Lemma：R 和 R' 是环，$f: R \longrightarrow R'$ 是环同态，则有：

对 $\forall n \in \mathbb{Z}$，$\forall x \in R$，有：$f(nx) = nf(x)$.

Proof：对 $\forall n \in \mathbb{Z}$，$\forall x \in R$，有：

①当 $n \in \mathbb{Z}_{\geqslant 1}$ 时，

$$f(nx) = f(\underbrace{x + \cdots + x}_{n\text{个}x}) = \underbrace{f(x) + \cdots + f(x)}_{n\text{个}f(x)} = nf(x)$$

②当 $n = 0$ 时

$$f(nx) = f(0x) = f(0_R) = 0_{R'} = 0 \cdot f(x) = nf(x)$$

③当 $n \in \mathbb{Z}_{\leqslant -1}$ 时，$-n \in \mathbb{Z}_{\geqslant 1}$

$$f(nx) = f((-(-n))x) = f(-((-n)x)) = -f((-n)x)$$

$$= -((-n)f(x)) = nf(x) \qquad \square$$

Lemma: p是素数，R是交换环，且满足$p\cdot 1_R = 0_R$.

$x\in R$，$n\in\mathbb{Z}$，$p\mid n$，则有：$n\cdot x = 0_R$

Proof: $\because p\mid n$ $\therefore \exists q\in\mathbb{Z}$，s.t. $n = pq = qp$

$\therefore n\cdot x = (qp)x = q(px) = q((p\cdot 1_R)x) = q(0_R\cdot x)$

$= q\cdot 0_R = 0_R$ $\square$

Lemma: R和R'都是整环，存在从R到R'的单同态$f: R\to R'$.

则有：$\mathrm{char}(R) = \mathrm{char}(R')$

Proof: $\because$ R是整环

$\therefore$ 存在唯一的$\mathrm{char}(R)\in\mathbb{Z}_{\geqslant 0}$，s.t. 对$\forall n\in\mathbb{Z}$，都有

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

$\because$ R'是整环

$\therefore$ 存在唯一的$\mathrm{char}(R')\in\mathbb{Z}_{\geqslant 0}$，s.t. 对$\forall n\in\mathbb{Z}$，都有

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

$\because \mathrm{char}(R)\in\mathbb{Z}_{\geqslant 0}$，$\mathrm{char}(R)\mid \mathrm{char}(R)$ $\therefore \mathrm{char}(R)\cdot 1_R = 0_R$

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

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

$\because \operatorname{char}(R') \in \mathbb{Z}_{\geqslant 0}$

$\therefore f(\operatorname{char}(R') \cdot 1_R) = \operatorname{char}(R') f(1_R) = \operatorname{char}(R') \cdot 1_{R'} = 0_{R'} = f(0_R)$

$\because f: R \to R'$ 是单射 $\quad \therefore \operatorname{char}(R') \cdot 1_R = 0_R$

$\therefore \operatorname{char}(R) \mid \operatorname{char}(R')$

$\because \operatorname{char}(R') \mid \operatorname{char}(R)$ 且 $\operatorname{char}(R) \mid \operatorname{char}(R')$

$\therefore$ 有三种可能性：

① $\operatorname{char}(R) = 0$ 且 $\operatorname{char}(R') = 0$. 此时 $\operatorname{char}(R) = \operatorname{char}(R')$

② $\operatorname{char}(R) = \operatorname{char}(R')$

③ $\operatorname{char}(R) = -\operatorname{char}(R')$. 此时只能是 $\operatorname{char}(R) = \operatorname{char}(R') = 0$

$\therefore \operatorname{char}(R) = \operatorname{char}(R') \qquad \square$

域的特征

Lemma：R是一个任意的整环，$\mathrm{char}(R)=p>0$，则有：

对$\forall x\in R$，$p\cdot x=0_R$

Proof：$\because$ R是整环，$\mathrm{char}(R)=p>0$ $\therefore$ p是素数，$p\in\mathbb{Z}_{\geqslant 2}$

