Math 108 - Introduction to Abstract Mathematics
Practice Final Exam

Name: ________________________________

Student ID: __________________________

Section: ______________________________

You have two hours to complete this exam. No books, references, cell phones, or communication of any sort is allowed during the exam. Write your answers in the space given below each problem, and if you need more room for a problem, you can go to the back of a page.

The table below is not to be filled in by you; it is for grading use only. (Grading scheme coming soon)
1. Three wolves, Alpha, Beta, and Gamma, have peculiar language habits. One of them (the truth-teller) always tells the truth, another (the liar) always lies, and the third (the copycat) tells the truth if and only if the previously spoken statement it heard was true.

They have the following conversation:

   Alpha: “Gamma always lies.”
   Beta: “I never lie.”
   Gamma: “Yes, you do!”
   Alpha: “No, he doesn’t!”

Which is the liar, which is the truth teller, and which is the copycat? Explain your answer, and show it is the only valid solution. SOLUTION: Since Gamma and Alpha each contradict a previous statement that they just heard, they cannot be the copycat. Therefore Beta is the copycat. But then Beta’s statement ”I never lie” is false, and so Alpha is lying as well just before him (since Beta copies the previous statement’s truth value). Now, analyzing each subsequent sentence, we find the sequence of statements are False, False, True, False, which is consistent with Alpha being the liar, Gamma the truth teller, and Beta the copycat.
2. Computational problems (25 points):

(a) Today is Thursday. What day of the week will it be 3^{500} days from today?

SOLUTION: We will compute $3^{500} \mod 7$. Note that $3^3 = 27 \equiv -1 \pmod{7}$, so we have:

\[
3^{500} = (3^3)^{166} \cdot 3^2 \\
\equiv (-1)^{166} \cdot 3^2 \pmod{7} \\
\equiv 9 \pmod{7} \\
\equiv 2 \pmod{7}
\]

Therefore, the day of the week will be two days from Thursday, which is Saturday.

(b) Evaluate this product as a simplified permutation in cycle notation, and then compute its inverse:

\[(1532)(476)(1735)(24) = \]

SOLUTION: The product is (164)(27), and its inverse is (461)(72).

(c) There are 105 cows in the UC Davis Dairy Teaching and Research Facility. Of them, 50 are spotted, 45 are docile (the others are aggressive), and 46 are overweight. Exactly 15 are both spotted and docile, exactly 20 are both docile and overweight, and exactly 16 are both spotted and overweight. Five of the cows have none of these three properties. How many spotted, aggressive, overweight cows are there in the facility?

SOLUTION: Let $S$ be the set of spotted cows, $D$ the set of docile cows, and $V$ the set of overweight cows. The Inclusion-Exclusion formula says that

\[|S \cup D \cup V| = |S| + |D| + |V| - |S \cap V| - |S \cap D| - |V \cap D| + |S \cap V \cap D|.
\]

We know all but one of these values from the problem: since 5 are in none of the sets, the union has size 100, the three sets have sizes 50, 45, and 46, and the three intersections have sizes 15, 20, 16. So:

\[100 = 50 + 45 + 46 - 15 - 20 - 16 + |S \cap V \cap D|\]

and so $|S \cap V \cap D| = 10$. This is the number of spotted, overweight, docile cows, so the number of spotted, overweight, aggressive cows are those that are spotted and overweight (16 total) but not docile (10 of these.) Therefore there are $16 - 10 = 6$ of the cows we are looking for.
3. **True or False**: (1 point each) State whether each of the following is True or False. (Write out the entire word “True” or “False” for your answer for each, rather than just T or F, so that we can easily read what you wrote.)

(a) \( \{1, 2, 3\} \subseteq \{\{1, 2, 3\}\} \)

**SOLUTION:** False

(b) \( \{a, c, e\} \subseteq \{a, b, c\} \cup \{c, e, f\} \)

**SOLUTION:** True

(c) \( N \in \mathcal{P}(N) \)

**SOLUTION:** True

(d) \( \forall A, \emptyset \subseteq A \)

**SOLUTION:** True

(e) \( \forall A, A \nsubseteq \emptyset \)

**SOLUTION:** False

(f) \( \forall A, \exists B, A \cap B = \emptyset \) and \( (A \cup B) \subseteq A \)

**SOLUTION:** True

4. **Injective, Surjective, Bijective, oh my!** For each of the following functions, determine whether it is injective and whether it is surjective. If it is bijective, find its inverse.

(a) \( f : \mathbb{R} \rightarrow \mathbb{R} \) by \( f(x) = 2x + 1 \).

**SOLUTION:** \( f \) is bijective with inverse \( f^{-1}(x) = (x - 1)/2 \)

(b) \( g : \mathbb{Z} \rightarrow \mathbb{N} \) by \( g(x) = |x| \).

**SOLUTION:** \( g \) is surjective but not injective.
5. **Is it a Group? Is it a Ring? No... it’s a Field!**

(a) For each of the following, determine whether or not it is a group. If it is not a group, state why.

