Monday
1/27

Def: Let R be a ring.

① Let $a \in R$. Then a is called a *zero divisor* if $a \neq 0$ and there exists $b \in R$ with $b \neq 0$ and either $ab = 0$ or $ba = 0$.

② Assume R has identity 1, with $1 \neq 0$.
An element $u \in R$ is called a *unit* if there exists $v \in R$ with $uv = vu = 1$.
We denote the set of units of R by $R^\times$.

Ex: $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\mathbb{Z}_6, \cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

zero divisors: $\bar{2}, \bar{3}, \bar{4}$

$\bar{2} \cdot \bar{3} = \bar{0}$ ← $\bar{2}$ & $\bar{3}$ are zero divisors

$\bar{4} \cdot \bar{3} = \bar{0}$ ← $\bar{4}$ is also a zero divisor

units:

$\bar{1} \cdot \bar{1} = \bar{1}$

$\bar{5} \cdot \bar{5} = \bar{1}$

} units are $\bar{1}, \bar{5}$

$\mathbb{Z}_6^{\times} = \{\bar{1}, \bar{5}\}$

Ex: Units of $\mathbb{Z}$ are $\mathbb{Z}^\times = \{1, -1\}$

There are no zero-divisors in $\mathbb{Z}$ [that is, if $ab = 0$ then $a = 0$ or $b = 0$]

Ex: Let F be a field, such as $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$.

Then $F^\times = F - \{0\}$.

Ex: $R = \{0\}$

no units
no zero divisors

Def: R is an integral domain if R is a commutative ring with identity $1 \neq 0$, and R has no zero divisors [that is, if $ab = 0$ then either $a = 0$ or $b = 0$]

Integral domains

$\mathbb{Z}$

$\mathbb{Q}$

$\mathbb{R}$

$\mathbb{C}$

$\mathbb{Z}_p$, p prime

$\mathbb{Z}_6$ is not an integral domain. because it has zero divisors: $\bar{2} \cdot \bar{3} = \bar{0}$

$\mathbb{Z}_n$, if $n \geq 4$ and n is composite, is not an integral domain.

pf: If n is composite then $n = ab$, $1 < a, b < n$.

So, $\bar{0} = \bar{n} = \bar{a}\,\bar{b}$.

↑ ↑ neither of these are $\bar{0}$

$\mathbb{Z}_p$ is a field (if p is prime)

proof: $\mathbb{Z}_p$ is a commutative ring with identity $\bar{1} \neq \bar{0}$.

Why does every non-zero element $\bar{a} \neq \bar{0}$ have an inverse? Since $\bar{a} \neq \bar{0}$ we have $p \nmid a$.

So, $\gcd(a, p) = 1$ [we used p is prime]

So there exist integers x and y such that

$ax + py = \gcd(a,p) = 1$.

So in $\mathbb{Z}_p$ we get

$\bar{a}\bar{x} + \bar{p}\bar{y} = \bar{1}$. ← $\bar{p} = \bar{0}$

So, $\bar{a}\bar{x} = \bar{1}$. So, $\bar{a}$ is a unit.

MATH 4460

Thm: Let F be a field.
Then F is an integral domain.

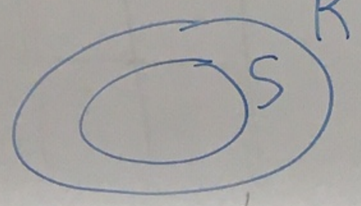
Proof: Since F is a field
we know F is a commutative
ring with $1 \neq 0$.
Let's show F has no zero-divisors.
Suppose $a, b \in F$ with $\boxed{ab = 0}$.
We need to show $a = 0$ or $b = 0$.

case 1: If $a = 0$, then we are done.

case 2: Suppose $a \neq 0$. Then a is a unit [because F is a field].
So, a^{-1} exists with $\boxed{a^{-1}a = aa^{-1} = 1}$. So, $b = a^{-1}ab = a^{-1}0 = 0$.

So, F has no zero divisors. ▨

Def: A **subring** S of a ring R is a subset of R that is also a ring under the same operations as R.



Ex:

$2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

$\mathbb{Z}$ is a subring of $\mathbb{R}$.

7.2 - Examples

Def: Let R be a commutative ring with identity.

The ring

$$R[x] = \left\{ a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \;\middle|\; \begin{array}{l} a_0, a_1, a_2, \ldots, a_n \in R \\ n \in \mathbb{Z},\ n \geq 0 \end{array} \right\}$$

is called the ring of polynomials in the variable x with coefficients in R.

You can verify that $R[x]$ is a ring under the usual addition and multiplication.

If $a_n \neq 0$, then $\deg(a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0) = n$

deg is for degree

Ex: $\mathbb{Z}_3[x] = \{\bar{0}, \bar{1}, \bar{2}, x, \bar{2}x, \bar{1}+x, \bar{1}+\bar{2}x, \bar{2}+x, \bar{2}+\bar{2}x, x^2, \dots\}$

Units of $\mathbb{Z}_3[x]$, $(\mathbb{Z}_3[x])^\times = \mathbb{Z}_3^\times$

$\mathbb{Z}_3$ is an integral domain

Zero polynomial

$\bar{1}\cdot x$

$$(\bar{2}+\bar{2}x+\bar{2}x^2)+(\bar{2}+x) = \bar{1}+\bar{2}x^2$$

$$(\bar{1}+x)(x+\bar{2}x^2) = x+\bar{2}x^2+x^2+\bar{2}x^3 = x+\bar{2}x^3$$

Ex: In $\mathbb{Z}_6[x]$

$$(\bar{1}+\bar{2}x^2)(\bar{3}+\bar{3}x^5) = \bar{3}+\bar{3}x^5+\bar{6}x^2+\bar{6}x^7 = \bar{3}+\bar{3}x^5$$

degree 2 · degree 5 · $\bar{6}=\bar{0}$ · degree 5

Prop: Let R be an integral domain.
Let $p(x), q(x) \in R[x]$ where $p(x)$ and $q(x)$ are non-zero. Then:

1. $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$
2. the units of $R[x]$ are just the units of R. That is, $(R[x])^\times = R^\times$.
3. $R[x]$ is an integral domain