§1.1: Statements & Conditional Statements , §1.2: Constructing Direct Proofs , §1.3: Ch. 1 Summary

Def. A **statement** is a declarative sentence that is either true or false but not both. §1.1 p1

▷. A statement is sometimes called a proposition, but we will avoid using the word proposition for statement since the word proposititon has a more common different use in math [cf. §3.3,p86]. SC1.1.1

Def. A **conditional statement** is a statement that can be written in the form "If P then Q," where P and Q are statements. For a conditional statement $P \Rightarrow Q$, the P is called the **hypothesis** ⟨or antecedent⟩ and Q is called the **conclusion** ⟨or consequent⟩. §1.1 p5
Other terms for conditional statement: implication, if-then.

▷. **Truth Table** for a conditional statement $P \Rightarrow Q$.

line	P	Q	$P \Rightarrow Q$
1	T	T	T
2	T	F	**F**
3	F	T	T
4	F	F	T

- Let's watch Screencast 1.1.4. ⟨Screencast $x.y.z$ is for Chapter x Section y and is the z^{th} screencast for $x.y.$⟩
- Take-aways from ScreenCast 1.1.4:
  - Think of a conditional statement as a promise.
  - $P \Rightarrow Q$ is false if and only if you break your promise.

▷. §1.1 p10

Number Systems		
English	symbol	other notation
real numbers	$\mathbb{R}$	$(-\infty, \infty)$
natural numbers	$\mathbb{N}$	$\{1, 2, 3, 4, \ldots\}$
integers	$\mathbb{Z}$	$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \overset{\text{or}}{=} \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots\}$
rational numbers	$\mathbb{Q}$	$\left\{\frac{a}{b} \colon a, b \in \mathbb{Z} \text{ and } b \neq 0\right\} \overset{\text{easier}}{=} \left\{\frac{a}{b} \colon a \in \mathbb{Z} \text{ and } b \in \mathbb{N}\right\}$
irrational numbers	$\mathbb{R} \setminus \mathbb{Q}$	$\{x \in \mathbb{R} \colon x \notin \mathbb{Q}\}$

▷. In $\mathbb{R} \setminus \mathbb{Q}$, the symbol $\setminus$ is set minus (i.e., set take away) and is not a divides sign (as in $1/2 = 0.5$).

▷. Def.: a set is **closed under an operation** provided performing that operation on members of the set always produces a member of that set. Examples of operations on the set of natural numbers $\mathbb{N}$: §1.1 p10

(+) the natural numbers are closed under addition since if $x \in \mathbb{N}$ and $y \in \mathbb{N}$, then $x + y \in \mathbb{N}$

(−) the set $\mathbb{N}$ is not closed under subtraction since $1 \in \mathbb{N}$ and $17 \in \mathbb{N}$ but $1 - 17 = -16 \notin \mathbb{N}$.

Important Definitions

Def. An integer a is an **even integer** provided that there exists an $k \in \mathbb{Z}$ such that $a = 2k$. §1.2
So $a \in \mathbb{Z}$ is even provided $(\exists k \in \mathbb{Z})\ [a = 2k]$. p15

Def. An integer a is an **odd integer** provided there exists an $k \in \mathbb{Z}$ such that $a = 2k + 1$. §1.2
So $a \in \mathbb{Z}$ is odd provided $(\exists k \in \mathbb{Z})\ [a = 2k + 1]$. p15

Rmk. Each integer is either even or odd (but not both), as shown on the next page (a corollary to the Division Algorithm).

Def. A **mathematical proof** is a convincing argument (within the accepted standards of the mathematical community) that a certain mathematical statement is necessarily true. §1.2 p22

Def. A triple (a, b, c) is a **Pythagorean Triple** provided $a, b, c \in \mathbb{N}$ with $a < b < c$ and $a^2 + b^2 = c^2$. §1.2
⟨Pythagorean Triple (a, b, c) are used often in homework problems throughout this book.⟩ p29

Important Theorems and Results

ER1.2.2a. **Lemma SEE**. The sum of two even integers is an even integer. §1.2

ER1.2.2b. **Lemma SEO**. The sum of an even integer and an odd integer is an odd integer. p27

ER1.2.2c. **Lemma SOO**. The sum of two odd integers is an even integer.

ER1.2.3a. **Lemma PEA**. The product of an even integer and any integer is an even integer. §1.2

Thm1.8. **Lemma POO**. The product of two odd integers is an odd integer. p27

►. After we show these results they will be considered *Previously Shown Results*. §1.2 p21

○. ER denotes Exercise. Thm denotes Theorem.