- $({\mathbb{R}}, \cdot)$  
  **SOLUTION:** Not a group, 0 has no inverse

- $({\mathbb{Z}}, +)$  
  **SOLUTION:** Is a group

- $({\mathbb{Z}}/6{\mathbb{Z}}, \cdot)$  
  **SOLUTION:** Not a group, 0 has no inverse

- $({\mathbb{N}}, +)$  
  **SOLUTION:** Not a group, 1 has no inverse since $-1 \not\in {\mathbb{N}}$

- $\{\text{id}, (123), (132)\}, \circ$  
  **SOLUTION:** Is a group.

(b) Which of the following are rings? If it is not a ring, state why. If it is a ring, determine whether it is also a field.

- $({\mathbb{S}}_n, \circ, \circ)$  
  **SOLUTION:** Not a ring; $({\mathbb{S}}_n, \circ)$ is not abelian, and distributive law doesn’t hold.

- $\{0\}, +, \cdot$  
  **SOLUTION:** Is a ring and a field.

- $({\mathbb{Z}}, +, \cdot)$  
  **SOLUTION:** Is a ring but not a field because 2 has no inverse.

- $({\mathbb{C}}, +, \cdot)$  
  **SOLUTION:** Is a ring and a field.
6. Fill in the input line numbers for each of the reasons in the following formal proof in the Predicate Logic axiom system. Blanks (\(\_\)) are given for each of the numbers that should be filled in. Each line is one point.

**Theorem 1.** \((\exists x, P(x) \Rightarrow Q) \iff (\forall x, P(x) \Rightarrow Q)\)

**Proof.**

1. Assume \((\exists x, P(x)) \Rightarrow Q\) -
2. Let \(y\) be arbitrary -
3. Assume \(P(y)\) -
4. \(\exists x, P(x)\) \(\exists +; 3\)
5. \(Q\) \(\Rightarrow -; 1, 4\)
6. \(\Leftarrow\) -
7. \(P(y) \Rightarrow Q\) \(\Rightarrow +; 3, 5, 6\)
8. \(\Leftarrow\) -
9. \(\forall x, P(x) \Rightarrow Q\) \(\forall +; 2, 7, 8\)
10. \(\Leftarrow\) -
11. \((\exists x, P(x)) \Rightarrow Q\) \(\Rightarrow (\forall x, P(x) \Rightarrow Q)\) \(\Rightarrow +; 1, 9, 10\)
12. Assume \(\forall x, P(x) \Rightarrow Q\) -
13. Assume \(\exists x, P(x)\) -
14. For some \(z\) -
15. \(P(z)\) \(\exists -; 13\)
16. \(P(z) \Rightarrow Q\) \(\forall -; 12\)
17. \(Q\) \(\Rightarrow -; 15, 16\)
18. \(\Leftarrow\) -
19. \((\exists x, P(x)) \Rightarrow Q\) \(\Rightarrow +; 13, 17, 18\)
20. \(\Leftarrow\) -
21. \((\forall x, P(x) \Rightarrow Q) \Rightarrow (\exists x, P(x)) \Rightarrow Q)\) \(\Rightarrow +; 12, 19, 20\)
22. \((\exists x, P(x)) \Rightarrow Q\) \(\iff (\forall x, P(x) \Rightarrow Q)\) \(\Leftarrow +; 11, 21\)

\(\Box\)
7. (20 points) Define the sequence $b_0, b_1, b_2, \ldots$ by the recursion $b_0 = 2$, $b_1 = 5$, and $b_n = 5b_{n-1} - 6b_{n-2}$ for all $n \geq 2$. Use strong induction to prove that for all $n \geq 0$, $b_n = 2^n + 3^n$.

**SOLUTION:** For the base cases, note that for $n = 0$ we have $2^0 + 3^0 = 1 + 1 = 2 = b_0$ and for $n = 1$ we have $2^1 + 3^1 = 2 + 3 = 5 = b_1$.

For the induction step, let $k \geq 1$ be arbitrary and assume that for all natural numbers $j \leq k$, we have $b_j = 2^j + 3^j$. Then by the recursion at $n = k + 1$, we have

$$b_{k+1} = 5b_k - 6b_{k-1} = 5(2^k + 3^k) - 6(2^{k-1} + 3^{k-1})$$

$$= 5 \cdot 2^k + 5 \cdot 3^k - 6 \cdot 2^{k-1} - 6 \cdot 3^{k-1}$$

$$= 2 \cdot 2^k + 3 \cdot 3^k$$

$$= 2^{k+1} + 3^{k+1}$$

where the second equality above is by the induction hypothesis for $j = k$ and $j = k - 1$. Thus we have shown the statement holds for $k + 1$, and the induction is complete.
8. (20 points) Prove that, for any sets $A, B, C$, if $A \subseteq B$ then $C - B \subseteq C - A$. Is the converse of this statement true? Why or why not?

