Chapter 0. Introduction: Prerequisites and Preliminaries

Note. The content of Sections 0.1 through 0.6 should be very familiar to you. However, in order to keep these notes complete, we include a synopsis of this material.

Section 0.1. Logic

Note. Sometimes it is helpful when proving a claim (or "conditional statement") of the form "if P then Q" to instead prove the logically equivalent "if not Q then not P." The second conditional statement is the *contrapositive* of the first.

Section 0.2. Sets and Classes

Note. We will mostly deal with sets "naively." Hungerford mentions the Gödel-Bernays axiomatic set theory on page 2. This is based on the *primitive* (that is, undefined) notions of *class*, *membership* ("$\in$"), and *equality* ("$=$"). A set is then a special type of class. Formally:

Definition. A *set* A is a class such that there exists a class B with $A \in B$. A class that is not a set is a *proper class*.

Note. A careful, axiomatic development of set theory is very tedious! However, care must be taken in the development of set theory because a purely naive approach can lead to paradoxes, such as Russell's Paradox. Russell's Paradox is often explained as: "Imagine a town in which a barber cuts the hair of all of those in the town who do not cut their own hair. Who cuts the barber's hair?" For more details, see my Analysis 1 (MATH 4217/5217) online notes on 1.1. Sets and Functions. The following example is Russell's Paradox, but spelled out in terms of classes and sets instead of towns and barbers.

Example. Consider the class $M = \{X \mid X \text{ is a set and } X \notin X\}$. If M is a set, then it is possible to determine the elements which are in it. So the statement $M \notin M$ makes sense and there are two choices: (1) $M \in M$, or (2) $M \notin M$. But by the definition of M, $M \in M$ implies that $X = M$ is a set and $M \notin M$, a contradiction. If $M \notin M$ then M satisfies the conditions of the definition of M (set M is defined using the "Axiom of Class Formation") and so $M \in M$, again a contradiction. So M is not a set, but it is a class. Therefore it is a proper class.

Definition/Axiom. The *power axiom* states that for every set A the class $\mathcal{P}(A)$ of all subsets of A is itself a set. Set $\mathcal{P}(A)$ is the *power set* of A, sometimes denoted 2^A.

Definition. A *family of sets* indexed by the nonempty class I is a collection of sets A_i, one for each i, denoted $\{A_i \mid i \in I\}$. Indexing class I may not be finite and may not even be countable! The *union* and *intersection* of the family is respectively the classes

$$\cup_{i\in I} A_i = \{x \mid x \in A_i \text{ for some } i \in I\},$$

$$\cap_{i\in I} A_i = \{x \mid A_i \text{ for all } i \in I\}.$$

Note. As Hungerford states "suitable axioms" insure that $\cup_{i\in I} A_i$ and $\cap_{i\in I} A_i$ are actually sets.

Definition. If A and B are classes, the *relative complement* of A in B is $B - A = \{x \mid x \in B \text{ and } x \notin A\}$. If all classes under discussion are subsets of some fixed set U, called the *universe of discussion*, then $U - A$ is the *complement* of A, denoted A'.

Theorem 0.2.A. The following properties of sets are easily proved:

$$A \cap (\cup_{i\in I} B_i) = \cup_{i\in I} (A \cap B_i) \text{ and } A \cup (\cap_{i\in I} B_i) = \cap_{i\in I} (A \cup B_i)$$

$$(\cup_{i\in I} A_i)' = \cap_{i\in I} A_i' \text{ and } (\cap_{i\in I} A_i)' = \cup_{i\in I} A_i' \quad \text{(DeMorgan's Laws)}$$

$$A \cup B = B \iff A \subset B \iff A \cap B = A.$$

Section 0.3. Functions

Note. When we use the notation $f : A \to B$ (where A and B are sets) then we mean that set A is the domain of f. Set B is the codomain of f. the range of f is the image of A under f, denoted $\text{Im}(f)$. In general, it may not be that $B = \text{Im}(f)$ (though Hungerford on page 3 says that B is the range, but we will not use the notation in this way).