对于$p\in\mathbb{Z}_{\geqslant 2}$ $\because$ $\mathrm{char}(R)=p$ $\therefore$ $\mathrm{char}(R)\mid p$ $\therefore$ $p\cdot 1_R=0_R$

对$\forall x\in R$，$\because$ $p\in\mathbb{Z}_{\geqslant 2}$，$x\in R$

$\therefore$ $p\cdot x=(p\cdot 1_R)x=0_R\cdot x=0_R$ $\square$

Lemma：R是一个任意的整环，$\mathrm{char}(R)=p>0$，则有：

对$\forall x\in R$，$\forall n\in\mathbb{Z}$，有：$(np)\cdot x=0_R$

Proof：对$\forall x\in R$，$\forall n\in\mathbb{Z}$，有：

$\because$ $n\in\mathbb{Z}$，$p\in\mathbb{Z}_{\geqslant 2}$，$x\in R$ $\therefore$ $(np)x=n(px)$

$\therefore$ $(np)\cdot x=n(px)=n\cdot 0_R=0_R$ $\square$

分$n\in\mathbb{Z}_{\geqslant 1}$，$n=0$，$n\in\mathbb{Z}_{\leqslant -1}$
三种情况讨论.

Lemma (Freshman's dream) p是素数，R是交换环，且满足

$p\cdot 1_R=0_R$. 则有：对$\forall x,y\in R$，有：$(x+y)^p=x^p+y^p$

Proof：对$\forall x,y\in R$，有：

$$(x+y)^p=\sum_{k=0}^{p}\binom{p}{k}x^k y^{p-k}=x^p+y^p+\sum_{k=1}^{p-1}\binom{p}{k}x^k y^{p-k}$$

$\because$ 对 $\forall k=1,2,\cdots,p-1$，有：$p \mid \binom{p}{k}$

$\therefore$ 对 $\forall k=1,2,\cdots,p-1$，有：$\binom{p}{k} x^k y^{p-k} = 0_R$

$\therefore (x+y)^p = x^p + y^p + \sum\limits_{k=1}^{p-1} 0_R = x^p + y^p$ $\square$

Lemma：R 是整环，$\cancel{R}$ R_0 是 R 的子环，则有：

$$\mathrm{char}(R_0) = \mathrm{char}(R)$$

Proof：$\because R$ 是整环，R_0 是 R 的子环 $\therefore R_0$ 是整环.

$\therefore$ 存在唯一的 $\mathrm{char}(R_0) \in \mathbb{Z}_{\geqslant 0}$，s.t. 对 $\forall n \in \mathbb{Z}$，都有

$n \cdot 1_{R_0} = 0_{R_0} \iff \mathrm{char}(R_0) \mid n$

$\because 0_{R_0} = 0_R$，$1_{R_0} = 1_R$

$\therefore$ 对 $\forall n \in \mathbb{Z}$，都有 $n \cdot 1_R = 0_R \iff \mathrm{char}(R_0) \mid n$

$\because R$ 是整环 $\therefore$ 存在唯一的 $\mathrm{char}(R) \in \mathbb{Z}_{\geqslant 0}$，使得

对 $\forall n \in \mathbb{Z}$，都有 $n \cdot 1_R = 0_R \iff \mathrm{char}(R) \mid n$

$\therefore \mathrm{char}(R_0) = \mathrm{char}(R)$ $\square$

Lemma: $\mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = 0$

Proof: $\because$ $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 都是域 $\therefore$ $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 都是整环

对于 $\mathbb{Q}$，有：$1_{\mathbb{Q}} = 1$（数"1"），$0_{\mathbb{Q}} = 0$（数"0"）

$\mathrm{char}(\mathbb{Q}) \in \mathbb{Z}_{\geq 0}$，且对 $\forall n \in \mathbb{Z}$，都有：$n \cdot 1 = 0 \Leftrightarrow \mathrm{char}(\mathbb{Q}) \mid n$