Division Algorithm

Ex. Division Algorithm in action: a chart examining dividing an integer a by the natural number $2 = n \in \mathbb{N}$.

Write $a \in \mathbb{Z}$ as $a = 2\,(q) + r$ where the quotient $q \in \mathbb{Z}$ and the remainder $r \in \{0, 1\}$.				
a	$\frac{a}{2}$	$a = 2\,(q) + r$	quotient $q \in \mathbb{Z}$	remainder $r \in \{0, 1\}$
5	$\frac{5}{2} = 2\frac{1}{2} = 2 + \frac{1}{2}$	$5 = 2\,(2) + 1$	2	1
4	$\frac{4}{2} = 2\frac{0}{2} = 2 + \frac{0}{2}$	$4 = 2\,(2) + 0$	2	0
3	$\frac{3}{2} = 1\frac{1}{2} = 1 + \frac{1}{2}$	$3 = 2\,(1) + 1$	1	1
2	$\frac{2}{2} = 1\frac{0}{2} = 1 + \frac{0}{2}$	$2 = 2\,(1) + 0$	1	0
1	$\frac{1}{2} = 0 + \frac{1}{2}$	$1 = 2\,(0) + 1$	0	1
0	$\frac{0}{2} = 0 + \frac{0}{2}$	$0 = 2\,(0) + 0$	0	0
-1	when $a < 0$ and $n > 2$	$-1 = 2\,(-1) + 1$	-1	1
-2	this intuition breaks down	$-2 = 2\,(-1) + 0$	-1	0
-3		$-3 = 2\,(-2) + 1$	-2	1

think. Divide $a \in \mathbb{N}$ $\langle$so $a > 0\rangle$ by $n \in \mathbb{N}$ to get a quotient is $q \in \mathbb{Z}$ and remainder is $r \in \mathbb{Z}$ with $0 \le r < n$.

$$n \overline{\smash{\big)}\, a}^{\;q}$$

$$\vdots$$

$$\overline{}$$

$$r$$

Thm. **Division Algorithm**. For all $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, there exist unique integers q and r such that §3.5 p143

$$`a \;=\; nq \;+\; r \qquad \text{and} \qquad 0 \le r < n\,. \tag{1}$$

One says: "when we divide the a by n, the **quotient** is q and the **remainder** is r."

▷. Division Algorithm symbolically: $(\forall n \in \mathbb{N})\ (\forall a \in \mathbb{Z})\ (\exists! q \in \mathbb{Z})\ (\exists! r \in \mathbb{Z})\ [\ a = nq + r \quad \wedge \quad 0 \le r < n\ ]$.

Rmk. The equality in (1) can be written as $\frac{a}{n} = q + \frac{r}{n}$ $\langle$but we do not write like this in our proofs$\rangle$. §3.5 p144

Cor. **Corollary to Division Algorithm**. If $a \in \mathbb{Z}$, then:

(0) either there exists $q \in \mathbb{Z}$ such that $a = 2q + 0$
(1) or there exists $q \in \mathbb{Z}$ such that $a = 2q + 1$

but not both. $\langle$Why? Apply the Division Algorithm, taking $n = 2$ and so r is either 0 or 1.$\rangle$

Cor. **Another Corollary to Division Algorithm**. Each integer is either even or odd (but not both).
$\langle$Why? Let $a \in \mathbb{Z}$. Now use the previous Corollary to conclude that a is either even or odd (but not both).$\rangle$

Some Math Terninology

§3.1 p85-86 §1.2 p22

1. A **proof** in mathematics is a convincing argument that some mathematical statement is true.
   $\langle$Proof is a noun while prove is a verb. So we prove a true stament by providing a proof of the statement.$\rangle$
2. A **definition** is simply an agreement as to the meaning of a particular term. $\langle$e.g., even integer$\rangle$
3. There are **undefined terms** in math. <Simply put, we must start somewhere. E.g., in Euclidean Geometry: point&line.>
4. An **axiom** is a mathematical statement that is accepted without proof.
5. A **lemma** is a true statement that was proven mainly to help in the proof of some theorem.
6. A **theorem** is a true mathematical statement for which we have a proof. $\langle$ *Theorem* is abbreviated by *Thm.*.$\rangle$
7. A **proposition** is a *small theorem*. $\langle$this def. of proposition is more common than using prop. to mean statement$\rangle$
8. A **corollary** is a (small) thm. that is easily proven once some other (bigger) thm. has been proven.
9. A **conjecture** is a statement that we believe is plausible (but we do not have a proof for it ... yet).

