Theorem 13.1 Cancellation

Let $a, b,$ and c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

Proof

$$ab = ac$$

$$ab - ac = 0 \quad \text{(Ring property 4)}$$

$$a(b-c) = 0 \quad \text{(Thm. 12.1.4)}$$

$$b - c = 0 \quad \text{(no zero divisors)}$$

$$b = c. \quad \text{(Ring property 4)} \quad \square$$

Theorem

Let R be a commutative ring with unity and the cancellation property. Then R is an integral domain.

Proof Let $a \in R - \{0\}$.

Let $b \in R$ and suppose $ab = 0$.

$$ab = a0 \quad \text{(Thm. 12.1.1)}$$

$$b = 0 \quad \text{(cancellation)}$$

Therefore a is not a zero-divisor, and R is an integral domain. $\square$

Theorem 13.2 A finite integral domain is a field.

Proof Let D be a finite integral domain with unity 1.

Goal: show $a \in D - \{0\}$ is a unit.

Case 1 $a = 1$

Then $a \cdot a = 1$ and $a = a^{-1}$.

Case 2 $a^1, a^2, \ldots, a^{|D|}, a^{|D|+1}$ has a repeat,

say $a^i = a^j$ with $1 \leq j < i \leq |D|+1$.

$a^{i-j} a^j = a^j \cdot 1$ (existence of unity)

$a^{i-j} = 1$ (cancellation)

assume $i - j \geq 2$, or else we are in Case 1.

$$a^{i-j} = a\, a^{i-j-1} = 1$$

where $i - j - 1 \geq 1$, and so

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

and a is a unit. $\square$

"n" in a ring with unity

Let $n \in \mathbb{Z}$. What is "n" in a ring R with unity 1?

$$\underbrace{1+1+\cdots+1}_{n \text{ times}} = n \qquad (n>0)$$

$-1 \in R$ by Ring Property 4

$$\underbrace{-1-1-\cdots-1}_{n \text{ times}} = -n \qquad (n>0,\ -n<0)$$

So for arbitrary $r \in R$, nr means:

$$nr = \begin{cases} \underbrace{r+r+\cdots+r}_{n \text{ times}}, & n \in \mathbb{Z}^+ \\ 0 \text{ (of the ring)}, & n = 0 \text{ (as an integer)} \\ \underbrace{-r-r-\cdots-r}_{|n| \text{ times}} & n \in \mathbb{Z}^- \end{cases}$$

But "n" may look strange!

in $M_2(\mathbb{Z}_5)$, $\quad 8 = \underbrace{\begin{bmatrix}1&0\\0&1\end{bmatrix}+\cdots+\begin{bmatrix}1&0\\0&1\end{bmatrix}}_{8 \text{ times}} = \begin{bmatrix}3&0\\0&3\end{bmatrix}$

so $8\begin{bmatrix}2&4\\0&3\end{bmatrix} = \begin{bmatrix}3&0\\0&3\end{bmatrix}\begin{bmatrix}2&4\\0&3\end{bmatrix} = \begin{bmatrix}1&2\\0&4\end{bmatrix}$.

Thm 13.3 Characteristic of a ring with unity

Let a ring R have unity 1. If $|1| = \infty$ additively, then $\text{char } R = 0$. If $|1| = n$ additively, then $\text{char } R = n$.

Proof

If $|1| = \infty$ additively, there is no smallest $n \in \mathbb{Z}^+$ with $nx = 0$ for all $x \in R$.
$\text{char } R = 0$ by definition.

If $|1| = n \in \mathbb{Z}^+$ additively, no $1 \leq n' < n$ satisfies $n' \cdot 1 = 0$ by definition of $|1|$.
Letting $x \in R$,

$$n \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ times}}$$

$$= \underbrace{1 \cdot x + 1 \cdot x + \cdots + 1x}_{n \text{ times}} \quad (\text{Defn. unity})$$

$$= \underbrace{(1 + 1 + \cdots + 1)}_{n \text{ times}} x \quad (\text{Distributivity})$$

$$= (n \cdot 1)x$$

$$= 0x = 0.$$

Therefore $\text{char } R = n$. □

Thm 13.4 The characteristic of an integral domain is 0 or prime.

Proof Let R be an integral domain with unity $1 \in R$.

Case 1 $|1| = \infty$ (additive order)

Then $\text{char } R = 0$ by Theorem 13.3.

Case 2 $|1| = n \in \mathbb{Z}^+$. $\text{char } R = n$ by Theorem 13.3.

Suppose $n = st$, where $1 \le s, t \le n$; $s, t \in \mathbb{Z}^+$.

$$0 = n \cdot 1 = \Big(\underbrace{1 + 1 + \cdots + 1}_{s \text{ times}}\Big) + \Big(\underbrace{1 + 1 + \cdots + 1}_{s \text{ times}}\Big) + \cdots + \Big(\underbrace{1 + 1 + \cdots + 1}_{s \text{ times}}\Big) \quad \Big\} t \text{ times}$$

$$= s \cdot 1 \Big(\underbrace{1 + \cdots + 1}_{t \text{ times}}\Big) \quad \text{by distributivity}$$

$$= (s \cdot 1)(t \cdot 1)$$

R is an integral domain, and so either $s \cdot 1 = 0$ or $t \cdot 1 = 0$; say $s \cdot 1 = 0$.

By definition of $|1|$, $s = n$.

Therefore n must be prime. □