Characteristic

Theorem Let R be an integral domain.

additive order

1/ $\mathrm{ord}(1_R) < \infty \Rightarrow \mathrm{ord}(a) = \mathrm{ord}(1_R) \; \forall a \in R \setminus \{0_R\}$

2/ $\mathrm{ord}(1_R) = \infty \Rightarrow \mathrm{ord}(a) = \infty \; \forall a \in R \setminus \{0_R\}$

Proof

$n > 1$ as $1_R \neq 0_R$

1/ Assume $\mathrm{ord}(1_R) = n \in \mathbb{N} \Rightarrow n 1_R = 0_R$

Let $a \in R \setminus \{0_R\}$.

$na = (n 1_R) a = 0_R a = 0_R \Rightarrow \mathrm{ord}(a) \mid n$

Let $m = \mathrm{ord}(a) \Rightarrow ma = 0_R \Rightarrow (m 1_R) a = 0_R$

R an integral domain

$\Rightarrow m 1_R = 0 \Rightarrow n \mid m \Rightarrow n \mid \mathrm{ord}(a)$

$\Rightarrow \mathrm{ord}(a) = \mathrm{ord}(1_R)$

2/ Assume $a \in R \setminus \{0_R\}$ and $\mathrm{ord}(a) = m < \infty$

R integral domain

$\Rightarrow ma = (m 1_R) a = 0_R \Rightarrow m 1_R = 0_R \Rightarrow \mathrm{ord}(1_R) < \infty$

Hence $\mathrm{ord}(1_R) = \infty \Rightarrow \mathrm{ord}(a) = \infty \; \forall a \in R \setminus \{0_R\}$

$\square$

Definition Let R be an integral domain.

characteristic of R — in this case we say R is finite characteristic

$$\mathrm{Char}(R) := \begin{cases} \mathrm{ord}(1_R) & \text{if } \mathrm{ord}(1_R) < \infty \\ 0 & \text{if } \mathrm{ord}(1_R) = \infty \end{cases}$$

Examples $\mathrm{Char}(\mathbb{Z} / \mathbb{Q} / \mathbb{R} / \mathbb{C}) = 0$

$\mathrm{Char}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}[x]) = p$

Theorem Let R be an integral domain of finite characteristic. Then $\mathrm{Char}(R)$ is prime.

Proof

R integral domain of finite characteristic $\Rightarrow$

- $\mathrm{ord}(1) = n \in \mathbb{N}$
- $\mathrm{ord}(1_R) \neq 1$ $(0_R \neq 1_R)$

Assume n not prime. $\Rightarrow$ $\exists\, a, b \in \mathbb{N}$ such that

$n = ab, \quad a, b < n.$

$\Rightarrow \quad 0_R = n 1_R = (ab) 1_R = (a 1_R)(b 1_R)$

R integral domain

$\Rightarrow$ Either $a 1_R = 0_R$ or $b 1_R = 0_R$

$\Rightarrow \quad \mathrm{ord}(1_R) \leq \max\{a, b\} < n.$ Contradiction $\square$

Remarks

1/ R integral domain $\Rightarrow$ $\mathrm{Char}(R) = \mathrm{Char}(\mathrm{Frac}(R))$

2/ R integral domain $\Rightarrow$ $\mathrm{Char}(R) = \mathrm{Char}(R[x_1, \dots, x_n])$

Theorem Let F be a field

1/ $\mathrm{Char}(F) = 0 \Rightarrow \exists !$ injective homomorphism $\phi : \mathbb{Q} \longrightarrow F$ ($\Rightarrow \mathbb{Q}$ is a subfield of F)

2/ $\mathrm{Char}(F) = p \Rightarrow \exists !$ injective homomorphism $\phi : \mathbb{Z}/p\mathbb{Z} \longrightarrow F$ ($\Rightarrow \mathbb{Z}/p\mathbb{Z}$ a subfield of F)

<u>Proof</u> (Outline)

Char$(F) = 0$

Forced because 1 goes to 1_R

1) $\exists!$ injective unique homomorphism $\mathbb{Z} \to F$
$$n \to n 1_F$$

F a field $\Rightarrow$ This extends uniquely to an injective

must check well-defined

homomorphism $\phi : \mathbb{Q} \to F$
$$\frac{n}{m} \to (n 1_F)(m 1_F)^{-1}$$

2) Char$(F) = p \Rightarrow \phi : \mathbb{Z}/p\mathbb{Z} \longrightarrow F$ an
$$[n] \longrightarrow n 1_F$$

injective homomorphism

$\square$

identified with subfield

<u>Examples</u> $\mathbb{Q} \subset \mathbb{C}$, $\mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}/p\mathbb{Z}(x_1, \dots, x_n)$