Definitions for Abstract Algebra

Riley Weber

February 19, 2020

Taken from Abstract Algebra: An Introduction by Thomas W. Hungerford (ISBN 978-1111569624). Created to study while taking MATH 3163: Modern Algebra at UNC Charlotte. Definitions ordered as they are in the book and are sectioned by chapter.

1 Arithmetic in $\mathbb{Z}$ Revisited

1.1

Definition 1.1.1 (Well-Ordering Axiom)
every non-empty subset of the set of non-negative integers has a least element

1.2

Definition 1.2.1 (Divisibility)
Let $a, b \in \mathbb{Z}$ with $b \neq 0$. We say that b divides a and write $b \mid a$ if $a = bc$ for some $c \in \mathbb{Z}$.

Definition 1.2.2 (Greatest Common Divisor)
Let $a, b \in \mathbb{Z}$, not both zero. The greatest common divisor (gcd) is the greatest integer that divides both a and b. This means that if d is the gcd of a and b, then

1. $d \mid a$ and $d \mid b$
2. if $c \mid a$ and $c \mid b$, then $c \leq d$

The greatest common divisor is often written $d = gcd(a, b)$ or simply (a, b). it is also frequently called the greatest common *denominator*.

1.3

Definition 1.3.1 (Primality)
An integer p is said to be **prime** if $p \neq 0, \pm 1$ and the only divisors of p are ± 1 and $\pm p$.

2 Congruence in $\mathbb{Z}$ and Modular Arithmetic

2.1

Definition 2.1.1 (Congruence Modulo n)
Let $a, b, n \in \mathbb{Z}$ and $n > 0$. We say a is congruent to b modulo n and write $a \equiv b(modn)$ if $n \mid a - b$.

Definition 2.1.2 (Congruence Class)
Let $a, n \in \mathbb{Z}$ and $n > 0$. The congruence class of a modulo n (written $[a]_n$ or $[a]$) is the set of all integers that are congruent to to a modulo n. That is, $[a] = \{b|b \in \mathbb{Z} \text{ and } b \equiv a(modn)\}$

Definition 2.1.3 (The Set of All Congruence Classes)
$\mathbb{Z}_n$, read "$\mathbb{Z}$ mod n" is the set of all congruence classes modulo n. Note that for every n where $n \in \mathbb{Z}$ and $n > 1$, $\mathbb{Z}_n$ is a finite set, but each congruence class in that set is an infinite set.

2.2

Definition 2.2.1 (Addition and Multiplication in $\mathbb{Z}_n$)
$[a] \oplus [b] = [a + b]$
$[a] \odot [b] = [a \cdot b]$

2.3

Definition 2.3.1 (Unit)
Let $n \in \mathbb{N}$. A member of $\mathbb{Z}_n$ is a **unit** of $\mathbb{Z}_n$ if the equation $a \odot x = [1]$ has a solution in $\mathbb{Z}_n$.

3 Rings

3.1

Definition 3.1.1 (Ring)
A ring is a nonempty set R equipped with two operations (usually written as addition and multiplication) that satisfy the following axioms.

For all $a, b, c \in R$:

1.	If $a \in R$ and $b \in R$, then $a + b \in R$	[Closure for addition]
2.	$a + (b + c) = (a + b) + c$	[Associative addition]
3.	$a + b = b + a$	[Commutative addition]
4.	There is an element $0_R \in R$ such that $a + 0_R = a = 0_R + a$ for every $a \in R$	[Additive identity or zero element]
5.	For each $a \in R$, the equation $a + x = 0_R$ has a solution in R	[Additive inverse]
6.	If $a \in R$ and $b \in R$, then $ab \in R$	[Closure for multiplication]
7.	$a(bc) = (ab)c$	[Associative multiplication]
8.	$a(b + c) = ab + ac$ and $(a + b)c = ac + bc$	[Distributive laws]

Definition 3.1.2 (Commutative Ring)
A commutative ring is a ring R in which $ab = ba$ for all $a, b \in R$ (commutative multiplication).

Definition 3.1.3 (Ring with Identity)
A ring with identity is a ring R that contains a special element 1_R such that $a \cdot 1_R = a = 1_R \cdot a$ for all $a \in R$ (multiplicative identity).