Proof Review

Monday, September 21

Theorem 0.1 *Theorem 1 If $\mathcal{P}(A) = \mathcal{P}(B)$ then $A = B$.*

Proof 1 $\mathcal{P}(A)$ and $\mathcal{P}(B)$ are the sets of all subsets of A an B. So for $\mathcal{P}(A)$ and $\mathcal{P}(B)$ to have all of the same subsets of elements, the sets A and B need to have all the same elements. Therefore, $A = B$.

Proof 2 Since $\mathcal{P}(A)$ is the set of all subsets of A and since $A \subset A$, we know that $A \in \mathcal{P}(A)$. But $\mathcal{P}(A) = \mathcal{P}(B)$, so this means that $A \in \mathcal{P}(B)$, and so $A = B$.

Proof 3 $x \in A \Leftrightarrow \{x\} \in \mathcal{P}(A) \Leftrightarrow \{x\} \in \mathcal{P}(B) \Leftrightarrow x \in B$.

Theorem 0.2 *Theorem 2 If $A \cup B = U$ and $A \subset C$ then $\overline{C} \subset B$.*

Proof 1 The given information (in propositional logic) is that $a \vee b \equiv \mathbf{T}$ and $a \Rightarrow c \equiv \mathbf{T}$, so $\neg a \vee c \equiv \mathbf{T}$. Therefore

$$\begin{aligned}
\neg c \Rightarrow b &\equiv c \vee b \\
&\equiv (a \wedge \neg a) \vee b \vee c \\
&\equiv ((a \vee b) \wedge (\neg a \vee b)) \vee c \\
&\equiv \neg a \vee b \vee c \\
&\equiv b \vee (\neg a \vee c) \\
&\equiv \mathbf{T}
\end{aligned}$$

Therefore, $\overline{C} \subset B$.

Proof 2 Since $A \cup B = U$ we know that if an element is not in A then it is in B, so $\overline{A} = B$. The premise $A \subset C$ is equivalent to $\overline{C} \subset \overline{A}$, and since $\overline{A} = B$ this means that $\overline{C} \subset B$.

Proof 3 Suppose $x \in \overline{C}$. Then since $A \subset C$, $x \notin A$. But $A \cup B = U$ means that $x \in A$ or $x \in B$, and since $x \notin A$ it follows that $x \in B$. Therefore, if $x \in \overline{C}$ then $x \in B$, meaning that $\overline{C} \subset B$.

Theorem 0.3 (Theorem 3) *If $a|c$ and $b|c$ then $c = 0$ or $a = b$.*

Proof Since $a|c$ there is some $k \in \mathbb{Z}$ such that $ak = c$. Since $b|c$ there is also some $k \in \mathbb{Z}$ such that $bk = c$. So we can write $ak = c = bk$, meaning that $ak = bk$. If $k \neq 0$ then we can divide by k to get $a = b$.

Theorem 0.4 (Theorem 4) *If $a|bc$ and $\gcd(a, b) = 1$ then $a|c$.*

Proof 1 By Bezout's Theorem there exist s and t such that $as + bt = 1$. So $asc + btc = c$, but since $a|bc$ we can say $bc = ak$ for some k. The previous equation then becomes $c = asc + akt = a(sc + kt)$, so $a|c$.

Proof 2 By Bezout's Theorem there exist s and t such that $as + bt = 1$. This means that there exists t such that $bt \equiv 1 \pmod{a}$. Suppose $a|bc$, so $bc \equiv 0 \pmod{a}$. Then $tbc \equiv t \cdot 0 \pmod{a}$, which means that $c \equiv 1 \cdot c \equiv 0 \pmod{a}$. Therefore $a|c$.

Proof 3 Break a, b, and c into products of prime factors. Since $a|bc$ we know that the prime factors of bc contain all the prime factors of a, but since $\gcd(a, b) = 1$ we know that none of these factors containing a can come from b. They must therefore all come form c, meaning that $a|c$.

Theorem 0.5 (The Prime Property) *If p is prime, and $p|ab$, then $p|a$ or $p|b$.*

Proof : Prove it.