Handout: Proof skills

(1) Write the negation of each of the following statements.
   (a) The numbers a and b are in the set S.
   Negation: Either a or b is not in the set S.
   (b) Either a or b is in the set S.
   Negation: Neither a nor b is in the set S.
   (c) There exists a group G which is not commutative.
   Negation: For all groups G, G is commutative.
   (d) Every integer is even.
   Negation: There exists an integer which is not even.

(2) For each pair of statements p and q below, determine whether the statement "p and q" and the statement "p or q" are true or false.
   (a) $p =$ "Every group has an identity element." (**true**)
   $q =$ "Every group is associative." (**true**)
   "p and q" is **true**, "p or q" is **true**.
   (b) $p =$ "Every operation is associative." (**false**)
   $q =$ "The set $\mathbb{Q}$ with the operation of subtraction forms a group." (**false**)
   "p and q" is **false**, "p or q" is **false**.
   (c) $p =$ "The group $\mathbb{Z}_6$ has order 5."(**false**)
   $q =$ "The group $\mathbb{Z}_2 \times \mathbb{Z}_4$ has 6 elements."(**false**)
   "p and q" is **false**, "p or q" is **false**.

(3) Prove the following statement using a direct proof.

Theorem 1. *Let $a, x,$ and y be elements of a group G. If $xay = a^{-1}$, then $yax = a^{-1}$.*

Note that there are several different correct direct proofs of this theorem. I will only provide one.

Proof. Let a, x, and y be elements of a group G. Assume that $xay = a^{-1}$. Then we know that

$$a = \left(a^{-1}\right)^{-1} = (xay)^{-1} = y^{-1}a^{-1}x^{-1}.$$

Thus

$$yax = y(y^{-1}a^{-1}x^{-1})x = (yy^{-1})a^{-1}(xx^{-1}) = ea^{-1}e = a^{-1},$$

as desired. □

(4) Prove the following statements using a proof by contradiction.

Theorem 2. *If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.*

Proof. Assume, towards a contradiction, that $a, b \in \mathbb{Z}$ and $a^2 - 4b = 2$. Then we have that

$$a^2 = 4b + 2 = 2(2b + 1).$$

Thus a^2 is an even integer. Note that the square of an odd number is odd:

$$(2n + 1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1,$$

thus a must be an even integer as well. Say $a = 2k$ for some integer k. Then we have that

$$(2k)^2 - 4b = 2,$$

i.e.,

$$4k^2 - 4b = 2.$$

i.e.,

$$4(k^2 - b) = 2.$$

However, the left-hand side of this equation is divisible by 4, while the right-hand side is not divisible by 4. This is a contradiction. Since we have arrived at a contradiction, it must be that $a^2 - 4b \neq 2$, as desired. □

The following two theorems are classic examples of proof by contradiction and are very important results for algebra and number theory.

Theorem 3. *The number $\sqrt{2}$ is irrational.*

Proof. Suppose, towards a contradiction, that $\sqrt{2}$ is a rational number. Then $\sqrt{2} = \frac{a}{b}$ for some integers a and b, where $\frac{a}{b}$ is fully reduced. Squaring both sides, we see that

$$2 = \frac{a^2}{b^2},$$

i.e.,

$$a^2 = 2b^2.$$

So a^2 is an even number. Note that the square of an odd number is odd:

$$(2n + 1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1,$$

thus a must be an even integer as well. Say $a = 2k$ for some integer k. The we have that

$$(2k)^2 = 2b^2,$$

i.e.,

$$4k^2 = 2b^2.$$

Dividing by 2, we get

$$2k^2 = b^2.$$

Thus b^2 is an even number and, by the same argument above, it follows that b is even. However, this means that a and b share a factor of 2, while $\frac{a}{b}$ was assumed to be fully reduced. This is a contradiction. Therefore, it must be that $\sqrt{2}$ is irrational. □

Theorem 4. *There are infinitely many prime numbers.*

Proof. Suppose, towards a contradiction, that there are only finitely many primes, say $p_1, p_2, p_3, \ldots, p_n$. Consider the number $p_1p_2p_3 \cdots p_n + 1$. For each prime number p_i, the number $p_1p_2p_3 \cdots p_n + 1$ leaves a remainder of 1 when divided by p_i. Therefore, $p_1p_2p_3 \cdots p_n + 1$ is not divisible by any of the prime numbers $p_1, p_2, p_3, \ldots, p_n$ and so it must be prime itself. However, $p_1, p_2, p_3, \ldots, p_n$ was assumed to be a complete list of primes, and we have reached a contradiction. Thus there are infinitely many prime numbers. □

(5) Prove the following statement by proving its contrapositive.

Theorem 5. *Let x and y be integers. If $x + y$ is even, then x and y are both even or x and y are both odd.*

Contrapositive: Let x and y be integers. If one x and y is even and one of x and y is odd, then $x + y$ is odd.

Proof. Suppose that x is an even integer and y is an odd integer. Then $x = 2k$ and $y = 2n + 1$ for some integers k and n. We have

$$x + y = 2k + 2n + 1 = 2(k + n) + 1,$$

which is odd, as desired. Since addition is commutative, the same follows for x odd and y even. □

(6) Prove the following "if and only if" statement.

Theorem 6. *Suppose that a, b, and c are elements of a group G and $c = c^{-1}$. Then, $ab = c$ if and only if $abc = e$.*

We assume the whole first sentence, and we need to prove the statement "If $ab = c$, then $abc = e$." and the statement "If $abc = e$, then $ab = c$."

Proof. Suppose that a, b, and c are elements of a group G and $c = c^{-1}$.
$\boxed{\Rightarrow}$ Assume that $ab = c$. Multiplying on each side by c, we get

$$\begin{aligned} abc &= cc \\ &= cc^{-1} \quad (\text{since } c = c^{-1}) \\ &= e. \end{aligned}$$

$\boxed{\Leftarrow}$ Assume that $abc = e$. Multiplying on each side by c^{-1}, we get

$$\begin{aligned} abcc^{-1} &= c^{-1} \\ ab(cc^{-1}) &= c \quad (\text{since } c = c^{-1}) \\ ab &= c. \end{aligned}$$

$\square$