Example Proof Problem Solutions

1. Prove that $1+4+9+...+n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

Solution: Let's use induction to prove this. Notice that when $n=1$, this statement says $1 = \frac{1(2)(3)}{6}$ which is true. Now, suppose that the statement is true for some $n \in \mathbb{N}$. That is, suppose that

$$1+4+9+...+n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Then,

$$1+4+9+...+n^2+(n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 =$$

$$= \frac{n(n+1)(2n+1)}{6} + \frac{6(n+1)^2}{6}$$

$$= \frac{2n^3+3x^2+x}{6} + \frac{6(n^2+2n+1)}{6}$$

$$= \frac{2n^3+9x^2+13n+1}{6}.$$

Note that

$$= \frac{2n^3+9x^2+13n+6}{6} = \frac{(n+1)(n+2)(2n+3)}{6},$$

so

$$1+4+9+...+n^2+(n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}$$

which proves that formula for all n. $\square$

2. Prove that $A\backslash(B \cup C) = (A\backslash B) \cap (A\backslash C)$.

Solution: To show that two sets are equal, you must prove that each set is a subset of the other. So we break our proof into two parts:

Claim 1: $A\backslash(B \cup C) \subseteq (A\backslash B) \cap (A\backslash C)$.

Suppose that $x \in A\backslash(B \cup C)$. That means $x \in A$ and $x \notin (B \cup C)$. In other words, $x \notin B$ and $x \notin C$. Thus $x \in A\backslash B$ and $x \in A\backslash C$. So $x \in (A\backslash B) \cap (A\backslash C)$.

Claim 2: $(A\backslash B) \cap (A\backslash C) \subseteq A\backslash(B \cup C)$.

Suppose that $x \in (A\backslash B) \cap (A\backslash C)$. Then x is in A and not in B, and also x is in A and not in C. So x is in A but x is not in $B \cup C$. So $x \in A\backslash(B \cup C)$. $\square$

3. Let $S = \mathbb{R}\backslash\{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

Solution: We need to prove two things: (1) that S is a group under the operation $*$ and (2) that the operation $*$ is commutative. It actually doesn't matter which order we prove these, so I will prove commutativity first. Notice that $a * b = a + b + ab = b + a + ba = b * a$ for all $a, b \in S$, so the operation is commutative.

To prove that S is a group, we need to make the following observations.

1. We have to show that $*$ is associative, since it is a new operation (not one inherited from a larger group). So we have to show that $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$. Consider

$$(a * b) * c = (a + b + ab) + c + (a + b + ab)c =$$

$$= a + b + ab + c + ac + bc + abc.$$

   Now, let's factor a out of terms where a is a factor. We get:

$$a + b + c + bc + a(b + c + bc)$$

   which is precisely $a + (b + c + bc) + a(b + c + bc) = a * (b * c)$. So $*$ is associative.

2. To show that S is closed under $*$, we need to make sure that $a * b$ never equals -1. Notice that if $a * b = a + b + ab = -1$, then $a + b + ab + 1 = 0$. If we factor out a where we can, we get: $a(b + 1) + (b + 1) = (b + 1)(a + 1) = 0$. Once you look at the formula this way, it is clear that since a and b are not -1, neither is $a + b + ab$. Therefore S is closed.

3. We need to show that S has an identity. Notice that $a * 0 = a + 0 + 0 = a$, so S does indeed have an identity. It is 0.

4. Finally, we need to prove that every $a \in S$ has an inverse. Choose any $a \in S$. Let $b = \frac{-a}{1+a}$. Notice that b cannot equal -1, since if it did:

$$-1 = \frac{-a}{1+a} \Longrightarrow a = 1 + a$$

which is impossible. Thus $b \in S$. Now,

$$a * b = a + \frac{-a}{1+a} + a\frac{-a}{1+a} =$$

$$= \frac{a(1+a)}{1+a} + \frac{-a}{1+a} + \frac{-a^2}{1+a} = 0$$

which is the identity. □

4. Prove that if H and K are both subgroups of a group G, then $H \cap K$ is also a subgroup of G.

Solution: To prove that $H \cap K$ is a subgroup, we have to make sure that it is closed, that it contains the identity, and that every element in $H \cap K$ has an inverse in $H \cap K$.

1. Suppose that $x, y \in H \cap K$. Then $x, y \in H$ and $x, y \in K$. Since H and K are each closed, we conclude that $xy \in H$ and $xy \in K$, so $xy \in H \cap K$. Thus $H \cap K$ is closed.
2. Since $e \in H$ and $e \in K$, it follows that $e \in H \cap K$.
3. If $x \in H \cap K$, then $x^{-1} \in H$ and $x^{-1} \in K$, since both H and K are subgroups. Thus $x^{-1} \in H \cap K$.

□

5. Prove that every finite group of even order has a subgroup of order 2.

Hint: You can prove this claim by proving even more! Show that the number of elements of order 2 in a finite group is odd. That will imply that there is a subgroup of order 2.