

CS 225

Some Definitions and Theorems from Chapter 4

Fall 2020

From 4.1:

Assumptions:

- Basic laws of algebra from appendix A (I assume we do not have to cite these—I listed some on the last page of this document)
- Properties of equality: $x = x$, $x = y \implies y = x$, $x = y$ and $y = z \implies x = z$
- Principle of substitution: if $x = y$, then we can substitute in y wherever x appears.
- The integers are closed under addition, subtraction and multiplication. (The book also mentions that there is no integer between 0 and 1—does that need to be an assumption??)

Definitions:

- An integer n is **even** if and only if it can be written as $n = 2k$ for some integer k .
- An integer n is **odd** if and only if it can be written as $n = 2k + 1$ for some integer k .
- An integer n is **prime** if and only if $n > 1$ and for all positive integers r and s , if $n = rs$, then either r or s equals n .
- An integer n is **composite** if and only if $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

Theorem 4.1.1

The sum of any two even integers is even.

From 4.2:

Theorem 4.2.1:

The difference of any odd integer and any even integer is odd.

From 4.3:

Definition:

A real number r is **rational** if and only if there are integers a and b with $b \neq 0$ so that $r = \frac{a}{b}$

Property:

The zero product property is: if neither of two real numbers is zero, then their product is also not zero. (this is T11 in appendix A)

Theorem 4.3.1:

Every integer is a rational number.

Theorem 4.3.2:

The sum of any two rational numbers is a rational number.

Corollary 4.2.3:

The double of a rational number is a rational number.

Result of Exercise 12:

The square of any rational number is a rational number.

Result of Exercise 13:

The negative of any rational number is a rational number.

Result of Exercise 14:

The cube of any rational number is a rational number.

Result of Exercise 15:

The product of any two rational numbers is a rational number.

Result of Exercise 17:

The difference of any two rational numbers is a rational number.

From 4.4:

Definition:

If n and d are integers, then n is **divisible by** d if and only if $d \neq 0$ and $n = kd$ for some integer k .

Some synonyms for “ d divides n ”:

- n is a multiple of d
- d is a factor of n
- d is a divisor of n
- d divides n
- $d \mid n$

The notation $d \nmid n$ means “ d does not divide n ”.

Theorem 4.4.1:

For all integers a and b , if a and b are positive and a divides b then $a \leq b$.

Theorem 4.4.2:

The only divisors of 1 are 1 and -1 .

Theorem 4.4.3:

For all integers a, b and c , if a divides b and b divides c , then a divides c .

Theorem 4.4.4:

Any integer $n > 1$ is divisible by a prime number.

Theorem 4.4.5:

Given any integer $n > 1$ there exists a positive integer k , distinct prime numbers p_1, p_2, \dots, p_k , and positive integers e_1, e_2, \dots, e_k such that

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} = \prod_{i=1}^k p_i^{e_i}$$

and any other expression for n as a product of prime numbers is identical to this except perhaps for the order in which the factors are written.

Definition:

Given any integer $n > 1$, the **standard factored form** of n is an expression of the form

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} = \prod_{i=1}^k p_i^{e_i}$$

where k is a positive integer, p_1, \dots, p_k are prime numbers, e_1, \dots, e_k are positive integers, and $p_1 < p_2 < \dots < p_k$.

From 4.7:**Theorem 4.7.1:**

There is no greatest integer.

Theorem 4.7.2:

There is no integer that is both even and odd.

Theorem 4.7.3:

The sum of any rational number and any irrational number is irrational.

Proposition 4.7.4:

For every integer n , if n^2 is even then n is even.

From 4.8:**Theorem 4.8.1:**

$\sqrt{2}$ is irrational.

Proposition 4.8.2:

$1 + 3\sqrt{2}$ is irrational.

Proposition 4.8.3:

For any integer a and any prime number p , if $p \mid a$ then $p \nmid (a + 1)$.

Theorem 4.8.4:

The set of prime numbers is infinite (i.e. there are infinitely many prime numbers).

From Appendix A:

- Field Axioms for real numbers:
 - F1 Commutative laws for addition and multiplication
 - F2 Associative laws for addition and multiplication
 - F3 Distributive laws
 - F4 Existence of an identity for addition and multiplication
 - F5 Existence of additive inverses (negative numbers)
 - F6 Existence of multiplicative inverses (reciprocals)
- Other theorems:
 - T1 Cancellation law for addition: $a + b = a + c \implies b = c$
 - T2 Possibility of subtraction: There is a unique solution to $a + x = b$ (namely $x = b - a$)
 - T3 $b - a = b + (-a)$
 - T4 $-(-a) = a$
 - T5 $a(b - c) = ab - ac$
 - T6 $0 \cdot a = a \cdot 0 = 0$
 - T7 Cancellation law for multiplication: $ab = ac$ and $a \neq 0 \implies b = c$
 - T8 Possibility of division: If $a \neq 0$, there is a unique solution to $ax = b$. (namely $x = b/a$)
 - T9 If $a \neq 0$, $\frac{b}{a} = b \cdot a^{-1}$
 - T10 If $a \neq 0$, $(a^{-1})^{-1} = a$
 - T11 Zero product property: If $ab = 0$, then $a = 0$ or $b = 0$
 - T12 $(-a)b = a(-b) = -(ab)$, $(-a)(-b) = ab$,
$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$$
 - T13 Equivalent fractions property: $\frac{a}{b} = \frac{ac}{bc}$ if $b \neq 0$ and $c \neq 0$
 - T14 Fraction addition: $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$ if $b \neq 0$ and $d \neq 0$
 - T15 Multiplying fractions: $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$
 - T16 Dividing fractions: $\frac{a/b}{c/d} = \frac{a}{b} \cdot \frac{d}{c}$
- Order Axioms (see the appendix on page A-2)
- Order Theorems (see the appendix A-3)
- Least upper bound axiom (see the appendix A-3)