In $\mathbb{Z}_6$, 2, 3, 4 are zero divisors
1, 5 are not zero divisors
0

pf a is not a zero divisor
$ba = ca \Rightarrow b = c$

Theorem 13.1 If $a \in R$ is not a zero divisor and $ab = ac$, then $b = c$. Consequently, if R is an integral domain and $a \in R$ is nonzero such that $ab = ac$, then $b = c$.

$\therefore ab = ac$, a is not a zero divisor in R.

Then $a(b-c) = ab - ac = 0$ $\therefore$ $b - c = 0$, i.e., $b = c$

In $\mathbb{Z}_4$
$2 \cdot b \equiv_4 2 \cdot a$
$\Rightarrow a = b$.

Remark: $AB = AC$ $A, B, C \in M_n(\mathbb{R})$
A^{-1} exists
Then
$B = C$

$0 = A(B-C)$ / $A^{-1}0 = A^{-1}A(B-C)$

Theorem 13.2 A finite integral domain is a field.

Proof. Let $D = \{0, 1, d_1, \cdots, d_r\}$ be an finite integral domain.

So we need to check $D^* = \{1, d_1, \cdots, d_r\}$ form a Abelian group under $\cdot$.

Check
- (G0) closed ✓ follows from (R0)
- (G1) associative follows from (R2)
- (G2) existence of 1 ✓ $\because$ D is an integral domain
- (G3) Let $d_i \in D^*$. Then if $d_i = 1$, then $1 \cdot 1 = 1$, so 1 is its own inverse. If $d_i \neq 1$, then $d_i, d_i^2, \cdots, d_i^n, \cdots$ will repeat so that $d_i^p = d_i^q$ with $q < p$. Then $d_i^{q-p} = 1$.
- (G4) Commutative ✓ $\therefore$ D is an integral domain

$d_i^{q-p} \cdot d_i^p = 1 \cdot d_i^p$

Corollary If p is a prime, then $\mathbb{Z}_p$ is a field.

$\mathbb{Z}_n$ is a commutative ring with unity 1

$\mathbb{Z}_n$ has zero divisor if and only if n is composite.

Remk $\mathbb{Z}$ is an integral domain not a field.

Proof 2: Define $f: D^* \to D^*$ by
$f(x) = d_i x$. Then $d_i x = d_i y \Rightarrow x = y$ (6)
$\therefore f$ is ... $\therefore \exists d_j$ s.t. ...

Then ~~d~~ Note $q - p > 1$ else
$d_i^1 = 1 \Rightarrow d_i = 1$.
So $d_i \cdot d_i^{q-p-1} = 1$.

Remark. Every field $\mathbb{F}$ is an integral domain.

Proof $\mathbb{F}$ is a field.

Then $\mathbb{F}$ is a commutative ring with unity.

It remains to show that $\mathbb{F}$ has no zero divisor.

Suppose it does, say $a \neq 0$ in $\mathbb{F}$ is a zero divisor.

Then $\exists\ b \in \mathbb{F}^*$ such that $a \cdot b = 0$.

Then ~~then~~ then it violate the fact that

$(\mathbb{F}^*, \cdot)$ is a group.

In particular, $a, b \in \mathbb{F}^*$, $ab \in \mathbb{F}^*$.

Proof of Theorem 13.3/4.

Assume R has unity 1. & $|1| = n$.

To prove $\mathrm{Char}(R) = n$, note that

$$\underbrace{x + x + \cdots + x}_{n} = 1\cdot x + \cdots + 1\cdot x \qquad (1 \text{ is the unity of } R)$$

$$= \underbrace{(1+1+\cdots+1)}_{n} x$$

$$= 0x$$

$$= 0$$

n is the smallest positive integer satisfying $x + \cdots + x = 0$

$\because$ $\underbrace{1+1+\cdots+1}_{n} = 0$, where n is the smallest positive integer ~~s[illegible] making~~ operating on 1 to produce 0.

Now suppose R is an integral domain

Then $1 \in R$. & $\mathrm{Char}(R) = |1|$

Case 1: If $|1| = \infty$ then $\mathrm{Char}(R) = 0$.

Case 2: Suppose $|1| = n$. &

If $n = a \cdot b$ $\quad 1 < a, b < n$.

then $\underbrace{1+\cdots+1}_{n} = \underbrace{(1+\cdots+1)}_{a \neq 0} \underbrace{(1+\cdots+1)}_{b \neq 0}$.

so that $a \cdot 1$ is a zero divisor

So n must be a prime.

Definition If there is $x \in R$ such that $nx = x + \cdots + x \neq 0$ for any $n \in \mathbb{N}$, then we say that R has has characteristic 0.

