SOME REMARKS ON STATEMENTS AND THEIR PROOFS

In this course, it will be very important to learn, understand, and remember definitions, theorems and their proofs.

For a definition, you need to

- Know the definition as it is given, in particular, know and understand the meaning of all the terminology and symbols used;
- be able to give an example of the object in the definition;
- be able to test whether a given object satisfies the definition; Caution: this is sometimes very difficult (for technical or other reasons) and not always practical. That's part of the reason we need theorems, propositions, etc.

For a statement (theorem, lemma, proposition, corollary) you need to

- Know the statement as it is given, in particular, know and understand all the symbols and objects used in the statement;
- Know the hypothesis of the statement and why you need them in the proof; In particular, you should think of counterexamples when the hypothesis are not satisfied;
- Know the idea of the proof and the key steps; In particular, the method of proof (direct verification, contradiction, explicit construction, etc.); What definitions and previous statements are used in the proof;
- Know the complete proof; Check what goes wrong if some of the hypothesis of the theorem are dropped;
- Know the consequence of the statement;
- Know a specific example of the statement;
- be able to use statement in constructing your own proofs and in doing computations;

In this course, we will learn proofs of several different types. In general, most of the theorems will be of the following type: Given that a Statement A is true, proof that a Statement B is true. Some of the methods to proof such theorems are the following:

1. *Direct verification:* Check the statement. For example, let the theorem be the following:
   THEOREM. *Let* $\mathbb{N}_0 = 0, 1, 2, 3, \cdots$ *be the set of all non-negative integers and* $\mathbb{Z}$ *be the set of all integers. The map* $f : \mathbb{N}_0 \to \mathbb{Z}$ *given by* $f(0) = 0$*,* $f(2k+1) = k+1$ *and* $f(2k) = -k$ *is an*

isomorphism.

The proof of this statement by direct verification consists of checking that the map f satisfies both conditions of being an isomorphism (that is, it is onto and one-to-one). As an exercise, complete this proof.

2. *By contradiction*: Suppose you need to prove that a set of conditions A (the *hypothesis*) implies that some statement B (the *conclusion)* is true. A proof by contradiction involves assuming that B is false (in other words, assuming that not-B is true), and by doing logical arguments, showing that this would imply that A is false. This proves that, if A is true then B is true, which is the original statement. For example, suppose that the theorem you want to prove by contradiction is the following:

   THEOREM. L*et X and Y be finite sets, and suppose that there exists a map $f : X \to Y$ which is onto. Then the number of elements in the set X is smaller or equal than the number of elements in the set Y, i.e., $\#(X) \leq \#(Y)$.*

   Here the hypothesis is that there is a map from a finite set X to a finite set Y which is onto. The conclusion is that the number of elements in X can not be smaller then the number of elements in Y. A proof of this statement by contradiction goes as follows. Assume that the conclusion is wrong. That is, the number of elements in X is smaller then the number of elements in Y,

$$\#(X) < \#(Y). \tag{1}$$

   Let f be a map from X to Y. The image of this map inside of Y contains no more then $\#(X)$ points, that is

$$\#(\mathrm{Im}(f)) \leq \#(X) \tag{2}$$

   (If for every pair $x_1 \neq x_2 \in X$ we have $f(x_1) \neq f(x_2) \in \mathrm{Im}(f)$, i.e., if f is one-to-one, then $\#(\mathrm{Im}(f)) = \#(X)$. Otherwise, $\#(\mathrm{Im}(f)) < \#(X)$). Since $\mathrm{Im}(f) \subseteq Y$, we obtain that $\#(\mathrm{Im}(f)) \leq \#(Y)$. Let f be a map which is onto (it exists by assumption.) Then $\#(\mathrm{Im}(f)) = \#(Y)$. Substituting this into (1), we obtain a contradiction with 2.

3. *Induction* is used to proof some statements which are claimed to be true for all non-negative integers. Let $P(n)$ be a statement depending on n for any $n \in \mathbb{Z}^+ = \mathbb{N} = \{1, 2, 3, \ldots\}$. To show that $P(n)$ is true for all n using the method of induction, one must do the following:

   1) First, check that the statement $P(1)$ for $n = 1$ is true. (This is

usually not very hard to do).
2). Assume that $P(n)$ is true for some n (*induction hypothesis!*) and show that $P(n)$ implies $P(n+1)$.
The principle of induction then says that the $P(n)$ is true for all n.
THEOREM. *For all $n \in \mathbb{Z}^+$ we have $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.*
This is a statement which can be proven by induction as follows:
1). Check that the statement is true for $n = 1$: Indeed, $\sum_{i=1}^{1} i = 1 = \frac{1\cdot 2}{2}$;
2). Assume that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ (that is, the statement is true for some number n) and conclude that the same formula is true for $n+1$:

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}.$$

4. *Explicit construction* is often used in proving the statements about the existence of objects with certain properties. For example, suppose that you need to prove the following
   THEOREM. The sets $\mathbb{Z}$ and $\mathbb{N}_0$ are isomorphic.
   A proof by explicit construction would consist in exhibiting a map from $\mathbb{Z}$ to $\mathbb{N}_0$ which is an isomorphism, and proving that it is indeed an isomorphism. (Such a map was explicitly given in part 1, direct verification). As an exercise, try to think whether the sets $\mathbb{R}$ and $\mathbb{C}$ are isomorphic.