Definition. For set A, the *identity function* on A, denoted 1_A, is the function given by $a \mapsto a$ (read "a maps to a"). If $S \subset A$, the function $1_A|S : S \to A$ (1_A restricted to set S) is the *inclusion map* of A into A. The inclusion map is usually denoted with an iota, ι.

Note. We will represent functions with diagrams. If $f : A \to B$, $g : B \to C$, and $h : A \to C$, then the diagram

$$\begin{tikzcd} A \arrow[r, "h"] \arrow[d, "f"'] & C \\ B \arrow[ur, "g"'] & \end{tikzcd}$$

is *commutative* if $g \circ f = h$ (or in a more concise notation, $gf = h$).

Definition. Let $f : A \to B$. If $S \subset A$, the *image* of S under f (denoted $f(S)$; Fraleigh would denote this as $f[S]$) is

$$f(S) = \{b \in B \mid b = f(a) \text{ for some } a \in S\}.$$

If $T \subset B$, the *inverse image of* T under f (denoted $f^{-1}(T)$) is

$$f^{-1}(T) = \{a \in A \mid f(a) \in T\}.$$

Example. If $f : \mathbb{R} \to \mathbb{R}$, then $f(\mathbb{R}) = [0, \infty)$ and $f^{-1}(\{9\}) = \{-3, 3\}$.

Theorem 0.3.A. Let $f : A \to B$ with $S \subset A$ and $T \subset B$. Then the following hold:

$$\text{for } S \subset A,\ f^{-1}(f(S)) \supset S;$$

$$\text{for } T \subset B,\ f(f^{-1}(T)) \subset T.$$

For any family $\{T_i \mid i \in I\}$ of subsets of B,

$$f^{-1}\left(\cup_{i \in I} T_i\right) = \cup_{i \in I} f^{-1}(T_i);$$

$$f^{-1}\left(\cap_{i \in I} T_i\right) = \cap_{i \in I} f^{-1}(T_i).$$

Definition. A function $f : A \to B$ is *one-to-one* (or *injective*) if

$$\text{for all } a, a' \in A,\ a \neq a' \Longrightarrow f(a) \neq f(a').$$

f is *onto* (or *surjective*) if $f(A) = B$. f is a *bijection* if it is one to one and onto (Fraleigh, confusingly I think, called a bijection a "one-to-one correspondence").

Note. By the contrapositive of the definition, f is one to one if and only if

$$\text{for all } a, a' \in A,\ f(a) = f(a') \Longrightarrow a = a'.$$

f is onto if and only if

$$\text{for all } b \in B,\ b = f(a) \text{ for some } a \in A.$$

Theorem 0.3.A. If $f : A \to B$ and $g : B \to C$ then

$$f \text{ and } g \text{ one to one } \Longrightarrow gf \text{ is one to one;}$$

$$f \text{ and } g \text{ onto } \Longrightarrow gf \text{ is onto;}$$

$$gf \text{ one to one } \Longrightarrow f \text{ is one to one;}$$

$$gf \text{ onto } \Longrightarrow g \text{ is onto.}$$

Theorem 0.3.1. Let $f : A \to B$ be a function, with A nonempty.

(i) f is injective (one to one) if there is a map $g : B \to A$ such that $gf = 1_A$.

(ii) If A is a set (as opposed to a class), then f is surjective (onto) if and only if there is a map $h : B \to A$ such that $fh = 1_B$.

Definition. The function g in Theorem 0.3.1 for which $gf = 1_A$ is a *left inverse* of f. The function h in Theorem 0.3.1 for which $fh = 1_B$ is a *right inverse* of f. If $f : A \to B$ and $g : B \to A$ such that $fg = 1_B$ and $gf = 1_A$ then g is a *two-sided inverse* of f.

Corollary 0.3.A. If $f : A \to B$, $g : B \to A$, and $h : B \to A$ where g is a left inverse of f and h is a right inverse of f. Then $g = h$. So a two-sided inverse of a function is unique.

Corollary 0.3.B. If A is a set and $f : A \to B$ then

$$f \text{ is bijective } \iff f \text{ has a two-sided inverse.}$$

Section 0.4. Relations and Partitions

Definition. The *Cartesian product* of sets (or classes) A and B is the set (class)

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

A subset (subclass) of R is a relation on $A \times B$.