Otherwise, we can let n be the smallest positive integer such that $0 = nx = x + \cdots + x$ (n times) for every $x \in R$; we say that R has characteristic n.

Notation Denote by $\mathrm{char}R$ the characteristic of R.

Theorem 13.3-4 If R has unity 1, then $\mathrm{char}R = n$ if $|1| = n$ in $(R, +)$. If R is an integral domain, then $\mathrm{char}R$ is zero or prime.

Remark : If R is a finite ring with m elements then

Then $(R, \cdot)$ is a group with m elements $\therefore$ $\underbrace{x + \cdots + x}_{m} = 0$.

$R = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{Z}_2 \right\}$ has 4 elements.

But $x + x = 0$

$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has char 2. $\rightarrow |(1,1)| = 2$.

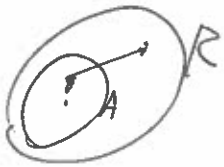
$(a,b) + (a,b) = (2a, 2b) = (0,0)$

$\mathbb{Z}_4$ has char 4. 1 has order 4. Char 4. $|1| = 4$.

$\mathrm{Char}(\mathbb{Z}_m) = n$ In $\mathbb{Z}_n$ $|1| = n$. $\mathbb{Z}_m \oplus \mathbb{Z}_n$ $(1,1) = (|1|, |1|)$

In general, for a finite ring $R = \{r_1, \cdots, r_m\}$

then $\mathrm{Char}(R) = \mathrm{lcm}(|r_1|, \cdots |r_m|)$.



Chapter 14 Ideals and Factor Rings

Definition A subring A of a ring R is a (two-sided) ideal if $ar, ra \in A$ for every $r \in R$ and every $a \in A$. [An ideal is a subring with left and right absorbing power!]

Theorem 14.1 A non-empty subset A of a ring R is an ideal if

1. $a - b \in A$ whenever $a, b \in A$, and
2. $ra, ar \in A$ whenever $a \in A, r \in R$.

$\Rightarrow$ A is a subring with the "strong absorbing" property.

Example $\{0\}$ $n\mathbb{Z}$ in $\mathbb{Z}$, $\langle f(x)\rangle$ in $\mathbb{R}[x]$, $\langle\{2,x\}\rangle = (2\mathbb{Z})[x] \subseteq \mathbb{Z}[x]$.

① For any ring R, $\{0\}$ & R are ideals of R.

② In $\mathbb{Z}$, $n\mathbb{Z}$ is an ideal.

We know that $n\mathbb{Z}$ is an subring.

Clearly, for $r \in \mathbb{Z}$, $a \in n\mathbb{Z}$, $a = nk$ for some $k \in \mathbb{Z}$.

$\therefore$ $ar = nkr \in n\mathbb{Z}$

$\|$

ra

---

③ Pf: Consider $\mathbb{R}[x] = \{a_0 + a_1x + \cdots + a_nx^n : n \in \mathbb{N}, a_0, \cdots, a_n \in \mathbb{R}, a_n \neq 0\}$

$A = \langle f(x)\rangle = \{f(x)g(x) : g(x) \in \mathbb{R}[x]\}$.

To prove A is an ideal.

1° $f(x)\cdot 0 = 0 \in A \neq \phi$.

2° If $h_1(x), h_2(x) \in A$, i.e., $h_1(x) = f(x)g_1(x)$ & $h_2(x) = f(x)g_2(x)$.

$\therefore$ $h_1(x) - h_2(x) = f(x)g_1(x) - f(x)g_2(x)$

$= f(x)\hat{g}(x)$ with $\hat{g}(x) = g_1(x) - g_2(x)$

$\in \langle f(x)\rangle$

3° If $a(x) \in A$, $\frac{h(x)}{f(x)} \in \mathbb{R}[x]$.

Then $a(x) = f(x)g(x)$, $g(x) \in \mathbb{R}[x]$ $\therefore$ $a(x)h(x) = f(x)[g(x)h(x)]$

$\|$ $\in$ ideal

Example $\mathbb{Z}[x]$

$$A = \langle \{2, x\} \rangle = \{ a_0 + a_1 x + \cdots + a_n x^n : a_0, a_1, \ldots, a_n \in 2\mathbb{Z},\ n \in \mathbb{N},\ a_n \neq 0 \} \cup \{0\}$$

$$\subsetneq \mathbb{Z}[x]$$

$\Downarrow$

an ideal.

Proof: ① $0 \in A$

② If $f(x), g(x) \in A$

then $f(x) - g(x)$ is a polynomial with even integer coefficients.

③ If $f(x) \in A$, $g(x) \in \mathbb{Z}[x]$

then $f(x) = 2\hat{f}(x)$

so that $f(x)g(x) = 2\hat{f}(x)g(x)$

$\in 2\mathbb{Z}[x]$.

∎