Lemma: R是整环，则有: $\mathrm{char}(R) \neq 1$

Proof: $\because$ R是整环 $\therefore$ $\mathrm{char}(R) \in \mathbb{Z}_{\geq 0}$，且对$\forall n \in \mathbb{Z}$，都有

$n \cdot 1_R = 0_R \iff \mathrm{char}(R) \mid n$

假设 $\mathrm{char}(R) = 1$，则有: 对于 $1 \in \mathbb{Z}$

$\because$ $\mathrm{char}(R) = 1$ $\therefore$ $\mathrm{char}(R) \mid 1$ $\therefore$ $1 \cdot 1_R = 0_R$

$\therefore$ $1_R = 0_R$ $\because$ R是整环 $\therefore$ R是非零环 $\therefore$ $1_R \neq 0_R$

矛盾. $\therefore$ $\mathrm{char}(R) \neq 1$ $\square$

域的特征

Lemma: R是一个任意的环，则有：存在唯一的环同态 $\mathbb{Z}\to R$.

Proof: 令 $f: \mathbb{Z} \longrightarrow R$

$$x \longmapsto x\cdot 1_R$$

对$\forall x\in\mathbb{Z}$，$f(x)=x\cdot 1_R\in R$ $\quad\therefore f(\mathbb{Z})\subseteq R$

对$\forall x_1, x_2\in\mathbb{Z}$，

若 $x_1=x_2$，则有：$f(x_1)=x_1\cdot 1_R=x_2\cdot 1_R=f(x_2)$

$\therefore f:\mathbb{Z}\longrightarrow R$是一个映射.

对$\forall x_1, x_2\in\mathbb{Z}$，

$$f(x_1+x_2)=(x_1+x_2)\cdot 1_R=x_1\cdot 1_R+x_2\cdot 1_R=f(x_1)+f(x_2)$$

$$f(x_1x_2)=\underbrace{(x_1x_2)}_{\text{整数和整数的乘法}}\cdot 1_R=x_1(x_2\cdot 1_R)=(x_1\cdot 1_R)(x_2\cdot 1_R)$$

$$=f(x_1)f(x_2)$$

$$f(1_{\mathbb{Z}})=f(\underbrace{1}_{\text{数“1”}})=1\cdot 1_R=1_R$$

$\therefore f:\mathbb{Z}\longrightarrow R$是环同态. 存在性得证.

假设 $\alpha:\mathbb{Z}\longrightarrow R$是环同态，$\beta:\mathbb{Z}\longrightarrow R$也是环同态. 则有：

$\alpha(1) = 1_R = \beta(1)$, $\alpha(0) = 0_R = \beta(0)$

对$\forall x \in \mathbb{Z}_{\geqslant 2}$，有：$\alpha(x) = \alpha(\underbrace{1+1+\cdots+1}_{x个1})$

$$= \underbrace{\alpha(1)+\alpha(1)+\cdots+\alpha(1)}_{x个\alpha(1)} = \underbrace{\beta(1)+\beta(1)+\cdots+\beta(1)}_{x个\beta(1)}$$

$$= \beta(\underbrace{1+1+\cdots+1}_{x个1}) = \beta(x)$$

$\alpha(-1) = -\alpha(1) = -\beta(1) = \beta(-1)$

对$\forall x \in \mathbb{Z}_{\leqslant -2}$，有：$x \in \mathbb{Z}$且$x \leq -2$ $\quad \therefore x = -(-x)$，$-x \geqslant 2$

$\therefore \alpha(x) = \alpha(-(-x)) = -\alpha(-x) = -\beta(-x) = \beta(-(-x))$
$= \beta(x)$

$\therefore$对$\forall x \in \mathbb{Z}$，有：$\alpha(x) = \beta(x)$

$\therefore \alpha = \beta$. 唯一性得证. $\square$

定义（$\mathbb{Z}$的子集K_R）R是一个任意的环，定义集合：

$$K_R = \{n \in \mathbb{Z} : n \cdot 1_R = 0_R\}$$

$\because 0 \in \mathbb{Z}$且$0 \cdot 1_R = 0_R$ $\quad \therefore 0 \in K_R$ $\quad \therefore K_R$是$\mathbb{Z}$的非空子集.

