§1 2019-11-01 Rings

Definition 1.1. A ring is a set R with two binary operations.

1. (+ is associative): $(a+b)+c = a+(b+c)$
2. There is an additive identity element $0 \in R$ such that $a+0 = a = 0+a$ for all $a \in R$.
3. Each $a \in R$ has an additive inverse $-a$ such that $a + -a = 0 = -a + a$
4. $+$ is commutative: $a+b = b+a$ for all $a, b \in R$.
5. Multiplication is associative: $a \cdot (bc) = (ab) \cdot c$
6. Left / right distributive: $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$

Definition 1.2. If R has a multiplicative identity element $1 \neq 0$ such that $1a = a = a1\ \forall a$ then R is a ring with unity / identity

If multiplication is commutative, R is a commutative ring.

If R is commutative with 1 and $(ab = 0) \Rightarrow (a = 0 \text{ or } b = 0)$, then R is an integral domain

If R has the identity element and every $x \neq 0$ has a multiplicative inverse in R then R is a division ring. i.e. $(R - \{0\}, \cdot) = (\mathbb{R}^*, \cdot)$ is a group.

If $(R^*, \cdot)$ is a commutative group then R is a field.

Example 1.3

$$\text{Integral domain: } (\mathbb{Z}, +, \cdot)$$
$$\text{Fields: } (\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{C}, +, \cdot)$$
$$\text{Commutative Ring: } (\mathbb{Z}_n, +, \cdot)$$
$$(\mathbb{Z}_p, +, \cdot) \text{ is a field because } a^{p-1} \equiv_p 1 \text{ for } a \neq 0 \text{ so } (a)(a^{p-2}) \text{ are inverses.}$$

$\mathbb{Z}_n$ is not a field when $n > 1$ is not prime. One example is $3 \in \mathbb{Z}_6$ which doesn't have a multiplicative inverse. $\mathbb{Z}_n$ is also not an integral domain when n is not prime. e.g. $3 \cdot 2 \equiv_6 = 0$ even though neither 3 nor 2 are equal to 0.

$\mathbb{Z}_1$ is commutative and $ab = 0 \Rightarrow a = 0$ or $b = 0$ but not a ring with unity because unity must be satisfied by an element other than the additive identity element. There is only one element so this is not possible.

Definition 1.4. A non zero element $a \in R$ such that $ab = 0$ but $b \neq 0$ is a zero divisor. A unit $u \in R$ is an element with a multiplicative inverse.

Definition 1.5. $\mathbb{Z}[x]$ is a ring of all polynomials with integer coefficients.
A polynomial $a_n x^n + a_{n-1}^{n-1} + \cdots = a_1 x^1 + a_0$ has degree n if $a_n \neq 0$ has degree n if $a_n \neq 0$. Add polynomials by corresponding coefficients. Multiply by multiplying and

then combining like terms.

$\mathbb{Z}[x]$ is an integral domain! It's commutative, it has unity, and there is no way to multiply two non zero polynomials and get 0.