CSE 311: Foundations of Computing I

Definitions and Theorems

What Is This?

This is a complete[1] listing of definitions and theorems relevant to CSE 311. The goal of this document is less as a reference and more as a way of indicating what is and is not allowed to be assumed in proofs.

Contents

[1] It's not actually complete. It's probably missing a lot. If you find an error or a missing theorem, please let us know! We will give you a rubber ducky.

1 Arithmetic

This section is all about arithmetic. You'll find that you can basically assume anything about arithmetic that you learned in high school algebra or earlier.

1.1 Definitions

Arithmetic Expression of Real Numbers — DEFINITION

An arithmetic expression of real numbers is an expression made up of real numbers, variables representing real numbers, addition, multiplication, subtraction, division, exponentiation, and logarithms.

Zero — CONSTANT

Zero (0, the additive identity) is the constant real number such that for any arithmetic expression X, $0 + X = X = X + 0$.

One — CONSTANT

One (1, the multiplicative identity) is the constant real number such that for any arithmetic expression X, $1 \cdot X = X = X \cdot 1$.

2 Equality

This section is all about equalities. You'll find that you can basically assume anything about arithmetic that you learned in high school algebra or earlier.

2.1 Definitions

Equality for Real Numbers — DEFINITION

If X and Y are two real numbers, then $X = Y$ ("X equals Y") when both expressions "evaluate" to the same real number.
(This means you should use what you learned in high school about these types of expressions.)

Inequality for Real Numbers — DEFINITION

If X and Y are two real numbers, then $X \neq Y$ ("X does not equal Y") when $\neg(X = Y)$.

2.2 Givens

Reflexivity of Equality for Real Numbers — GIVEN

If x is a real number, then $x = x$.

Symmetry of Equality for Real Numbers — GIVEN

If x, y are real numbers, then $x = y \leftrightarrow y = x$.

Transitivity of Equality for Real Numbers — GIVEN

If x, y, and z are real numbers, then $(x = y \wedge y = z) \rightarrow x = z$.

Identities for Real Numbers GIVEN

If x is a real number, then:

- $x + 0 = x = 0 + x$
- $x \cdot 1 = x = 1 \cdot x$
- $x^0 = 1$ (unless x evaluates to 0, in which case x^0 is undefined)
- $0^x = 0$ (unless x evaluates to 0, in which case 0^x is undefined)
- $1^x = 1$
- $x/1 = x$

Domination for Real Numbers GIVEN

If x is a real number, then:

- $x \cdot 0 = 0 = 0 \cdot x$
- $x \cdot 1 = x = 1 \cdot x$

Inverse Operations for Real Numbers GIVEN

If a and b are real numbers, then:

- $a - b = a + (-b)$
- $a \cdot \frac{b}{a} = b$

Inverses for Real Numbers GIVEN

If x and b are real numbers, then:

- $x + (-x) = 0 = (-x) + x$
- $x \cdot \frac{1}{x} = 1 = \frac{1}{x} \cdot x$ (unless x evaluates to 0)
- $b^{\log_b(x)} = x$
- $\log_b(b^x) = x$
- $-(-x) = x$

Associativity of Arithmetic Expressions GIVEN

If x, y, and z are real numbers, then:

- $(x + y) + z = x + (y + z)$
- $(xy)z = x(yz)$

As a consequence, we can omit the parentheses in these expressions.

Commutativity of Arithmetic Expressions GIVEN

If x and y are real numbers, then:

- $x + y = y + x$
- $xy = yx$

Distributivity of Arithmetic Expressions GIVEN

If $a, b, c,$ and d are real numbers, then:

- $a(b+c) = ab + ac$
- $(a+b)(c+d) = ac + ad + bc + bd$

Algebraic Properties of Real Numbers GIVEN

If a, b, c, and d are real numbers, then:

- $\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}$
- $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$
- $(a^b)(a^c) = a^{b+c}$
- $\left(a^b\right)^c = a^{bc}$
- $\log_c(ab) = \log_c(a) + \log_c(b)$
- $\log_c\left(\frac{a}{b}\right) = \log_c(a) - \log_c(b)$

Adding Equalities GIVEN

If a and b are real numbers, $a = b$, and $c = d$, then $a + c = b + d$.

Multiplying Equalities GIVEN

If a and b are real numbers, $a = b$, and $c = d$, then $ac = bd$.