对$\forall x, y \in K_R$，有：

$\because x \in K_R$ $\quad \therefore x \in \mathbb{Z}$且$x \cdot 1_R = 0_R$

$\because y \in K_R$ $\quad \therefore y \in \mathbb{Z}$且$y \cdot 1_R = 0_R$

$\because x\in\mathbb{Z}$ 且 $y\in\mathbb{Z}$ $\quad\therefore x+y\in\mathbb{Z}$

$\because (x+y)\cdot 1_R = x\cdot 1_R + y\cdot 1_R = 0_R + 0_R = 0_R$

$\therefore x+y\in K_R$

对 $\forall a\in\mathbb{Z}$, $\forall x\in K_R$, 有:

$\because x\in K_R$ $\quad\therefore x\in\mathbb{Z}$ 且 $x\cdot 1_R = 0_R$

$\because a\in\mathbb{Z}$, $x\in\mathbb{Z}$ $\quad\therefore ax\in\mathbb{Z}$

$\because (ax)\cdot 1_R = a(x\cdot 1_R) = a\cdot 0_R = 0_R$

$\therefore ax\in K_R$

$\therefore$ 存在唯一的 $g\in\mathbb{Z}_{\geqslant 0}$, s.t. $K_R = g\mathbb{Z} = \{gd : d\in\mathbb{Z}\}$

Lemma: R 是一个任意的环，定义集合 $K_R = \{n\in\mathbb{Z} : n\cdot 1_R = 0_R\}$.
则有: 存在唯一的 $g\in\mathbb{Z}_{\geqslant 0}$, s.t. $K_R = g\mathbb{Z} = \{gd : d\in\mathbb{Z}\}$

Proof: 上面已证. $\square$

Lemma: R 是一个任意的整环，则有: 存在唯一的 $char(R)\in\mathbb{Z}_{\geqslant 0}$
使得对 $\forall n\in\mathbb{Z}$ 都有: $n\cdot 1_R = 0_R \iff char(R)\mid n$

Proof: $\because R$ 是整环 $\quad\therefore R$ 是环. 定义集合 $K_R = \{n\in\mathbb{Z} : n\cdot 1_R = 0_R\}$.

$\therefore$ 存在唯一的 $char(R)\in\mathbb{Z}_{\geqslant 0}$, s.t. $K_R = char(R)\mathbb{Z}$

$\therefore K_R = char(R)\mathbb{Z} = \{char(R)\cdot d : d\in\mathbb{Z}\}$

对 $\forall n\in\mathbb{Z}$,

若 $n\cdot 1_R=0_R$，则有：$n\in\mathbb{Z}$ 且 $n\cdot 1_R=0_R$ $\quad\therefore n\in K_R=\mathrm{char}(R)\mathbb{Z}$

$\therefore \exists\, d\in\mathbb{Z}$，s.t. $n=\mathrm{char}(R)\cdot d$

当 $\mathrm{char}(R)>0$ 时，有：$\dfrac{n}{\mathrm{char}(R)}=d\in\mathbb{Z}$ $\quad\therefore \mathrm{char}(R)\mid n$

当 $\mathrm{char}(R)=0$ 时，$n=\mathrm{char}(R)\cdot d=0\cdot d=0$．也可以说 $\mathrm{char}(R)\mid n$

若 $\mathrm{char}(R)\mid n$，则有：$\exists\, q\in\mathbb{Z}$，s.t. $n=\mathrm{char}(R)\cdot q$

$\therefore n=\mathrm{char}(R)\cdot q\in K_R$ $\quad\therefore n\cdot 1_R=0_R$

$\therefore$ 对 $\forall n\in\mathbb{Z}$，有：$n\cdot 1_R=0_R \iff \mathrm{char}(R)\mid n$ $\quad\square$

