1 Rings and Homomorphisms (condinued)

Definition 1.1. The *characteristic* of R is the least positive integer n such that $n1 = 0$. If no such n exists, we say R has characteristic 0

Example 1.2. $\mathrm{char}(\mathbb{Z}) = 0$

Example 1.3. Fix $n \in \mathbb{N}$, $\mathbb{Z}_n := \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. Define $+, \cdot$ as $\overline{a} + \overline{b} = \overline{c}$, $\overline{a} \cdot \overline{b} = \overline{d}$ where $= \leq c, d \leq n-1$ and $a + b \equiv c \pmod{n}$, $ab \equiv d \pmod{n}$. Then $\mathbb{Z}_n$ is a ring and $\mathrm{char}(\mathbb{Z}_n) = n$.

Definition 1.4. R is an *integral domain* whenever $ab = 0 \Rightarrow a = 0$ or $b = 0$ for $a, b \in \mathbb{R}$.

Example 1.5. $\mathbb{Z}_6$ is not an integral domain, since $\overline{3} \cdot \overline{2} = \overline{0}$.

Proposition 1.6. *If R is an integral domain with characteristic $n \neq 0$, then n is a prime.*

Proof. Suppose $n = st$, where $1 < s, t < n$. $0 = n \cdot 1 = (\underbrace{1 + 1 + \cdots + 1}_{s})(\underbrace{1 + 1 + \cdots + 1}_{t})$ $= s \cdot t \cdot 1$, hence $s \cdot 1 = 0$ or $t \cdot 1 = 0$, $\rightarrow\leftarrow$. $\square$

Definition 1.7. A map $f : R \to R'$ from ring R into ring R' is a *homomorphism* if $f(a+b) = f(a) + f(b)$ and $f(a \cdot b) = f(a) \cdot f(b)$, for $a, b \in R$.

Lemma 1.8. *If $f : R \to R'$ is homomorphism then $f(0) = 0'$.*

Proof. $f(0) = f(0+0) = f(0) + f(0) \Rightarrow f(0) = 0'$. $\square$

Definition 1.9. An *isomorphism* $f : R \to R'$ is a bijective homomorphism.