Integral Domains

Defn An integral domain is a commutative ring with unity that has no zero divisors.

Ex $\mathbb{Z}$ (hence the term integral domain)

Ex* $\mathbb{Z}_p$ is an integral domain $\Leftrightarrow$ p is prime.

($\Rightarrow$) Sps p is not prime.

$p = mn$ for some $0 \leq m, n < p$

so $m, n \in \mathbb{Z}_p$

So m, n are zero-divisors in $\mathbb{Z}_p$ so, not an integral domain.

($\Leftarrow$) Sps p is prime and $a, b \in \mathbb{Z}_p$

$ab = 0 \in \mathbb{Z}_p \Rightarrow p \mid ab$

$\Leftrightarrow p \mid a$ or $p \mid b$, ie. $a = 0$ or $b = 0$ in $\mathbb{Z}_p$ ...

so not a zero divisor.
Thus $\mathbb{Z}_p$ is an integral domain.

Thm In an integral domain, if $a \neq 0$, then

$$ab = ac \Rightarrow b = c.$$

proof: $a \neq 0$ and R integral domain so $a(b-c) = 0 \Rightarrow b - c = 0$

i.e. $b = c$.

Note: proof does not make use of multiplicative inverses (unlike groups)