Definition. A relation R on $A \times A$ is an *equivalence relation* on A provided R is

(i) reflexive: $(a, a) \in R$ for all $a \in A$;

(ii) symmetric: $(a, b) \in R$ implies $(b, a) \in R$;

(iii) transitive: $(a, b) \in R$ and $(b, c) \in R$ implies $(a, c) \in R$.

If $(a, b) \in R$ for equivalence relation R then we denote this as $a \sim b$. For $a \in A$, the *equivalence class* if a is the class $\overline{a}$ of all elements of A which are equivalent to a. The class of all equivalence classes in A is denoted A/R (called the *quotient class* of A by R).

Lemma 0.4.A. For $a, b \in A$ and R an equivalence relation on $A \times A$, we have either (1) $\overline{a} \cap \overline{b} = \varnothing$, or (2) $\overline{a} = \overline{b}$.

Definition. Let A be a nonempty class and $\{A_i \mid i \in I\}$ a family of subsets of A such that:

(i) $A_i \neq \varnothing$ for all $i \in I$;

(ii) $\cup_{i \in I} A_i = A$;

(iii) $A_i \cap A_j = \varnothing$ for all $i \neq j$ where $i, j \in I$.

Then $\{A_i \mid i \in I\}$ is a *partition* of A.

Note. Lemma above implies that the equivalence classes of an equivalence relation on a class (or set) is a partition of the class (or set). This is one of the most useful properties of an equivalence relation! We will make big use of it when introducing cosets in a group.

Theorem 0.4.1. Let A be a nonempty set and R an equivalence relation on A. Then assignment $R \mapsto A/R$ (where A/R is the class of all equivalence classes off R) defines a bijection from the set $E(A)$ of all equivalence relations on A onto the set $Q(A)$ of all partitions of A.

Section 0.5. Products

Note. In Section 0.5, we deal with sets (as opposed to classes).

Definition 0.5.1. Let $\{A_i \mid i \in I\}$ be a family of sets indexed by a nonempty set I. The *Cartesian product* of the sets A_i is the set of all functions $f : I \to \cup_{i\in I} A_i$ such that $f(i) \in A_i$ for all $i \in I$. The set of functions is denoted $\prod_{i\in I} A_i$.

Note. If $I = \{1, 2\}$ and we have sets A_1 and A_2, then the Cartesian product $A_1 \times A_2$ consists of all pairs $\{(a_1, a_2) \mid a_1 \in A_1, a_2 \in A_2\}$. We can associate this with a *function* (as in the definition) $f : I \to A_1 \cup A_2$ where $f(1) \in A_1$ and $f(2) \in A_2$. So function f is "associated" with pair $(f(1), f(2))$ (and conversely). You also encounter then in Calculus II (MATH 1920) when you see a series defined as a function mapping $\mathbb{N} \to \mathbb{R}$ (so the nth term of the series is this function evaluated at n). This is good stuff to *think* about when dealing with $\prod_{i\in I} A_i$, but don't overuse these examples! You may think that for each $i \in I$, an element of $\prod_{i\in I} A_i$ has an "ith component," but be careful—there may not be a first component, a second component, and so forth (namely, in the event that set I is not countable).

Definition. Let $\prod_{i\in I} A_i$ be a Cartesian product. For each $k \in I$ define a map $\pi_k : \prod A_i \to A_k$ by $f \mapsto f(k)$. This map is the *canonical projection* of the product onto its kth component.

Example. Let $I = \mathbb{R}$ and $A_i = \mathbb{C}$ for all $i \in I$. Then an element of $\prod_{k\in I} A_k = \prod_{k\in I} \mathbb{C}$ is a function f that maps $\mathbb{R} \to \mathbb{C}$. Say $f(x) = ix$. Applying π_k to f (where $k \in I = \mathbb{R}$) gives $\pi_k(f) = f(k) = ik$.

Note. We will use the following when we deal with “categories” (see pages 54 and 60).