(You must be fully rigorous in your use of definitions for subsets and set operations.)

**SOLUTION:** Assume $A \subseteq B$. Let $x \in C - B$; we wish to show $x \in C - A$. Then $x \in C$ and $x \notin B$ by the definition of set subtraction.

Assume for contradiction that $x \in A$. Since $A \subseteq B$, $x \in B$, a contradiction since $x \notin B$.

Therefore $x \notin A$, and so $x \in C - A$ as desired. This proves $C - B \subseteq C - A$.

The converse is not true; if $C = \emptyset$ and $A = \{1\}$ and $B = \{2\}$ then $C - B = \emptyset \subseteq C - A$ but $A \notin B$. 
9. Give a combinatorial proof of the identity

\[ \binom{n}{m} \binom{n-m}{k} = \binom{n}{k} \binom{n-k}{m}. \]

(You may NOT use algebra, induction, factorials, or any other method. The proof must be entirely combinatorial.)

The left hand side counts the number of ways to choose, from a school of \( n \) students, a basketball team of \( m \) people (in \( \binom{n}{m} \) ways), and then choose a cheerleading squad of \( k \) people from the remaining \( n-m \) (in \( \binom{n-m}{k} \) ways).

The right hand side similarly counts the number of ways to first choose the basketball team and then choose the cheerleading squad, so both quantities count the number of ways to choose a \( m \)-person basketball team and a \( k \)-person cheerleading squad. It follows that

\[ \binom{n}{m} \binom{n-m}{k} = \binom{n}{k} \binom{n-k}{m}. \]
10. Prove that the set \( \mathbb{N} \times \mathbb{N} \) is countable.

**SOLUTION 1:** We can write \( \mathbb{N} \times \mathbb{N} \) as a countable union of countable sets as follows: let \( A_i = \{(i, n) : n \in \mathbb{N}\} \) for all \( i \in \mathbb{N} \). Then there are countably many sets \( A_i \), and each \( A_i \) is countable. Clearly \( \mathbb{N} \times \mathbb{N} = \bigcup_i A_i \), so it is countable.

**SOLUTION 2:** Every ordered pair \((x, y)\) has an associated sum \( x + y \in \mathbb{N} \). There are finitely many pairs with a given sum \( s \), namely \((0, s)\), \((1, s - 1)\), \((2, s - 2)\), \ldots, \((s, 0)\). Let \( B_s \) be the set of ordered pairs in \( \mathbb{N} \times \mathbb{N} \) with sum equal to \( s \); then each \( B_s \) is finite and the union \( B_0 \cup B_1 \cup B_2 \cup \cdots \) is equal to \( \mathbb{N} \times \mathbb{N} \). Therefore our set is a countable union of finite sets, which is countable.

**SOLUTION 3:** We can find an explicit bijection with \( \mathbb{N} \) as follows. Define \( f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \) by \( f(m, n) = 2^m(2n + 1) - 1 \).

To show \( f \) is injective, assume \( f(m, n) = f(x, y) \). Then \( 2^m(2n + 1) = 2^x(2y + 1) \). The left hand side and right hand side of this equation are equal and thus have the same power of 2 in their prime factorization, and therefore \( m = x \). So we can cancel the powers of 2 and find \( 2n + 1 = 2y + 1 \), which implies \( x = y \). Therefore \( (m, n) = (x, y) \), so \( f \) is injective.

To show \( f \) is surjective, let \( x \in \mathbb{N} \). Let \( m \) be the exponent of 2 in the prime factorization of \( x + 1 \) (note that \( x + 1 \geq 1 \) so it has a prime factorization). Then \( x + 1 = 2^m(2n + 1) \) for some \( n \in \mathbb{N} \), and so \( f(m, n) = x \). This completes the proof that \( f \) is bijective.
11. Let $G$ be a group and let $a \in G$. The **centralizer** of $a$ in $G$, written $C_G(a)$, is the set

$$C_G(a) = \{ x \in G : xa = ax \}.$$ 

In other words, it is the set of all elements that commute with $a$ under the group operation. Prove that $C_G(a)$ is a subgroup of $G$.

**SOLUTION:** To prove $C_G(a)$ is a subgroup, it suffices to show that it is nonempty and that for all $x, y \in C_G(a)$, $xy^{-1} \in C_G(a)$. It is nonempty because $ae = ea$ and so the identity element $e$ is in $C_G(a)$. Now, let $x, y \in C_G(a)$. Then $xa = ax$ and $ya = ay$. Multiplying both sides of the latter equation on the left and right by $y^{-1}$, we get:

$$y^{-1}yay^{-1} = y^{-1}ayy^{-1}$$

(yay!) and the $yy^{-1}$ and $y^{-1}y$ above cancel, leaving us with

$$ay^{-1} = y^{-1}a.$$ 

Therefore, we have $xy^{-1}a = xay^{-1} = axy^{-1}$, and so $xy^{-1} \in C_G(a)$ as desired.