Notes CH3) Theorem Types and Proof Methods

3.1 Existence theorems

Either one constructs an example of the object in question → Proof by construction
Shows that if it did not exist a known fact would be falsified → Proof by contradiction

3.2 Uniqueness theorems

theorems stating the uniqueness of a mathematical object X whose existence has already been established.
To prove a uniqueness theorem one takes an arbitrary mathematical object Y that satisfies the conditions defining X, and shows that $X = Y$.

3.3 Classification Theorems

Once the existence and and non-uniqueness of a mathematical object are established, one may pose the question of its classification

3.4 Proving Implications

Majority of theorems in mathematics are implications they involve a hypothesis a and a conclusion b, and the theorem states that $c := (a \Rightarrow b)$ is a true statement. c means that if a is true, then so is b.

3.4.1 Trivial Proof

The easiest way of proving an implication is to ~~show th~~ show that its hypothesis is false. The main problem with this method is that it cannot be applied to arbitrary implication.

3.4.2 Direct Proof

Assume a is true and show that b is true. May be applied to any implication.

3.4.3 Contrapositive Proof

$(a \Rightarrow b) = (\cancel{\quad}) = (\neg b \Rightarrow \neg a)$

To establish $a \Rightarrow b$ is true we can proove that $\neg b \Rightarrow \neg a$ is true.

3.4.4 Deductive Proof

$(a \Rightarrow c \Rightarrow b) \Rightarrow (a \Rightarrow b)$ in other words, to prove $a \Rightarrow b$ is true, one can use an intermediary c s.t $(a \Rightarrow c) \wedge (c \Rightarrow b)$ is true.

3.5 Proof By Contradiction

1. Find appropriate statement b
2. Prove that $\neg a \Rightarrow b$, and
3. Prove that b is false.

OR

Prove that ($\neg a \Rightarrow a$ is true $\Rightarrow a$ is true.

In practice, one usually finds the appropriate b in the process of applying the method of direct proof to $\neg a \Rightarrow b$. In other words one assumes that $\neg a$ is true, and seeks among the logical consequences of this assumption for one that contradicts a known fact. If the assumption of $\neg a$ leads to a false statement, then one has found an appropriate b and in the process has also achieved 2 and 3.

3.6 Proof by Cases

Basically proves all cases.

3.7 Proof by Induction

$(a_1 \wedge (\forall m \in \{1, 2, \cdots, N-1\}, (a_m \Rightarrow a_{m+1}))) \Rightarrow (\forall_n \in \{1, 2 \cdots N-1\}, a_n)$.

1. Prove a_1
2. Assume $\exists m \in \mathbb{Z}^+$ s.t. a_m is true, and
3. prove a_{m+1}

~~Induction Axiom~~:

$(a_1 \wedge (\forall m \in \mathbb{Z}^+, (a_m \Rightarrow a_{m+1}))) \Rightarrow (\forall_n \in \mathbb{Z}^+, a_n)$

3.7.2 Complete Induction

1. Prove a_1,
2. Assume $\exists m \in \mathbb{Z}^+$ such that for all $\ell \in \{1 \dots m\}$, a_ℓ is true and
3. Prove a_{m+1}

$$(a_1 \land (\forall m \in \mathbb{Z}^+, ((a_1 \land a_2 \land \cdots \land a_m) \Rightarrow a_{m+1}))) \Rightarrow (\forall n \in \mathbb{Z}^+, a_n).$$

Definitions:

Definition 3.1.1 Let m and n be integers. then m is said to divide n, if there exists an integer k such that $n = k \cdot m$, i.e., the following statement holds. $\exists k \in \mathbb{Z}, n = km.$
In this case, m is said to be a divisor of n, and n is called a multiple of m. $m \mid n$

Definition 3.5.1 Let m and n be integers, then an integer that divides both m and n is said to be their common divisor. the largest of which is called the greatest common divisor. We denote it by "$\gcd(m,n)$".

Definition 3.5.2 Two integers m and n (not both zero) are said to be relatively prime if $\gcd(m,n) = 1$. i.e. the only positive integer that divides m and n is 1.
We can express this as
$$\forall k \in \mathbb{Z}^+, (k \mid m \wedge k \mid n) \Rightarrow (k = 1) \blacksquare$$

Definition 3.8.1 Let $n \in \mathbb{Z}^+$ and $j, k \in \mathbb{Z}$. Then j is said to be congruent to k modulo n, if j and k have the same remainder.