假设 $\mathrm{char}(\mathbb{Q}) > 0$，则 $\mathrm{char}(\mathbb{Q}) \in \mathbb{Z}_{>0}$

$\because \mathrm{char}(\mathbb{Q}) \mid \mathrm{char}(\mathbb{Q})$ $\therefore \mathrm{char}(\mathbb{Q}) \cdot 1 = 0$

$\therefore \mathrm{char}(\mathbb{Q}) = 0$. 矛盾. $\therefore \mathrm{char}(\mathbb{Q}) = 0$

对于 $\mathbb{R}$，有：$1_{\mathbb{R}} = 1$（数"1"），$0_{\mathbb{R}} = 0$（数"0"）

$\mathrm{char}(\mathbb{R}) \in \mathbb{Z}_{\geq 0}$，且对 $\forall n \in \mathbb{Z}$，都有 $n \cdot 1 = 0 \Leftrightarrow \mathrm{char}(\mathbb{R}) \mid n$

假设 $\mathrm{char}(\mathbb{R}) > 0$，则 $\mathrm{char}(\mathbb{R}) \in \mathbb{Z}_{>0}$

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

矛盾 $\therefore \mathrm{char}(\mathbb{R}) = 0$.

同理可证：$\cancel{\mathrm{char}(\mathbb{Q}) =}$ $\mathrm{char}(\mathbb{C}) = 0$

$\therefore \mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = 0$ $\square$

之前已经证明了：对 $\forall N \in \mathbb{Z}_{\geq 1}$，有：

$$\mathbb{Z}/N\mathbb{Z} \text{ 是域} \Leftrightarrow N \text{ 是素数}.$$

设 p 为任意一个素数，则有：$\mathbb{Z}/p\mathbb{Z}$ 是域. 引入符号 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$

Lemma：对$\forall$素数p，有：$\mathrm{char}(\mathbb{F}_p)=p$

Proof：$\because$ p是素数　$\therefore$ $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$是域　$\therefore$ $\mathbb{F}_p$是整环

$\therefore$存在唯一的$\mathrm{char}(\mathbb{F}_p)\in\mathbb{Z}_{\geqslant 0}$，s.t. 对$\forall n\in\mathbb{Z}$，都有

$n\cdot 1_{\mathbb{F}_p}=0_{\mathbb{F}_p} \Leftrightarrow \mathrm{char}(\mathbb{F}_p)\mid n$

$\therefore$对$\forall n\in\mathbb{Z}$，都有　$n\cdot[1]=[0] \Leftrightarrow \mathrm{char}(\mathbb{F}_p)\mid n$

$\therefore$对$\forall n\in\mathbb{Z}$，都有　$[n]=[0] \Leftrightarrow \mathrm{char}(\mathbb{F}_p)\mid n$

(分$n\in\mathbb{Z}_{\geqslant 1}$，$n=0$，$n\in\mathbb{Z}_{\leqslant -1}$三种情况讨论，很容易证$n\cdot[1]=[n]$)

$\therefore$对$\forall n\in\mathbb{Z}$，都有　$p\mid n \Leftrightarrow \mathrm{char}(\mathbb{F}_p)\mid n$

$\because$ $p\mid p$　$\therefore$ $\mathrm{char}(\mathbb{F}_p)\mid p$　$\therefore$ $\mathrm{char}(\mathbb{F}_p)=1$或$p$

$\because$ $\mathrm{char}(\mathbb{F}_p)=0$或$\mathrm{char}(\mathbb{F}_p)$是素数　$\therefore$ $\mathrm{char}(\mathbb{F}_p)=p$. $\square$

Lemma：R是一个任意的整环，已经证明了$\mathrm{Frac}(R)$是域，称为整环R的分式域. 则有：$\mathrm{char}(R)=\mathrm{char}(\mathrm{Frac}(R))$

Proof：$\because$ R是整环，$\mathrm{Frac}(R)$是域，存在$R\to\mathrm{Frac}(R)$的单同态

$\therefore$ $\mathrm{char}(R)=\mathrm{char}(\mathrm{Frac}(R))$ $\square$