定义（整环R的特征）R是一个任意的整环，已经证明了存在唯一的 $\mathrm{char}(R)\in\mathbb{Z}_{\geqslant 0}$，使得对 $\forall n\in\mathbb{Z}$ 都有：$n\cdot 1_R=0_R \iff \mathrm{char}(R)\mid n$．称 $\mathrm{char}(R)\in\mathbb{Z}_{\geqslant 0}$ 为整环R的特征．

Lemma：R是整环，则有：$\mathrm{char}(R)\cdot 1_R=0_R$

proof：$\because$ R是整环 $\quad\therefore \mathrm{char}(R)\in\mathbb{Z}_{\geqslant 0}$

若 $\mathrm{char}(R)=0$，则有：$\mathrm{char}(R)\cdot 1_R=0\cdot 1_R=0_R$

若 $\mathrm{char}(R)>0$，则有：$\mathrm{char}(R)\in\mathbb{Z}_{>0}$． $\therefore \mathrm{char}(R)\mid \mathrm{char}(R)$

$\therefore \mathrm{char}(R)\cdot 1_R=0_R$ $\quad\square$

Lemma：R是整环，则有：$\mathrm{char}(R)=0$ 或 $\mathrm{char}(R)$ 是素数

proof：$\because$ R是整环，则有：$\mathrm{char}(R)\in\mathbb{Z}_{\geqslant 0}$

若 $\mathrm{char}(R)=0$，则 $\mathrm{char}(R)=0$

若 $\mathrm{char}(R)\neq 0$，则 $\mathrm{char}(R)\in\mathbb{Z}_{>0}=\mathbb{Z}_{\geqslant 1}$

$\because$ R是整环 $\therefore$ $\mathrm{char}(R)\neq 1$ $\therefore$ $\mathrm{char}(R)\in\mathbb{Z}_{\geqslant 2}$

设 $\mathrm{char}(R)=ab$，其中 $a\in\mathbb{Z}$ 且 $a\neq 0$，$b\in\mathbb{Z}$ 且 $b\neq 0$.

$\because$ R是整环 $\therefore$ R是环 $\therefore$ $f:\mathbb{Z}\longrightarrow R$ 是环同态

$$x\longmapsto x\cdot 1_R$$

$\therefore$ $f(\mathrm{char}(R))=\mathrm{char}(R)\cdot 1_R=0_R$

$f(\mathrm{char}(R))=f(ab)=f(a)f(b)=(a\cdot 1_R)(b\cdot 1_R)$

$\therefore$ $(a\cdot 1_R)(b\cdot 1_R)=0_R$，$a\cdot 1_R\in R$，$b\cdot 1_R\in R$

$\because$ R是整环 $\therefore$ $a\cdot 1_R=0_R$ 或 $b\cdot 1_R=0_R$

$\therefore$ $a\in K_R$ 或 $b\in K_R$ $\therefore$ $a\in\mathrm{char}(R)\mathbb{Z}$ 或 $b\in\mathrm{char}(R)\mathbb{Z}$

$\therefore$ $\mathrm{char}(R)\mid a$ 或 $\mathrm{char}(R)\mid b$

$\therefore$ $ab\mid a$ 或 $ab\mid b$.

若 $ab\mid a$，则 $\exists q_1\in\mathbb{Z}$，s.t. $a=abq_1$ $\because$ $a\neq 0$ $\therefore$ $bq_1=1$

$\because$ $b\in\mathbb{Z}$ 且 $q_1\in\mathbb{Z}$ 且 $bq_1=1$ $\therefore$ $b=\pm 1$ $\therefore$ $a=\pm\mathrm{char}(R)$

若 $ab\mid b$，则 $\exists q_2\in\mathbb{Z}$，s.t. $b=abq_2$ $\because$ $b\neq 0$ $\therefore$ $aq_2=1$

$\because$ $a\in\mathbb{Z}$ 且 $q_2\in\mathbb{Z}$ 且 $aq_2=1$ $\therefore$ $a=\pm 1$ $\therefore$ $b=\pm\mathrm{char}(R)$

$\therefore$ $\mathrm{char}(R)$是素数. $\square$