Integral Domains

Definition

To say that a R is an *integral domain* means:

1). R is a commutative ring with unity $1 \neq 0$

2). R has no zero divisors

Theorem

Let R_1 and R_2 be rings. $R_1 \times R_2$ is never an integral domain.

Proof

Let $r_1 \in R_1, r_1 \neq 0$
Let $r_2 \in R_2, r_2 \neq 0$
$(r_1, 0) \in R_1 \times R_2$
$(0, r_2) \in R_1 \times R_2$
$(r_1, 0)(0, r_2) = (0, 0)$
$(r_1, 0)$ and $(0, r_2)$ are zero divisors in $R_1 \times R_2$
$\therefore R_1 \times R_2$ is not an integral domain.

Theorem

F is a field $\implies F$ is an integral domain.

Proof

Assume F is a field
F is a commutative ring with unity $1 \neq 0$
Assume $a \in F, a \neq 0$
Assume $b \in F, ab = 0$
$a^{-1} \in F$
$a^{-1}(ab) = a^{-1}0$
$(a^{-1}a)b = 0$
$1b = 0$
$b = 0$
Thus, a is not a zero divisor of F
F has no zero divisors
$\therefore F$ is an integral domain.

Theorem

F is a finite integral domain $\implies F$ is a field.

Proof

Assume F is a finite integral domain
F is a commutative ring with unity $1 \neq 0$

Assume $a \in F, a \neq 0$
Let $L_a : F \to F$ be defined by $L_a(x) = ax$

Assume $L_a(x) = L_a(y)$
$ax = ay$
But F is an integral domain, so the cancellation laws hold
$x = y$
$\therefore L_a$ is one-to-one.

But F is finite, so L_a is also onto
$\therefore L_a$ is a bijection on F.

$1 \in F$
$\exists\, x \in F, L_a(x) = 1$
$ax = 1$
But F is cummutative so $xa = 1$
So x is a multiplicative inverse for a
Thus every non-zero element of F has a multiplicative inverse

$\therefore F$ is a field.

Corollary

p prime $\implies \mathbb{Z}_p$ is a field.