$, $f | f_1$ 且 $f_1 | f$ $\therefore f \sim f_1$

$\because g \in R, g_1 \in R$, $g | g_1$ 且 $g_1 | g$ $\therefore g \sim g_1$ □