Theorems (Lemmas, Propositions, Corollaries included)

Theorem 3.1.1 Every integer has a divisor.

Theorem 3.2.1 The only natural number n satisfying the following condition is 0.

$$\forall j \in \mathbb{N}, n + j = j.$$

Proposition 3.4.1 Let m, n, p be integers. If m divides n and n divides p, then m divides p, i.e., $(m|n \wedge n|p) \Rightarrow m|p$

Proposition 3.4.2 For every integer n, if n^2 is even, then so is n.

$$2|n^2 \Rightarrow 2|n$$

Theorem 3.4.1 Let $n \in \mathbb{Z}^+$ and $c_1, c_2, \cdots c_n, a, b$ be statements. Then the following is a tautology

$$t := ((a \Rightarrow c_1 \Rightarrow c_2 \Rightarrow \cdots \Rightarrow c_n \Rightarrow b) \Rightarrow (a \Rightarrow b)).$$

Theorem 3.5.1 Let m and n be integers such that at least one of them is nonzero. Then m and n have a greatest common divisor that is greater than or equal to 1.

Lemma 3.5.1 Every rational can be expressed as the ratio of two relatively prime integers. i.e,

$$\forall r \in \mathbb{Q}, \exists p, q \in \mathbb{Z}, (q \neq 0) \wedge (r = \tfrac{p}{q}) \wedge (g.cd(p,q) = 1).$$

Theorem 3.5.2 $\sqrt{2}$ is not a rational number.

Axiom 3.7.1 (Induction Axiom)

Let S be a collection of positive integers (a subset of $\mathbb{Z}^+$). If $1 \in S$ and $\forall m \in \mathbb{Z}^+, ((m \in S) \Rightarrow ((m+1) \in S))$, then S includes all positive integers, i.e. $S = \mathbb{Z}^+$

Theorem 3.7.1 (Principle of Mathematical Induction)

Let a_n be a statement for all $n \in \mathbb{Z}^+$. Suppose that a_1 and "$\forall m \in \mathbb{Z}^+, (a_m \Rightarrow a_{m+1})$" are true, then a_n is true for all $n \in \mathbb{Z}^+$.

Proposition 3.7.1 Every positive integer can be written as the sum of distinct powers of 2, i.e.,
$\forall n \in \mathbb{Z}^+, \exists \ell \in \mathbb{Z}^+, \exists p_1, p_2, \dots p_\ell \in \mathbb{N}$, s.t. $p_1 < p_2 \dots < p_\ell$, and

$$n = 2^{p_1} + 2^{p_2} + \dots 2^{p_\ell} = \sum_{k=1}^{\ell} 2^{p_k}$$

Theorem 3.7.2 (Principle of Complete Induction)

Let a_n be a statement for all $n \in \mathbb{Z}^+$. Suppose that a_1 and $(\forall m \in \mathbb{Z}^+, ((a_1 \wedge a_2 \wedge \dots \wedge a_m) \Rightarrow (a_{m+1}))$ are true. Then a_n is true for all $n \in \mathbb{Z}^+$.

Theorem (Division Algorithm)

Let $n \in \mathbb{Z}^+$ and $i \in \mathbb{Z}$. Then $\exists! m \in \mathbb{Z}$ and $\exists! r \in \{0 \dots n-1\}$ s.t. $i = mn + r$. r is called the remainder of the division.

Theorem 3.8.1

Let $n \in \mathbb{Z}^+$ and $j, k \in \mathbb{Z}$. then j is congruent to k modulo n if and only if n divides $j-k$.

Theorem 3.8.2

Let $\forall n \in \mathbb{Z}^+$, a_n be a statement. Then for every integer k greater than 1, the following two statements are logically equivalent.

$b_k := (a_1 \Leftrightarrow a_2 \Leftrightarrow \dots a_k)$,

$c_k := (a_1 \Rightarrow a_2 \Rightarrow \dots a_k \Rightarrow a_1)$