Thm Finite integral domains are fields.

proof: Sps R is an finite integral domain

and $a \in R$ is nonzero. (NTS: a has an inverse)

1... exists in R

Consider: $a^0, a^1, a^2, \ldots$ ← elements of R.

pigeon hole principle

R is finite so $a^i = a^j \neq 0$ for some $i > j$.

Note: $a^i = 0$ would imply $a = 0$ b/c R an I.D.

$$a^i = a^j$$

$$\Rightarrow a^i - a^j = 0.$$

$a^j \neq 0$

$$\Rightarrow a^j(a^{i-j} - 1) = 0$$

$$\Rightarrow a^{i-j} - 1 = 0$$ (because R has no zero divisors)

$$\Rightarrow a^{i-j} = 1.$$

nonneg power of a, thus in R.

But $i > j \Rightarrow i - j \geq 1$. So: $a(a^{i-j-1}) = 1$

Thus $a^{-1} = a^{i-j-1}$.

<u>Ex</u> $\mathbb{Z}_p$ is a field $\Leftrightarrow$ p is prime.

because from earlier, $\mathbb{Z}_p$ is a finite integral domain precisely when p is prime.