1-14

Integral Domains

Ring w/ identity / commutativity / no zero-div.

a is a left zero-divisor if $b \neq 0$ but

$ab = 0$, likewise for right zero-divisors.
→mutatis mutandis←

Examples: In $\mathbb{Z}_4$ $2 \cdot 2 = 0$

If n is composite, does $\mathbb{Z}_n$ always have zero divisors?

In $\mathbb{Z}_{20}$, which #'s are units and which are zero-divisors? Any overlaps.

Units: $\{1, 3, 7, 9, 11, 13, 17, 19\} = U_{20}$

Zero-divisors: $\{2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18\}$

Huge property of domains.

Domains permit cancellation.

Pf: Given $ab = ac$, want to show $b = c$.

Write as $ab - ac = 0 = a(b-c)$. We may assume $a \neq 0$ or expression is degenerate. Since there are no zero divisors, it must be the case that $(b-c) = 0$ or $b = c$ ✓ ■

$$\mathbb{Z} \oplus \mathbb{Z} = \{(m,n) : m,n \in \mathbb{Z}\}$$

$$(1,0)\cdot(0,1) = (0,0)$$

<u>Field</u> : Integral domain where every non-zero element is (multiplicatively) invertible.

$x^2 - 4x + 3$ over $\mathbb{Z}_{12}$

$P(x) = (x-3)(x-1) = 0$

Try:

1 Yes	7 Yes
2 No	8 No
3 Yes	9 Yes
4 No	10 No
5 No	11 No
6 No	

8 $\mathbb{Z} \oplus \mathbb{Q} \oplus \mathbb{Z}$

$(0,0,1) \rightarrow (0,0,k)$ $\quad$ (a,b,c)

$(0,1,0)$ $\quad$ $(l,0,0.)$

$(0,0,1)$.

$(\pm 1, r, \pm 1)$

$(1,1,0)$

$(1,0,1)$ $\quad$ $r \neq 0$

$(0,1,1)$ $\quad$ $(1,3,-1)$

$(1, \frac{1}{3}, -1)$

$\mathbb{Q} \oplus \mathbb{Q}$ field?

16 a is an idempotent if $a^2 = a$.

$a^2 - a = 0 \Rightarrow a(a-1) = 0$

$a = 0$ or 1

Subfield Test: If $a, b \in R \Rightarrow a-b \in R$ and $ab \in R$.

Replace $ab \in R$ by $ab^{-1} \in R$ $(b \neq 0)$

26 Let $R = \{0, 2, 4, 6, 8\}$ under add/mult mod 10. Is R a field.

6 is identity.

$4 \cdot 4 = 6 \mod 10$

$2 \cdot 8 = 6$ " "