Definitions for Abstract Algebra

Riley Weber

March 29, 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 are ordered as they are in the book and 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 $\mathbb{Z}_n$. In this case, the element x is called the **multiplicative inverse** and is denoted a^{-1}

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]

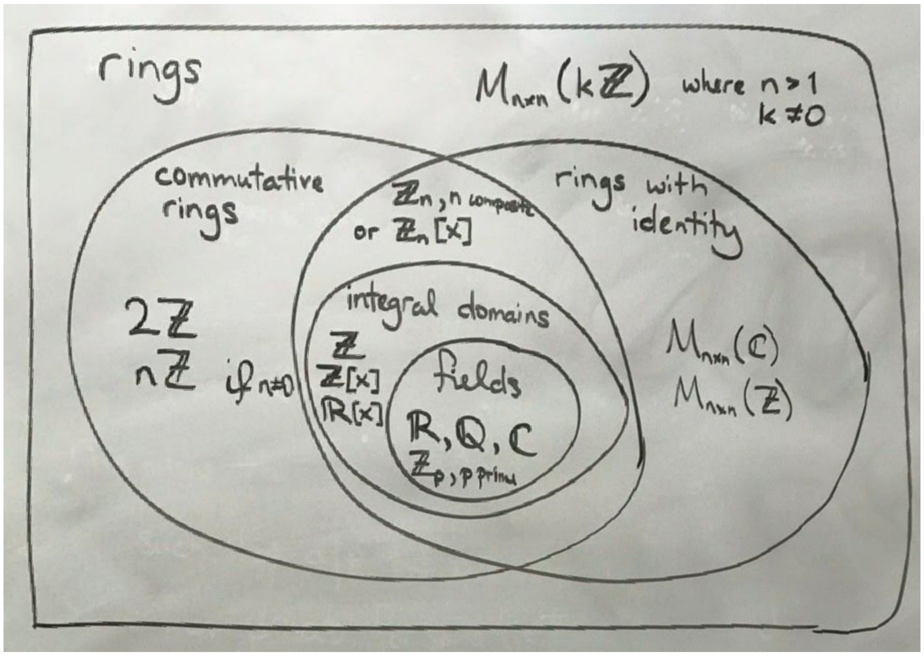
Definition 3.1.2 (Commutative Ring)
A commutative ring is a ring R in which $ab = ba$ for all $a, b \in R$ (commutative multiplication).

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).

Definition 3.1.4 (Integral Domains)
An integral domain is a commutative ring R with identity such that if $a, b \in R$ and $ab = 0_R$ then either $a = 0_R$ or $b = 0_R$.

Definition 3.1.5 (Field)
A field is a commutative ring R with identity 1_R such that if $a \in R \setminus \{0_R\}$ then a is a unit (i.e. the equation $ax = 1_R$ has a solution in R)

Following is a diagram which illustrates what common sets are also rings, fields, and the like.



4 Arithmetic in $F[x]$

4.1 Polynomial Arithmetic and the Division Algorithm

Definition 4.1.1 (Polynomials)
Note: this "definition" is listed as theorem 4.1 in the book. However, since it is assumed in the text and honestly it defines what it means to be a polynomial, it has been included here.

Suppose R is a ring. Then, $R[x]$ is the ring of polynomials with coefficients in R; i.e., $R[x] = R \cup \{r_0 + r_1x + r_2x^2 + ... + r_nx^n : r_0, ..., r_n \in R \text{ and } r_n \neq 0_R\}$

Here x is just a letter. Also, notice that saying $R[x] = R \cup \{r_0 + r_1x + r_2x^2 + ... + r_n\}$ is redundant. The content of the curly braces includes R, because R is the special case of $R[x]$ where all coefficients except r_0 are 0_R. It is included in this definition for emphasis only.

Observations:

- R is a subring of $R[x]$
- The members of R are called the "constant polynomials" in $R[x]$.

Definition 4.1.2 (Degrees and Leading Coefficients)
If $f(x) \in R[x] \setminus R$, then $f(x) = r_0 + r_1x + r_nx^n$ for some $n \in \mathbb{N}$ and $a_n \neq 0_R$. We say:

- n is the **degree** of $f(x)$. This is often denoted "deg $f(x)$" or "deg(f)".

- r_n is the **leading coefficient** of $f(x)$

There are a couple things to note about the degree of a polynomial:

- If $f(x) \in R \setminus \{0_R\}$, then the degree of $f(x)$ in $R[x]$ is 0. Note that this means $f(x)$ have no variable terms, no x.
- The degree of 0_R in $R[x]$ is undefined. (But it can make sense to think of it as having degree $-\infty$)

5 Divisibility in $F[x]$

Definition 5.0.1 (Greatest Common Denominators in Polynomials)
Let F be a field and let $f(x), g(x) \in F[x]$ with at least one of them not equal to 0_F. Then, the **greatest common divisor** of $f(x)$ and $g(x)$ is the unique, monic $d(x) \in F[x] \setminus \{0_F\}$ such that

1. $d(x) \mid f(x)$ and $d(x) \mid g(x)$
2. if $h(x) \mid f(x)$ and $h(x) \mid g(x)$ for some $h(x) \in F[x]$, then $deg(h) \leq deg(d)$

This is often written as $d(x) = gcd(f(x), g(x))$

Definition 5.0.2 (Relative Primality)
Let F be a field and let $f(x), g(x) \in F[x]$, not both 0_F. (read "f and g are polynomials under the field F, not both zero). We say $f(x)$ and $g(x)$ are **relatively prime** if $gcd(f(x), g(x)) = 1_F$

For example:

- $gcd(x^2 - 1, x^2 + 2x + 1) = x + 1$, so these are **not** relatively prime
- $gcd(x^2 - 1, x^3 + x) = 1$, so these **are** relatively prime