Mathematics W4041x
Introduction to Modern Algebra

Answers to Practice Midterm #1

October 6, 2016

1. A relation $\sim$ on a set S is an equivalence relation if:

(a) it is *reflexive*: for all $x \in S$, $x \sim x$;

(b) it is *symmetric*: for all $x, y \in S$, $x \sim y$ implies $y \sim x$; and

(c) it is *transitive*: for all $x, y, z \in S$, $x \sim y$ and $y \sim z$ imply $x \sim z$.

2. Since $A \setminus (B \cup C) = \{x \in A \,|\, x \notin B \cup C\}$, we have the chain of equivalences $x \in A \setminus (B \cup C) \Leftrightarrow x \in A$ and $x \notin B \cup C \Leftrightarrow x \in A$ but it is false that ($x \in B$ or $x \in C$) $\Leftrightarrow x \in A$ and $x \notin B$ and $x \notin C \Leftrightarrow x \in A \setminus B$ and $x \notin C \Leftrightarrow x \in (A \setminus B) \setminus C$. Hence by the definition of set equality, $A \setminus (B \cup C) = (A \setminus B) \setminus C$.

3. P1, saying that $[0]$ is not a successor, is violated: indeed, $[0] = [4 + 1] = f([4])$. P2, saying that f is injective, is satisfied: indeed, if $f([i]) = f([j])$, then $[i+1] = [j+1]$, so $5 \,|\, (i+1) - (j+1) = i - j$ using commutativity and associativity in $\mathbb{Z}$, so $[i] = [j]$. P3, the axiom of induction, is satisfied, as the following proof shows. Assume $[0] \in S$ and $[n] \in S$ implies $[n + 1] \in S$. Taking $n = 0$ in the latter, we find that $[1] = [0 + 1] \in S$; taking $n = 1$, $[2] \in S$; taking $n = 2$, $[3] \in S$, and taking $n = 3$, $[4] \in S$. Hence every element of $\mathbb{Z}_5$ is in S, so $S = \mathbb{Z}_5$.

4. For f to be well-defined means that for all $i, j \in \mathbb{Z}$, $i \equiv j \pmod m$ implies $[ki] = [kj] \in \mathbb{Z}_m$, that is, $ki \equiv kj \pmod n$. Equivalently, for all $i, j \in \mathbb{Z}$, $m \,|\, (i - j)$ implies $n \,|\, (ki - kj)$. If we suppose $n \,|\, km$, then $m \,|\, (i - j)$ implies $n \,|\, km \,|\, k(i - j) = ki - kj$, so f is well-defined. Conversely, if we suppose f is well-defined, let $i = m$ and $j = 0$. Then $m \,|\, (i - j) = m$, so $n \,|\, (ki - kj) = k(i - j) = km$.

5. If $m+n = m$, then $m+n = m+0$ by the definition of addition, hence $n+m = 0+m$ by commutativity, hence $n = 0$ by cancellation. Thus we have proved that if $m + n \neq m$ is false, then $n = 0$ is true. That is, $m + n \neq m$ or $n = 0$.

6. If $m \,|\, n$ and $p \,|\, q$, then there exist $c, d \in Z$ such that $n = cm$ and $q = dp$, but then $nq = (cm)(dp) = (cd)(mp)$ by commutativity and associativity, so $mp \,|\, nq$.

7. By the Main Theorem on GCDs, (x, y) is the least positive element of $\{ax + by \,|\, a, b \in \mathbb{Z}\}$, while $(x + y, y)$ is the least positive element of $\{c(x + y) + dy \,|\, c, d \in \mathbb{Z}\}$. But $ax + by = a(x + y) + (b - a)y$, so every element of the first set belongs to the second; and $c(x + y) + dy = cx + (c + d)y$, so every element of the second set belongs to the first. Hence the two sets are equal.