Dividing Equalities GIVEN

If a and b are real numbers, $a = b$, and $c \neq 0$, then $\frac{a}{c} = \frac{b}{c}$

Subtracting Equalities GIVEN

If a and b are real numbers, $a = b$, and $c = d$, then $a - c = b - d$.

Raising Equalities To A Power GIVEN

If a and b are real numbers and $a = b$, then $a^c = b^c$.

Log Change-Of-Base Formula GIVEN

If x, a, and b are real numbers, $x, a, b > 0$, $a \neq 1$, $b \neq 1$, then $\log_a(x) = \frac{\log_b(x)}{\log_b(a)}$

3 Inequalities

This section is all about inequalities. You'll find that you can basically assume anything about arithmetic that you learned in high school algebra or earlier.

3.1 Definitions

Less-Than for Real Numbers DEFINITION

If x and y are two real numbers, then $x < y$ ("x is less than y") when x "evaluates" to a smaller real number than y evaluates to.
(This means, use what you learned in high school about these types of expressions.)

Greater-Than for Real Numbers DEFINITION

If x and y are two real numbers, then $x > y$ ("x is greater than y") when $y < x$.

Less-Than-Or-Equal-To for Real Numbers DEFINITION

If x and y are two real numbers, then $x \leq y$ ("x is less than or equal to y") when $\neg(x > y)$.

Greater-Than-Or-Equal-To for Real Numbers DEFINITION

If x and y are two real numbers, then $x \geq y$ ("x is greater than or equal to y") when $\neg(x < y)$.

3.2 Givens

Trichotomy for Real Numbers GIVEN

If x and y are two real numbers, then $x = y \vee x < y \vee x > y$.

Antisymmetry of Inequality for Real Numbers GIVEN

If x, y are real numbers, then $(x \leq y \wedge y \leq x) \to x = y$.

Transitivity of Inequality for Real Numbers GIVEN

If x, y, and z are real numbers, then $(x < y \wedge y < z) \to x < z$.

Adding Inequalities GIVEN

If a and b are real numbers, $a < b$ and $c < d$, then $a + c < b + d$.

Subtracting Inequalities GIVEN

If a and b are real numbers and $a < b$ and $c > d$, then $a - c < b - d$.

Multiplying (Positive) Inequalities GIVEN

If a and b are real numbers, $0 < a < b$ and $0 < c < d$, then $0 < ac < bd$.

Multiplying (Negative) Inequalities GIVEN

If a and b are real numbers, $a < 0$, and $b < 0$, then $ab > 0$.

Inverting Inequalities GIVEN

If a and b are real numbers and $0 < a < b$, then $\frac{1}{a} > \frac{1}{b} > 0$.

Same Sign GIVEN

If a and b are real numbers and $ab > 0$, then a and b are both positive or a and b are both negative.

Squares Are Positive GIVEN

If a is a real number, then $a^2 \geq 0$.

4 Absolute Value

This section is all about absolute values. In general, we don't care much about absolute values, but they're something easy to prove things about. So, we list out a bunch of givens you may use here.

4.1 Definitions

Absolute Value DEFINITION

If x is a real number, then

$$|X| = \begin{cases} X & \text{if } X \geq 0 \\ -X & \text{if } X < 0 \end{cases}$$

4.2 Givens

Absolute Value Magnitude GIVEN

If x and M are real numbers and $M \geq 0$, then $|x| \leq M \leftrightarrow -M \leq x \leq M$.

Positive Definite GIVEN

If x is a real number, then $|x| \geq 0$ and $|x| = 0 \leftrightarrow x = 0$.

Multiplying Absolute Values GIVEN

If x and y are real numbers, then $|xy| = |x||y|$

Triangle Inequality GIVEN

If x and y are real numbers, then $|x + y| \leq |x| + |y|$.

5 Parity

This section is all about parity (even-ness/odd-ness) of integers. Unlike all the previous sections, we will use this as a starting point for discussing proofs. This means that you may *only* assume what is written here explicitly and nothing more.

5.1 Definitions

Even DEFINITION

An integer n is *even* iff $\exists k\ (n = 2k)$

Odd — Definition

An integer n is *odd* iff $\exists k \; (n = 2k + 1)$

Perfect Square — Definition

An integer n is a *perfect square* iff there exists an integer x for which $n = x^2$.

Closure Under $\star$ — Definition

A set S is *closed* under a binary operation $\star$ iff $x \star x$ is an element of S.