Theorem 0.5.2. Let $\{A_i \mid i \in I\}$ be a family of sets indexed by I. Then there exists a set D, together with a family of maps $\{\pi_i : D \to A_i \mid i \in I\}$ with the following property: For any set C and family of maps $\{\varphi_i : C \to A_i \mid i \in I\}$, there exists a unique map $\varphi : C \to D$ such that $\pi_i \varphi = \varphi_i$ for all $i \in I$. Furthermore, D is uniquely determined up to a bijection.

Section 0.6. The Integers

Note. In Section 0.6, Hungerford avoids an axiomatic development of the natural numbers. A classical axiomatic development of the natural numbers along with 0 (that is, $\mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}$; in these developments, 0 is included for reason to be explained soon and this is why Hungerford uses the notation $\mathbb{N} = \{0, 1, 2, \ldots\}$ for the “natural numbers” and $\mathbb{N}^* = \{1, 2, 3, \ldots\}$ for the “non-negative natural numbers”—this is nonstandard, however, and so in these class notes we will use the standard notation for the natural numbers, $\mathbb{N} = \{1, 2, 3, \ldots\}$, and when we wish to include 0 then we simply add it).

Note. A common axiomatic development of $\mathbb{N} \cup \{0\}$ is the system of five axioms of Italian mathematician Giuseppe Peano in 1899. The five axioms of Peano are (from E. Nagel J. and Newman’s *Gödel’s Proof*, revised edition, New York University Press, 2001; this is a nice semi-technical book on the ideas behind Gödel’s work on incompleteness):

Axiom 1. 0 is a number.

Axiom 2. The immediate successor of a number is a number.

Axiom 3. 0 is not the immediate successor of a number.

Axiom 4. No two numbers have the same immediate successor.

Axiom 5. Any property belonging to 0, and also to the immediate successor of every number that has the property, belongs to all numbers.

Axiom 5 is called the Principle of Mathematical Induction.

Note. Set theoretic definitions of $\mathbb{N} \cup \{0\}$ are very abstract and define all numbers in terms of sets. In K. Hrbacek and T. Jech's Introduction to Set Theory, 2nd Edition Revised and Expanded, in Pure and Applied Mathematics, A Series of Monographs and Textbooks, Marcel Dekker (1984), this approach is taken. It is extremely tedious and off to a slow start. Numbers, being defined in terms of sets, are given as follows:

- $0 = \varnothing$.
- $1 = \{0\} = \{\varnothing\}$.
- $2 = \{0, 1\} = \{\varnothing, \{\varnothing\}\}$.
- $3 = \{0, 1, 2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}$.
- $4 = \{0, 1, 2, 3\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}$.
- And so forth.

The *successor* of a set x is then defined as $S(x) = x \cup \{x\}$; the successor of x is denoted $x + 1$. A set I is *inductive* if (a) $0 \in I$, and (b) if $n \in I$ then $(n + 1) \in I$. The set of natural numbers (plus 0) is then defined as $\mathbb{N} \cup \{0\} = \{x \mid x \in I \text{ for every inductive set } I\}$. With this definition and the standard axioms of set theory (the "ZFC Axioms," which are spelled out in detail in the notes for Section 0.8), we can prove this usual properties of the natural numbers. In particular, with $a < b$ being defined as $a \subset b$, we can prove the following three properties (the second of which is a restatement of Peano's Axiom 5):

Law of Well Ordering. Every nonempty subset S of $\mathbb{N} \cup \{0\}$ contains a least element (that is, an element $b \in S$ such that $b \leq c$ for all $c \in S$).

Theorem 0.6.1. Principle of Mathematical Induction.
If S is a subset of the set $\mathbb{N} \cup \{0\}$ such that $0 \in S$ and either

(i) $n \in S$ implies $n + 1 \in S$ for all $n \in \mathbb{N} \cup \{0\}$, or

(ii) $m \in S$ for all $0 \leq m < n$ implies $n \in S$ for all $n \in \mathbb{N} \cup \{0\}$,

then $S = \mathbb{N} \cup \{0\}$.

