Section 19 Integral Domains

One algebraic property that you have used alot is that when $a, b \in \mathbb{R}$ and $ab = 0$ then $a = 0$ or $b = 0$.
~~This is called the~~
You use this when solving a quadratic by factoring

$$x^2 + x - 2 = 0$$
$$(x-1)(x+2) = 0$$
$$x - 1 = 0 \qquad x + 2 = 0$$
$$x = 1 \qquad x = -2$$

But - get used to it - this property fails for arbitrary rings. Look. Suppose we try to solve this equation for x in $\mathbb{Z}_{10}$

$$x^2 + x - 2 = 0$$
$$(x-1)(x+2) = 0$$
$$x = 1 \qquad x = -2 = 8$$

You got solutions 1 and 8. They check back $\left\{ \begin{array}{l} 1^2 + 1 - 2 = 0 \\ 8^2 + 8 - 2 = 70 = 0 \end{array} \right.$

$$3^2 + 3 - 2 = 10 = 0$$

But you missed ~~some~~ too.

The solutions of $x^2 + x - 2 = 0$ in $\mathbb{Z}_{10}$ are 1, 3, and 8.

How did we miss 3?

The reason is that its not true that if $ab = 0$ in $\mathbb{Z}_{10}$ then either $a = 0$ or $b = 0$, because we have

$$2 \cdot 5 = 0$$

$$(\underset{3}{x-1})(\underset{3}{x+2}) = 0$$

This is important stuff and we make some definitions about it.

Definition Nonzero element a in a ring is a **zero divisor** if $ab = 0$ for a nonzero element b.

{ p divides q : $pr = q$
{ p divides 0 : $pr = 0$

Ex Zero divisors in $\mathbb{Z}_{10}$: $2, 5$

Ex Zero divisors in $\mathbb{Z}_{12}$: $2, 3, 4, 6, 8, 10$

$$2 \cdot 6 = 0$$
$$3 \cdot 8 = 0$$
$$4 \cdot 3 = 0$$
$$10 \cdot 6 = 0$$

> **Theorem** The zero divisors of $\mathbb{Z}_n$ are those elements not rel. prime to n.

Not all zero divisors can be found this way though.

Ex $\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}$ is a zero divisor in $M_2(\mathbb{R})$.

$\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. There are many more.

> **Observation** Solving a quadratic by factoring works if and only if the ring has no zero divisors.

Cancellation Laws For a Ring.

We would like a ring to satisfy $ac = bc \Rightarrow a = b$ for any nonzero c.
and $ca = cb \Rightarrow a = b$

Unfortunately this may not always be the case.

Example In $\mathbb{Z}_{12}$ $8 \cdot 3 = 4 \cdot 3$ but $8 \neq 4$.

Theorem Cancellation in R hold if and only if R has no 0 divisors.

Reason: $ac = bc \iff ac - bc = 0 \quad (a-b)c = 0 \iff a - b = 0 \iff a = b$.

Obviously, we want our rings not to have zero divisors. They are bad.

Definition An *integral domain* is a commutative ring with 1 and no zero divisors.

Ex $\mathbb{Z}$ $\mathbb{R}$ $\mathbb{C}$ $\mathbb{Q}$

Ex $\mathbb{Z}_2$ $\mathbb{Z}_3$ $\mathbb{Z}_5$ $\mathbb{Z}_7$ ... $\mathbb{Z}_p$ p prime.

Ex Polynomials $\mathbb{R}[x] = \{ a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \}$

Be careful because an integral domain is not the deluxe model yet. Its not a field. Not every element will have a multiplicative inverse.

However we do have:

Theorem Every finite integral domain is a field.

Theorem $\mathbb{Z}_p$ is a field when p is prime.

Characteristic of a ring

If R is a ring, its characteristic is the smallest pos. integer n for which $na = 0$ $\forall a \in R$. If no such n exists, R has characteristic 0.

Theorem If R has 1, then its characteristic is the smallest n for which $n \cdot 1 = 0$.

Ex $\mathbb{Z}_8 \times \mathbb{Z}_6$ characteristic 24.

Ex $\mathbb{Z}_5$ characteristic 5

Ex $\mathbb{R}$ characteristic 0.