5.2 Theorems

$\mathbb{Z}$ is closed under $+$ — Theorem

The integers are closed under addition.

$\mathbb{Z}$ is closed under $\times$ — Theorem

The integers are closed under multiplication.

The square of every even integer is even — Theorem

If n is even, then n^2 is even.

The square of every odd number is odd — Theorem

If n is odd, then n^2 is odd.

The sum of two odd numbers is even — Theorem

If n and m are odd, then $n + m$ is even.

No even number is the largest even number — Theorem

For all even numbers n, there exists a larger even number m.

$\mathbb{Z}$ is closed under $-$ — Theorem

The integers are closed under subtraction.

$\mathbb{Z}$ is not closed under $/$ — Theorem

The integers are *not* closed under division.

No Integer is Odd and Even — Theorem

If n is an integer, n is not both odd and even.

Every Integer is Odd or Even — Theorem

If n is an integer, n is even or odd.

6 Rationals

This section is all about rational numbers. We also use proofs about rational numbers as a starting point for discussing proofs. This means that you may *only* assume what is written here explicitly and nothing more.

6.1 Definitions

Rational — Definition

An real number x is *rational* iff there are two integers p and $q \neq 0$ such that $x = \frac{p}{q}$.

6.2 Theorems

$\mathbb{Q}$ is closed under $\times$ — Theorem

The rationals are closed under multiplication

$\mathbb{R} \setminus \mathbb{Q}$ is not closed under $+$ — Theorem

The irrationals are not closed under addition.

7 Sets

7.1 Definitions

The Set of Natural Numbers — Definition

$\mathbb{N} = \{0, 1, 2, \ldots\}$ is the set of *Natural Numbers*

The Set of Integers — Definition

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the set of *Integers*.

The Set of Rationals — Definition

$\mathbb{Q} = \left\{ \dfrac{p}{q} \;:\; p, q \in \mathbb{Z} \land q \neq 0 \right\}$ is the set of *Rational Numbers*.

The Set of Reals — Definition

$\mathbb{R}$ is the set of *Real Numbers*.

Set Inclusion — Definition

If A and B are sets, then $x \in A$ ("x is an *element* of A") means that x is an element of A, and $x \notin A$ ("x is *not* an *element* of A") means that x is *not* an element of A.

Set Equality — Definition

If A and B are sets, then $A = B$ iff $\forall x \; (x \in A \leftrightarrow x \in B)$.

Subset and Superset — DEFINITION

If A and B are sets, then $A \subseteq B$ ("A is a *subset* of B") means that all the elements of A are also in B, and $A \supseteq B$ ("A is a *superset* of B") means that all the elements of B are also in A.

Set Comprehension — DEFINITION

If $P(x)$ is a predicate, then $\{x \ : \ P(x)\}$ is the set of all elements for which $P(x)$ is true. Also, if S is a set, then $\{x \in S \ : \ P(x)\}$ is the subset of all elements of S for which $P(x)$ is true.

Set Union — DEFINITION

If A and B are sets, then $A \cup B$ is the *union* of A and B. $A \cup B = \{x \ : \ x \in A \vee x \in B\}$.

Set Intersection — DEFINITION

If A and B are sets, then $A \cap B$ is the *intersection* of A and B. $A \cap B = \{x \ : \ x \in A \wedge x \in B\}$.

Set Difference — DEFINITION

If A and B are sets, then $A \setminus B$ is the *difference* of A and B. $A \setminus B = \{x \ : \ x \in A \wedge x \notin B\}$.

Set Symmetric Difference — DEFINITION

If A and B are sets, then $A \oplus B$ is the *symmetric difference* of A and B. $A \oplus B = \{x \ : \ x \in A \oplus x \in B\}$.

Set Complement — DEFINITION

If A is a set, then $\overline{A}$ is the *complement* of A. If we restrict ourselves to a "universal set", $\mathcal{U}$ (a set of all possible things we're discussing), then $\overline{A} = \{x \in \mathcal{U} \ : \ x \notin A\}$.

Brackets n — DEFINITION

If $n \in \mathbb{N}$, then $[n]$ ("*brackets* n") is the set of natural numbers from 1 to n. $[n] = \{x \in \mathbb{N} \ : \ 1 \leq x \leq n\}$.

Cartesian Product — DEFINITION

If A and B are sets, then $A \times B$ is the *cartesian product* of A and B. $A \times B = \{(a, b) \ : \ a \in A, \ b \in B\}$.