Theorem 0.6.2. The Recursion Theorem.
If S is a set, $a \in S$ and for each $n \in \mathbb{N} \cup \{0\}$, $f_n : S \to S$is a function, then there is a unique function $\varphi : \mathbb{N} \cup \{0\} \to S$ such that $\varphi(0) = a$ and $\varphi(n + 1) = f_n(\varphi(n))$ for every $n \in \mathbb{N} \cup \{0\}$.

Note. With $\mathbb{N} \cup \{0\}$ defined, it is straightforward to define the integers $\mathbb{Z}$ by introducing the "negatives" as additive inverses of the "positives." This then gives a *positive set* $P = \mathbb{N} = \{1, 2, 3, \ldots\}$ in $\mathbb{Z}$ and allows us to define greater than and less than in terms of the positive set: $a < b$ or $b > a$ if $b - a \in P$. Of course, it must be confirmed that this "<" coincides with the "<" defined on $\mathbb{N} \cup \{0\}$ which is given above (namely, for $a, b \in \mathbb{N} \cup \{0\}$, $a < b$ means $a \subset b$).

Note. We take the following, The Division Algorithm for $\mathbb{Z}$, as given. A proof is given in John Fraleigh's *A First Course in Abstract Algebra*, 7th edition, based on the integers as a cyclic group (see page 60, Theorem 6.3):

Theorem 0.6.3. Division Algorithm.
If $a, b \in \mathbb{Z}$ and $a \neq 0$, then there exist unique integers q and r such that $b = aq + r$, and $0 \leq r < |a|$.

Definition. Integer $a \neq 0$ *divides* an integer b (written $a \mid b$) if there is an integer k such that $ak = b$. If a does not divide b we write $a \nmid b$.

Definition 0.6.4. The positive integer c is the *greatest common divisor* of the integers $a_1, a_2, \ldots, a_n$ if:

(1) $c \mid a_i$ for $1 \leq i \leq n$;

(2) $d \in \mathbb{Z}$ and $d \mid a_i$ for $1 \leq i \leq n$ implies $d \mid c$.

c is denoted $(a_1, a_2, \ldots, a_n)$.

Note. The following is an application of the division algorithm.

Theorem 0.6.5. If $a_1, a_2, \ldots, a_n$ are integers, not all 0, then $(a_1, a_2, \ldots, a_n)$ exists. Furthermore there are integers $k_1, k_2, \ldots, k_n$ such that

$$(a_1, a_2, \ldots, a_n) = k_1a_1 + k_2a_2 + \cdots + k_na_n.$$

Definition. The integers $a_1, a_2, \ldots, a_n$ are *relatively prime* if $(a_1, a_2, \ldots, a_n) = 1$. A positive integer $p > 1$ is said to be *prime* if its only divisors are ± 1 and $\pm p$.

Note. An application of Theorem 0.6.5 is the following.

Theorem 0.6.6. If a and b are relatively prime integers and $a \mid bc$, then $a \mid c$. If p is prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i.

Note. The following result, The Fundamental Theorem of Arithmetic, is proved in Fraleigh's text (see Section 45 and Corollary 45.18). To be be precise, Fraleigh shows that $\mathbb{Z}$ is a *unique factorization domain.*

Definition. Let $m > 0$ be a fixed integer. If $a, b \in \mathbb{Z}$ and $m \mid (a - b)$ then a is *congruent to b modulo m.*

Note. The following result gives a precise definition to $\mathbb{Z}_n$. Notice that, as a result, the elements of $\mathbb{Z}_n$ are not $\{0, 1, 2, \ldots, n-1\}$ but instead equivalence classes of elements of $\mathbb{Z}$ modulo n (as you may recall from Introduction to Modern Algebra [MATH 4127/5127] the elements of $\mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z})$ are also cosets of $n\mathbb{Z}$).

Theorem 0.6.8. Let $m > 0$ be an integer and $a, b, c, d \in \mathbb{Z}$.

(i) Congruence modulo m is an equivalence relation on the set of integers $\mathbb{Z}$, which has precisely m equivalence classes.

(ii) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b_d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

(iii) If $ab \equiv ac \pmod{m}$ and a and m are relatively prime, then $b \equiv c \pmod{m}$.