<To show a conjecture is true, we prove the conjecture.
To show a conjecture is false, you can find a counterexample to the conjecture.>

Definitions: moving from high school level to university level

Divides

§3.1 p82

Def. A nonzero integer n **divides** an integer b, denoted $n|b$, provided that $(\exists k \in \mathbb{Z})\ [nk = b]$.

Rmk. Note $n|b$ if and only if when we apply Division Algorithm and divide b by n ⟨to get $b = nq + r$⟩ the remainder is 0.

Set Containment

§2.3 p55

Defs. Let A and B be two sets.

1. The sets A and B are **equal** when they have precisely the same elements.
   If A and B are equal, then we write $A = B$. If A and B are not equal, then we write $A \neq B$.
2. The set A is a **subset** B provided that each element of A is an element of B.
   If A is a subset of B, then we write $A \subseteq B$ and also say A is **contained** in B or say B **contains** A.
   When A is not a subset of B, we write $A \nsubseteq B$.

Rmk. $[A \subseteq B] \overset{\text{by def.}}{\iff} [\ x \in A \implies x \in B\ ]$

$[B \subseteq A] \overset{\text{by def.}}{\iff} [\ x \in B \implies x \in A\ ]$

$[A = B] \overset{\text{by def.}}{\iff} [\ x \in A \iff x \in B\ ]$ ... so we get ... $[A = B] \overset{\text{so get}}{\iff} [\ (A \subseteq B) \wedge (B \subseteq A)\ ]$

Def. When a set contains no elements, we say that the set is the **empty set**. p60
In mathematics, the empty set is usually designated by the symbol $\emptyset$.
⟨The symbol $\emptyset$ is the last letter in the Danish-Norwegian alphabet and is LaTex-ed \emptyset.⟩

Cartesian Product

§5.4 p256

Def. Let X and Y be sets.

1. The **Cartesian Product** of X and Y, denoted $X \times Y$, is the set
$$X \times Y = \{\ (x, y) : x \in X \text{ and } y \in Y\ \}.$$
   In $X \times Y$:
   - the point (x, y) is an **ordered pair**, with **first coordinate** x and **second coordinate** y.
   - $(x_1, y_1) = (x_2, y_2)$ if and only if $[\ x_1 = x_2 \text{ and } y_1 = y_2\ ]$.
2. Frequently $X \times X$ is denoted X^2. So $X^2 = X \times X = \{\ (a, b) : a \in X \text{ and } b \in Y\ \}$.

Function

§6.1 §6.3

Def. A **function** f from the set X to the set Y, denoted $f : X \to Y$, is a rule that associated with each element $x \in X$ exactly one element $y \in Y$.

Defs. Let $f : X \to Y$ be a function from the set X to the set Y.

- The **domain** of the function f is the set X. Denote: $X = \operatorname{dom}(f)$.
- The **codomain** of the function f is the set Y. Denote: $Y = \operatorname{codom}(f)$.
- If $x \in X$, then f associates to x exactly one $y \in Y$, which is denoted $f(x)$ and called the **image of x under f**.
- The $(x, y) \in X \times Y$ and $f(x) = y$, then x is the **preimage of y under f**.
- The **range of f**, denoted $\operatorname{range}(f)$, is the set defined by $\operatorname{range}(f) \overset{\text{def}}{=} \{f(x) \in Y : x \in X\} \overset{\text{note}}{\subseteq} Y$.
- The function f is **injective** (also called one-to-one) provided
$$\text{for all } x_1, x_2 \in X, \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2.$$
  Symbolically: $(\ \forall (x_1, x_2) \in X^2\ )\ [\ f(x_1) = f(x_2) \implies x_1 = x_2\ ]$.
- The function f is **surjective** (also called onto) provided
$$\text{for all } y \in Y, \text{ there exists } x \in X \text{ such that } f(x) = y.$$
  Symbolically: $(\ \forall y \in Y\ )\ (\ \exists x \in X\ )\ [\ f(x) = y\ ]$.
  Note, f is surjetive if and only if $\operatorname{codom}(f) = \operatorname{range}(f)$.
- The function f is **bijective** provided f is both injective and surjective.