Mathematics GU4041
Introduction to Modern Algebra

Answers to Midterm Exam #1

October 6, 2016

1. There exist a set $\mathbf{N}$, an element $0 \in \mathbf{N}$, and a successor function $f : \mathbf{N} \to \mathbf{N}$, denoted $f(n) = n'$, satisfying the following axioms.

P1: There does not exist $n \in \mathbf{N}$ such that $0 = n'$.

P2: For all $m, n \in \mathbf{N}$, if $m' = n'$, then $m = n$.

P3: If $S \subset \mathbf{N}$ is a subset, if $0 \in S$, and if all $n \in S$ satisfy $n' \in S$, then $S = \mathbf{N}$.

2. Note $x \in X \setminus (A \cup B) \iff x \in X$ but $x \notin A \cup B \iff x \in X$ but it is false that $x \in A$ or $x \in B \iff x \in X$ and $x \notin A$ and $x \notin B \iff x \in X$ and $x \notin A$ and $x \in X$ and $x \notin B \iff x \in X \setminus A$ and $x \in X \setminus B \iff x \in (X \setminus A) \cap (X \setminus B)$. Hence the two sides are equal by the definition of set equality.

3. If $g \circ f(x) = g \circ f(y)$, then $g(f(x)) = g(f(y))$ (by definition of $\circ$), hence $f(x) = f(y)$ (since g is injective), hence $x = y$ (since f is injective). Hence $g \circ f$ is injective.

Given $z \in U$, there exists $y \in T$ such that $z = g(y)$ (since g is surjective), and there exists $x \in S$ such that $y = f(x)$ (since f is surjective). Then $x = g(f(x)) = g \circ f(x)$, so $g \circ f$ is surjective.

Alternative proof: By the main theorem on inverses, there exist functions $f^{-1} : T \to S$ and $g^{-1} : U \to T$ such that $f^{-1} \circ f = \mathrm{id}_S$, $f \circ f^{-1} = \mathrm{id}_T$, $g^{-1} \circ g = \mathrm{id}_T$, and $g \circ g^{-1} = \mathrm{id}_U$. Then $(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ (\mathrm{id}_T) \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_U$ and $(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ (\mathrm{id}_T) \circ f = f^{-1} \circ f = \mathrm{id}_S$, so $f^{-1} \circ g^{-1}$ is an inverse for $g \circ f$. By the main theorem on inverses again, $g \circ f$ is bijective.

4. If $m \leq n$, then by definition of $\leq$ there exists $a \in \mathbf{N}$ such that $n = m + a$. Then $n^2 = n \cdot n = (m + a) \cdot (m + a) = (m + a) \cdot m + (m + a) \cdot a = (m^2 + am) + (ma + a^2) = m^2 + (am + ma + a^2)$. Since $\mathbf{N}$ is closed under addition and multiplication by the definitions of these operations, $am + ma + a^2 \in \mathbf{N}$, so $m^2 \leq n^2$ by the definition of $\leq$.

5. Yes: it is reflexive since $x - x = 0 \in \mathbf{Z}$, symmetric since $x - y \in \mathbf{Z}$ implies $y - x = -(x - y) \in \mathbb{Z}$ (as taking the negative is an operation $\mathbf{Z} \to \mathbf{Z}$), and transitive since $x - y \in \mathbf{Z}$ and $y - z \in \mathbf{Z}$ imply $x - z = (x - y) + (y - z) \in \mathbb{Z}$ (as addition is an operation $\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$).

6. Since $a \,|\, b$, there exists $m \in \mathbf{Z}$ such that $b = am$, and since $b \,|\, c$, there exists $n \in \mathbf{Z}$ such that $c = bn$. Then $a + b + c = a + am + bn = a + am + (am)n = a(1 + m + mn)$ where $1 + m + mn \in \mathbf{Z}$ since $\mathbf{Z}$ is closed under addition and multiplication. Hence $a \,|\, a + b + c$.

7. By A4#4, $(i, n) = 1$ if and only if $[i] \in \mathbf{Z}_n$ has a reciprocal. Hence there exist $[c], [d] \in \mathbf{Z}_n$ such that $[ac] = [a][c] = [1]$ and $[bd] = [b][d] = [1]$ in $\mathbf{Z}_n$. Hence $[ab][cd] = [abcd] = [ac][bd] = [1][1] = [1] \in \mathbf{Z}_n$, so $[ab]$ also has a reciprocal and hence $(ab, n) = 1$.

Alternative proof: By the main theorem on gcd's, there exist $c, e \in \mathbf{Z}$ such that $ac + ne = 1$ and $d, f \in \mathbf{Z}$ such that $bd + nf = 1$. Hence $ac = 1 - ne$ and $bd = 1 - nf$, so $abcd = (1 - ne)(1 - nf) = 1 - n(e + f - nef)$, so $(ab)(cd) + n(e + f - nef) = 1$. Hence 1 is the least positive integer of the form $(ab)x + ny$ for $x, y \in \mathbf{Z}$, so by the main theorem on gcd's again, $(ab, n) = 1$.