Powerset — DEFINITION

If A is a set, then $\mathcal{P}(A)$ is the *power set* of A. $\mathcal{P}(A) = \{S \ : \ S \subseteq A\}$.

7.2 Theorems

Subset Containment — THEOREM

If A and B are sets, then $(A = B) \iff (A \subseteq B \wedge B \subseteq A)$.

Russell's Paradox — THEOREM

The set of all sets that do not contain themselves does not exist. That is, $\{x \ : \ x \notin x\}$ does not exist.

DeMorgan's Laws for Sets	THEOREM
If A and B are sets, then $\overline{A \cup B} = \overline{A} \cap \overline{B}$ and $\overline{A \cap B} = \overline{A} \cup \overline{B}$.	

Distributivity for Sets	THEOREM
If A and B are sets, then $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.	

$A \cap B \subseteq A$	THEOREM
If A and B are sets, then $A \cap B \subseteq A$.	

8 Modular Arithmetic

8.1 Definitions

$a \mid b$ ("a *divides* b")	DEFINITION
For $a, b \in \mathbb{Z}$, where $a \neq 0$: $a \mid b$ iff $\exists(k \in \mathbb{Z})\ b = ka$	

$a \equiv b \pmod{m}$ ("a *is congruent to* b *modulo* m)	DEFINITION
For $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$: $a \equiv b \pmod{m}$ iff $m \mid (a - b)$	

8.2 Theorems

Division Theorem	THEOREM
If $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, then there exist unique $q, r \in \mathbb{Z}$, where $0 \leq r < d$ such that $a = dq + r$. We call $q = a$ **div** d and $r = a$ **mod** d.	

Relation Between Mod and Congruences	THEOREM
If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $a \equiv b \pmod{m} \leftrightarrow a \bmod m = b \bmod m$.	

Adding Congruences	THEOREM
If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $(a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}) \rightarrow a + c \equiv b + d \pmod{m}$.	

Multiplying Congruences	THEOREM
If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $(a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}) \rightarrow ac \equiv bd \pmod{m}$.	

Squares are congruent to 0 or 1 mod 4	THEOREM
If $n \in \mathbb{Z}$, then $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.	

Additivity of mod	THEOREM
If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$	

Multiplicativity of mod — THEOREM

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

Base b Representation of Integers — THEOREM

Suppose n is a positive integer (in base b) with exactly m digits.

Then, $n = \sum_{i=0}^{m-1} d_i b^i$, where d_i is a constant representing the i-th digit of n.

Raising Congruences To A Power — THEOREM

If $a, b, i \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $a \equiv b \pmod{m} \to a^i \equiv b^i \pmod{m}$.

9 Primes

9.1 Definitions

Factor — DEFINITION

A *factor* of an integer n is an integer f such that $\exists x\ (n = fx)$. Alternatively, f is a factor of n iff $f \mid n$.

Prime — DEFINITION

A integer $p > 1$ is *prime* iff the only positive factors of p are 1 and p.

Composite — DEFINITION

A integer $p > 1$ is *composite* iff it's not prime. That is, an integer $p > 1$ is composite iff it has a factor other than 1 and p.

Trivial Factor — DEFINITION

A *trivial factor* of an integer n is 1 or n. We call it a "trivial factor", because all numbers have these factors.

Coprime / Relatively Prime — DEFINITION

Two integers, a and b, are *coprime* (or *relatively prime*) if the only positive integer that divides both of them is 1. That is, their prime factorizations don't share any primes.

9.2 Theorems

Fundamental Theorem of Arithmetic — THEOREM

Every natural number can be *uniquely* expressed as a product of primes raised to powers.

All Composite Numbers Have a Small Non-Trivial Factor — THEOREM

If n is a composite number, then it has a non-trivial factor $f \in \mathbb{N}$ where $f \leq \sqrt{n}$.

Euclid's Theorem THEOREM

There are infinitely many primes.

10 GCD

10.1 Definitions

GCD (Greatest Common Divisor) DEFINITION

The *gcd* of two integers, a and b, is the largest integer d such that $d \mid a$ and $d \mid b$.

Euclidean Algorithm ALGORITHM

```
gcd(a, b) {
   if (b == 0) {
      return a;
   }
   else {
      return gcd(b, a mod b);
   }
}
```

10.2 Theorems

GCD Property THEOREM

For any $a, b \in \mathbb{Z}^+$, $\gcd(a, b) = \gcd(b, a \bmod b)$.

Index