AlgebraNotes07
Rings

Definition. A ring $(R, +, \cdot)$ is a set with two binary operations such that

i. $(R, +)$ is a commutative (addition) group;

ii. the multiplication operator $\cdot$ is associative;

iii. the operation $\cdot$ distributes over the operation $+$ so that for elements $a, b, c \in R$ we have:

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (b + c) \cdot a &= b \cdot a + c \cdot a. \end{aligned}$$

Theorem 8.1. For the ring $(R, +, \cdot)$ with additive identity 0 and $a, b \in R$ we have:

$$\begin{aligned} 0a = a0 &= 0 \\ a(-b) = (-a)b &= -(ab) \\ (-a)(-b) &= ab. \end{aligned}$$

Definition. If $(R_1, +_1, \cdot_1)$ and $(R_2, +_2, \cdot_2)$ are rings and $\varphi : R_1 \to R_2$ is a function then φ is a ring homomorphism means that, for $a, b \in R_1$:

$$\begin{aligned} \varphi(a +_1 b) &= \varphi(a) +_2 \varphi(b) \\ \varphi(a \cdot_1 b) &= \varphi(a) \cdot_2 \varphi(b). \end{aligned}$$

Definition. If $(R, +, \cdot)$ is a ring then it is called a division ring if R has a multiplicative identity 1 with $1 \neq 0$ and each element x of R has a multiplicative inverse so that:

$$xx^{-1} = x^{-1}x = 1.$$

Definition. R is a field means that R is a division ring in which the multiplication operation is commutative.

Definition. If R is a ring then the element $a \neq 0$ is called a zero divisor if there is an element $b \in R$ with $b \neq 0$ so that either $ab = 0$ or $ba = 0$.

Exercise. 8.1. If $R = (\mathbb{Z}_n, +_n, \cdot_n)$, then R is a finite ring.

[Notation: The statement "R is the ring Z_n" is a shorthand statement that means that, with the canonical operations $+_n, \cdot_n$, R is the ring $(\mathbb{Z}_n, +_n, \cdot_n)$.]

Theorem 8.2. Let R be the ring $\mathbb{Z}_n$ then $a \neq 0$ is a zero divisor in $\mathbb{Z}_n$ if and only if $\gcd(a, n) \neq 1$.

Definition. The ring R is an integral domain means that R is a commutative ring (with respect to multiplication as well as addition) with a multiplicative identity $1 \neq 0$ which has no zero divisors.

Theorem 8.3. If F is a field and $a, b \in F$ are such that $ab = 0$, then either $a = 0$ or $b = 0$.

Exercises 8.2:

a. What are the zero divisors of the ring $\mathbb{Z}_{14}$? of the ring $\mathbb{Z}_3 \times \mathbb{Z}_6$; what is the multiplicative identity?

b. Verify that with the natural definition of operations on products, that if each of R_1 and R_2 is a ring then $R_1 \times R_2$ is a ring.

c. Show that the ring $\mathbb{Z}_{pq}$ for p and q integers greater than 1, is not a division ring.

d. Determine for which integers n the ring $\mathbb{Z}_n$ is a division ring.

Exercises 8.3. Suppose that $\varphi : R_1 \to R_2$ is a ring homomorphism verify the following (add additional assumptions that you need - e.g. multiplicative inverses etc.)

$$\begin{aligned}
\varphi(0) &= 0 \\
\varphi(-x) &= -\varphi(x) \\
\varphi(1) &= 1 \\
\varphi(x^{-1}) &= (\varphi(x))^{-1}.
\end{aligned}$$

Theorem 8.4. Suppose that $(R, +, \cdot)$ is a ring with a multiplicative identity. Then the set of all invertible elements of R form a Group.

Theorem 8.5. Let $R_p = \{a + p\mathbb{Z} | a \in \mathbb{Z}\}$ be set of cosets of pZ in the ring $\mathbb{Z}$. Define $\oplus$ and $\otimes$ on R_p by:

$$\begin{aligned}
(a + p\mathbb{Z}) \oplus (b + p\mathbb{Z}) &= (a + b) + p\mathbb{Z} \\
(a + p\mathbb{Z}) \otimes (b + p\mathbb{Z}) &= ab + p\mathbb{Z}
\end{aligned}$$

Then $(R_p, \oplus, \otimes)$ is a ring and is isomorphic to $\mathbb{Z}_p$.

Theorem 8.6. If p is a prime number then for any integer $a > 1$ such that p does not divide a we have $a^{p-1} \equiv_p 1$.

Theorem 8.7. Let $G_n = \{x \in Z_n | x \neq 0, x \text{ is not a zero divisor }\}$. Then $(G_n, \cdot_n)$ is a group.

Theorem 8.8. Suppose $a, b \in \mathbb{Z}_n$ and $d = \gcd(a, n)$. Then the equation $ax = b$ has a solution if and only if $d|b$. Furthermore, in that case it has exactly d solutions.

Exercise 8.4. For the selected rings, solve the indicted equations or determine if they do not have solutions. [Note that I am suppressing the equivalence class notation $[\cdot]_n$.]

a.) $R = \mathbb{Z}_{13}$

$$
\begin{array}{rcl}
7x & = & 4 \\
6 - 4x & - & 5 \\
3x - 2 & = & 2 \\
3x - 5 & = & 4 \\
x^2 & = & 0 \\
6x & = & 0 \\
(2x - 4)(7x + 3) & = & 0.
\end{array}
$$

b.) $R = \mathbb{Z}_{15}$

$$
\begin{array}{rcl}
7x & = & 4 \\
6 - 4x & - & 5 \\
3x - 2 & = & 2 \\
3x - 5 & = & 4 \\
x^2 & = & 0 \\
6x & = & 0 \\
(2x - 4)(7x + 3) & = & 0.
\end{array}
$$