<u>Recall</u>: In a ring R, an element $a \in R$ is

- a <u>zero divisor</u> if $a \neq 0$ and $a \cdot b = 0$ or $b \cdot a = 0$ for some non-zero $b \in R$

- a <u>unit</u> if R has 1 and a has a multiplicative inverse (i.e. $a \cdot b = 1 = b \cdot a$ for some $b \in R$).

<u>Warm-Up</u>: Find all zero divisors and units in

- $\mathbb{Z}_4$
- $\mathbb{Z}_5$
- $\mathbb{Z}_6$
- $\mathbb{Z}_n$, $n \in \mathbb{N}$

Ex: In $\mathbb{R}[x]$, we have

$$\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x))$$

Thus,

- There are no zero divisors, since $\deg(p(x) \cdot q(x)) \geq 0$ for non-zero $p(x)$ and $q(x)$.

- The units are precisely the non-zero constant polynomials, since $\deg(1) = 0$.
  The inverse of $p(x) = c \in \mathbb{R}^\times$ is $\frac{1}{c}$.

Thm (Cancellation Laws):

Let R be a ring. Then R has no zero divisors if and only if for all $a, b, c \in R$,

$$① \ ab = ac \Rightarrow a = 0 \text{ or } b = c$$

and

$$② \ ba = ca \Rightarrow a = 0 \text{ or } b = c.$$

Proof: ($\Rightarrow$) Suppose R has no zero divisors. Then $ab = ac$ implies

$$ab - ac = 0$$
$$a(b-c) = 0. \quad \text{(Dist. Law)}$$

Since a is not a zero divisor, either $a = 0$ or $b - c = 0$, i.e. $b = c$, proving ①. ② is similar.

($\Leftarrow$) Suppose the cancellation laws ① and ② hold in R.

If $a \neq 0$, then

$$ab = 0 \Rightarrow ab = a \cdot 0 \Rightarrow b = 0$$

and

$$ba = 0 \Rightarrow ba = 0 \cdot a \Rightarrow b = 0.$$

So a is not a zero divisor. $\blacksquare$

So if we have no zero divisors, we can "cancel a" – even if a doesn't have an inverse!

Ex: In $\mathbb{Z}$, $8n = 8m \Rightarrow n = m$.

In $\mathbb{R}[x]$, $x p(x) = x q(x) \Rightarrow p(x) = q(x)$.

etc.

Ex: Find all $x \in \mathbb{Z}_{13}$ satisfying

$$x^2 - 3x - 10 = 0.$$

Well,

$$x^2 - 3x - 10 = (x+2)(x-5) = 0.$$

Since $\mathbb{Z}_{13}$ has no zero divisors, this implies

$$x + 2 = 0 \quad \Rightarrow \quad x = -2 = 11$$

or

$$x - 5 = 0 \quad \Rightarrow \quad x = 5.$$

So the two solutions are $x = 5, 11$.

Ex: Solve the same equation in $\mathbb{Z}_{12}$.

We still have $x = -2 = 10$ and $x = 5$ as solutions, since the factorization

$$x^2 - 3x - 10 = (x+2)(x-5)$$

remains true in $\mathbb{Z}_{12}$.

But $\mathbb{Z}_{12}$ has zero divisors, so we get additional solutions:

$\underline{x=1}$: $(1+2)(1-5) = 3\cdot(-4) = 3\cdot 8 = 24 = 0.$

$\underline{x=2}$: $(2+2)(2-5) = 4\cdot(-3) = 4\cdot 9 = 36 = 0.$

Def: Let R be a ring with 1.

- If R is commutative and has no zero divisors, then we say R is an <u>integral domain</u>.

  Ex: $\mathbb{Z}$, $\mathbb{R}[x]$, $\mathbb{R}[x,y]$

- If $R^{\times} = R \setminus \{0\}$, then we say R is a <u>division ring</u>.

  group of units

  Ex: $\mathbb{H}$ (next example)

- If R is a commutative division ring, then we say R is a <u>field</u>.

  Ex: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ for prime p

Ex: Let $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ be the real vector space with basis $\{1, i, j, k\}$.

Define multiplication on $\mathbb{H}$ to be given by distributing and following the rules for multiplication in Q_8.

Ex: $(4i - 6j)(2 + 3i) = 8i + 12\underbrace{i^2}_{=-1} - 6j - 18\underbrace{ji}_{=-k}$

$= -12 + 8i - 6j + 18k$

Then

- Multiplication is associative, so $\mathbb{H}$ is a ring, call the ring of <u>quaternions</u>.

- $\mathbb{H}$ is <u>not</u> commutative (e.g. $ij \neq ji$)

- $\mathbb{H}$ is a division algebra, since

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$$