Abstract Algebra 113

Alexander Paulin

September 18, 2009

Question Sheet 1 Solutions

Question 1

If $S$ is a set of cardinality 5 then (i) there are $5^5$ maps from $S$ to itself and (ii) there are $5!$ bijections from $S$ to itself.

Question 2

Let $f$ and $g$ both be injective. Let $x, y \in A$ such that $gf(x) = gf(y)$. Hence $g(f(x) = g(f(y))$. Injectivity of $g \Rightarrow f(x) = f(y)$. Injectivity of $f \Rightarrow x = y$. Hence $gf$ is injective.

Let $f$ and $g$ both be surjective. Let $z \in C$. Surjectivity of $g \Rightarrow \exists y \in B$ such that $g(y) = z$. Surjectivity of $f \Rightarrow \exists x \in A$ such that $f(x) = y$. Hence $gf(x) = z$. Thus $gf$ is surjective.

If $gf$ is injective then we can only deduce that $f$ is injective. In general $g$ may not be injective as a function on all of $B$. It must however be injective when restricted to the image of $f$.

Question 3

1. (reflexive). $\forall a \in \mathbb{Z} \ a - a = 0. \ m|0$, hence $a \sim a$.

2. (symmetric) Let $a, b \in \mathbb{Z}$ such that $a \sim b$. Thus $m|(a - b) \Rightarrow m|(b - a) \Rightarrow b \sim a$.

3. Let $a, b, c \in \mathbb{Z}$ such that $a \sim b$ and $b \sim c \Rightarrow m|(a - b)$ and $m|(b - c) \Rightarrow m|(a - c) \Rightarrow a \sim c$.

Question 4

Let $S$ be a set together with an equivalence relation $\sim$. Let $X, Y \subset S$ be two equivalence classes with non-trivial intersection. Let $s \in X \cap Y$. Given $x \in X$ and $y \in Y$ we know by definition that $x \sim s$ and $y \sim s$. Thus by transitivity $x \sim Y$. Thus every element of $X$ is equivalent to every element of $Y$. By the maximality $X = Y$.  

1
Question 5

Let’s do (ii) first. \(0a = (0 + 0)a = 0a + 0a\) Adding \(-0a\) to both sides tells us that \(0a = 0\). Now we’ll do (i). \(a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = 0\). This and the fact that addition is commutative shows that \((-1)a = -a\).

Question 6

Assume that \(x = \frac{p}{q}\) is a non-integral solution. By the FTOA we know that we may choose \(p\) and \(q\) to be coprime. Thus \(p^n = q^n c\). Because \(p\) and \(q\) are coprime they do not share any common prime divisors. This would contradict the uniqueness of prime factorisation in the FTOA. Hence no such \(p\) and \(q\) can exist.

Question 7

A case by case check shows the only solution is \([1] \in \mathbb{Z}/23\mathbb{Z}\).

Question 8

Let \(a, b \in \mathbb{Z}\) be coprime and \(x_0, y_0 \in \mathbb{Z}\) such that \(ax_0 + by_0 = 1\). Then \(\forall k \in \mathbb{Z} \ x_k = x_0 + kb, y_k = y_0 - ka\) are solutions. Hence there are infinitely many solutions. If \(x, y \in \mathbb{Z}\) such that \(ax + by = 1 \Rightarrow a(x - x_0) = b(y - y_0)\) Because \(a\) and \(b\) are coprime we know that \(b|(x - x_0)\) and \(a|(y - y_0)\). Hence \(\exists k \in \mathbb{Z}\) such that \(x = x_k\). This forces \(y = y_k\). Thus the above list is complete.