Chap 20. Integral domains.

An integral domain is a commutative ring with unity having the cancellation property:

if $a \neq 0$ and $ab = ac$, then $b = c$.

It may also be defined as a commutative ring with unity having no divisors of zero:

if $ab = 0$, then $a = 0$ or $b = 0$.

Define: $n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ times}}$ for $n > 0$. $0 \cdot a = 0$.

$-n \cdot a = -(n \cdot a)$

In a ring with unity, if 1 has additive order n, we say the ring has "characteristic n".

In other words, if A is a ring with unity, the characteristic of A is the least positive integer n s.t. $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$. If there is no such positive integer n, A has characteristic 0.

Thm: All the nonzero elements in an integral domain have the same additive order.

Pf: $n \cdot a = \underbrace{a + \cdots + a}_{n \text{ times}} = \underbrace{1a + \cdots + 1a}_{n \text{ times}} = \underbrace{(1 + \cdots + 1)}_{n \text{ times}} a = (n \cdot 1)a$

$n \cdot a = 0 \iff (n \cdot 1)a = 0 \overset{a \neq 0}{\iff} n \cdot 1 = 0$.

So if the characteristic of an integral domain is a positive integer n, then

$n \cdot x = 0$ for every element in the domain

Thm 2: In an integral domain with nonzero characteristic, the characteristic is a prime number

Proof: $n = k \cdot \ell \Rightarrow 0 = n \cdot 1 = \underbrace{(1 + \cdots + 1)}_{k}\underbrace{(1 + \cdots + 1)}_{\ell} = (k \cdot 1)(\ell \cdot 1)$

$n \cdot 1 = 0$ (n = characteristic of A)

$\Rightarrow k \cdot 1 = 0$ or $\ell \cdot 1 = 0$.

(integral domain)

Thm 3: In any integral domain A of characteristic p,

$$(a+b)^p = a^p + b^p \quad \forall\, a, b \in A$$

Pf: $(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{p-1} a b^{p-1} + b^p$

$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$ is a multiple of p $\forall\, 1 < k < p$.

$\Rightarrow \binom{p}{k} a^{p-k} b^k = 0 \ \forall\, 1 < k < p \Rightarrow (a+b)^p = a^p + b^p$.

Any field is an integral domain: $ax = ay,\ a \neq 0 \Rightarrow x = a^{-1}ax = a^{-1}ay = y$ (cancellation holds).

integral domain is not necessarily a field. $\not\Leftarrow$ but:

Thm: Every finite integral domain is a field.

Pf: $A = \{0, 1, a_1, a_2, \cdots, a_n\} \Rightarrow \exists\, a_j$ s.t. $a_i a_j = 1$

$\forall\, a_i = \{a_i 0, a_i 1, a_i a_1, a_i a_2, \cdots, a_i a_n\}$ $\Downarrow$ $a_i^{-1} = a_j$ exists $\forall\, a_i$

1-1 $\Rightarrow$ every nonzero element in the integral domain is invertible

$\Rightarrow A$ is a field.

Exer: A.4 A is an integral domain. $256 \cdot a = 0$ $\quad \text{char}(A) \mid 256 = 2^8 \Rightarrow \text{char}(A) = 2$ (char(A) is prime)

A.7 $10a = 0,\ 14b = 0 \quad p \mid 10,\ p \mid 14 \Rightarrow p = 2 = \text{char}(A)$

B.2 $\text{ord}(A) = p \Rightarrow \text{char}(A) \mid \text{ord}(A) \Rightarrow \text{char}(A) = p$

E.1 $n \cdot a = 0,\ p \nmid n \Rightarrow \exists\, k, l$ s.t. $kp + nl = 1 \Rightarrow a = (kp + nl) \cdot a = 0$ ($p = \text{char}(A)$)

F.1 A is a finite field $\Rightarrow$ 1 has finite order $\Rightarrow \text{char}(A) < \infty$.