Chapter 3.2 part 4

Th 3.9 Every finite integral domain R is a field. | $\mathbb{Z}$ is an integral domain but not a field

Pf Let $a \in R$, $a \neq 0_R$. Wanted: a is a unit
(equivalently, there exists $c \in R$ such that $ac = 1_R$)

Consider the map

$$f : R \longrightarrow R$$
$$b \longmapsto ab \quad \Big| \quad f(b) = ab$$

It suffices to prove that f is surjective. Indeed, the $1_R \in \mathrm{Im}(f)$ meaning $ac = 1_R$ for some $c \in R$.

However, a map from a finite set to itself is surjective iff the map is injective.

We thus will prove that f is injective, and this will suffice.

For the injectivity, let $b_1 \neq b_2$ (thus $b_1 - b_2 \neq 0_R$).

Their images under f are ab_1 and ab_2 correspondingly

$$ab_1 - ab_2 = a(b_1 - b_2) \neq 0_R$$ because $a \neq 0_R$ by assumption
$b_1 - b_2 \neq 0_R$
and R is an integral domain

Thus $ab_1 \neq ab_2$, therefore f is injective.