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, $A = B$.

This is not very convincing since all it really does is restate the theorem in slightly different words without giving any additional evidence as to why it should be true. Two main notes for this:

First, if you want to make sure that you are rigorously proving that $A = B$ for a pair of sets A and B, you should probably do one of these three things.

1. Show that $x \in A$ if and only if $x \in B$.
2. Prove that $A \subset B$ and $B \subset A$.
3. Use a series of set equivalences that parallel the equivalences in propositional logic.

Second, this proof can be improved by taking the idea of Proof 3, so we could say the following: if $\mathcal{P}(A) = \mathcal{P}(B)$ then the singleton sets in $\mathcal{P}(A)$ are the same as those in $\mathcal{P}(B)$. But the elements in singleton sets in $\mathcal{P}(A)$ are precisely the same as the elements of A and the elements in singleton sets in $\mathcal{P}(B)$ are precisely the same as the elements of B, so this implies that $A = B$. The difference is that it is more clear that this explanation can be turned into a rigourous proof if necessary.

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 $A = B$.

This is half of a rigorous proof: it is almost correct, but $A \in \mathcal{P}(B)$ shows that $A \subset B$, not $A = B$. To complete the proof, use the same explanation but with the set names switched to show that $B \subset A$.

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

This is correct but very terse and does not explain itself at all. It could be improved by adding a sentence or two explaining the idea of the proof.

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

This proof is technically correct but is uninformative and hard to follow. If you are proving theorems about sets, avoid turning set equalities into propositional logic unless you are forced to do so.

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 $\overline{C} \subset B$.

It is not true that $\overline{A} = B$, but it is true that $\overline{A} \subset B$. If we fix this part the proof becomes valid.

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 $\overline{C} \subset B$.

The proof is valid and largely the same as the previous proof. Which one you prefer is a matter of taste.

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 $a = b$.

Counterexample: $c = 6, a = 2, b = 3$. The proof is invalid because it mistakenly assumes that the k in $ak = c$ and the k in $bk = c$ are necessarily the same k. This is why it is good practice to use different variable names for every new existential statement you use in a proof.

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 $a|c$.

This proof is not only correct, it reveals more than the previous proof.

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 $a|c$.

Okay but a little hand-wavey. As it turns out, we use this theorem to prove that numbers have a unique prime factorization in the first place, so this is in danger of relying on circular logic.

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

Proof : Suppose that p is prime and $p|ab$. If $p|a$ then we are done. If $p \nmid a$ then $\gcd(a, p) = 1$. Therefore by the previous theorem, $p|b$.

To show the claim that if $p \nmid a$ then $\gcd(a, p) = 1$: the only positive divisors of p are 1 and p by defninition. If $\gcd(a, p) = p$ then $p|a$. So if $p \nmid a$ then $\gcd(a, p) \neq p$, meaning that $\gcd(a, p) = 1$.