Written Assignment 9
Math 290, Dr. Walnut

Lucas Bouck

12/11/15

1 Problem 1a

Let $f : A \to B$. Prove that f is injective if and only if for all $D \subseteq A, f^{-1}(f(D)) = D$.
Proof:
($\Leftarrow$) (By contrapostive)

Let $f : A \to B$. Assume f is not injective. We want to show that there exists a set $D \subseteq A$ such that $f^{-1}(f(D)) \neq D$. Since f is not injective, there exists $x, y \in A$ such that $f(x) = f(y)$ and $x \neq y$. Let's call $f(x) = z = f(y)$. Let $D = \{x\}$. Since $x \in A$, $D \subseteq A$. Since $f(x) = z$, $f(D) = \{z\}$. Since $f(x) = z$ and $f(y) = z$, $f^{-1}(f(D)) = \{x, y\}$. Since $y \notin D$, $f^{-1}(f(D)) \neq D$. Thus, there exists a $D \subseteq A$ such that $f^{-1}(f(D)) \neq D$. By contrapostive, if for all $D \subseteq A, f^{-1}(f(D)) = D$, then f is injective.
($\Rightarrow$)

Let $f : A \to B$. Assume f is injective. We want to show that for all $D \subseteq A, f^{-1}(f(D)) = D$. Let $D \subseteq A$. We want to show inclusion both ways. Let $x \in D$. Since f is a function, there exists a $y \in B$ such that $f(x) = y$. Since there exists an $x \in D$ such that $f(x) = y$, $y \in f(D)$. Since $f(x) = y$ and $y \in f(D)$, $x \in f^{-1}(f(D))D$. Thus, $D \subseteq f^{-1}(f(D))$.

We must now show that $f^{-1}(f(D)) \subseteq D$. Let $x \in f^{-1}(f(D))$. Then, there exists a $y \in f(D)$ such that $f(x) = y$. Since $y \in f(D)$, there exists a $z \in D$ such that $f(z) = y$. Since $f(x) = f(z)$, and f is injective, $x = z$. Since $z \in D$, $x \in D$. Therefore, $f^{-1}(f(D)) \subseteq D$. Because $D \subseteq f^{-1}(f(D))$ and $f^{-1}(f(D)) \subseteq D$, $f^{-1}(f(D)) = D$. Thus, if f is injective then for all $D \subseteq A, f^{-1}(f(D)) = D$.

2 Problem 1b

Let $f : A \to B$. Prove that f is surjective if and only if for all $E \subseteq B$, $f(f^{-1}(E)) = E$.
Proof:
($\Leftarrow$) (By contrapositve)

Let $f : A \to B$. Assume f is not surjective. We want to show that there exists a set $E \subseteq B$ such that $E \neq f(f^{-1}(E))$. Since f is not surjective, there exists an $x \in B$ such that

for all $a \in A$, $f(a) \neq x$. Let $E = \{x\}$. Since for all $a \in A$, $f(a) \neq x$, $f^{-1}(E) = \emptyset$. Since $f(f^{-1}(E))$ contains all z such that there exists an element, $y \in f^{-1}(E)$ such that $f(y) = z$, and $f^{-1}(E) = \emptyset$, then $f(f^{-1}(E)) = \emptyset$. Since $x \notin \emptyset$, $x \notin f(f^{-1}(E))$, and $E \neq f(f^{-1}(E))$. Therefore, by contrapositive, if for all $E \subseteq B$, $f(f^{-1}(E)) = E$, then f is surjective.
$(\Rightarrow)$

Let $f : A \to B$. Assume f is surjective. We want to show that for all $E \subseteq B$, $f(f^{-1}(E)) = E$. We must show inclusion both ways. Let $x \in E$. Because f is surjective, there exists a $z \in A$ such that $f(z) = x$. Since $x \in E$ and $f(z) = x$, $z \in f^{-1}(E)$. Since $f(z) = x$ and $z \in f^{-1}(E)$, $x \in f(f^{-1}(E))$. Thus, $E \subseteq f(f^{-1}(E))$.

We will now show that $f(f^{-1}(E)) \subseteq E$. Let $x \in f(f^{-1}(E))$. Then, there exists a $z \in f^{-1}(E)$ such that $f(z) = x$. Since $z \in f^{-1}(E)$, there exists a $d \in E$ such that $f(z) = d$. Since f is a function, $f(z) = d$, and $f(z) = x$, $x = d$. Since $d \in E$, $x \in E$, and $f(f^{-1}(E)) \subseteq E$. Since $f(f^{-1}(E)) \subseteq E$ and $E \subseteq f(f^{-1}(E))$, $f(f^{-1}(E)) = E$. Therefore, if f is surjective, for all $E \subseteq B$, $f(f^{-1}(E)) = E$.

3 Problem 2a

Let $p, q \in \mathbb{N}$ be relatively prime. Prove that given $\bar{y}^{pq} \in \mathbb{Z}_{pq}$, there exist unique $\bar{c}^p \in \mathbb{Z}_p$ and $\bar{d}^q \in \mathbb{Z}_q$ such that $\bar{y}^p = \bar{c}^p$ and $\bar{y}^q = \bar{d}^q$.

Proof:

Let $\overline{y}^{pq} \in \mathbb{Z}_{pq}$. We want to show that there exist unique $\bar{c}^p \in \mathbb{Z}_p$ and $\bar{d}^q \in \mathbb{Z}_q$ such that $\bar{y}^p = \bar{c}^p$ and $\bar{y}^q = \bar{d}^q$. Let $c = y \pmod p$ and let $d = y \pmod q$. Then, $p|(y-c)$ and $q|(y-d)$. Since $p|(y-c)$ and $q|(y-d)$, $\overline{y}^p = \overline{c}^p$, and $\overline{y}^q = \overline{d}^q$. We have shown that there exist $\bar{c}^p \in \mathbb{Z}_p$ and $\bar{d}^q \in \mathbb{Z}_q$ such that $\bar{y}^p = \bar{c}^p$ and $\bar{y}^q = \bar{d}^q$. We now must show that $\bar{c}^p$ and $\bar{d}^q$ are unique.

Suppose $\overline{x}^p = \overline{y}^p$ and $\overline{z}^q = \overline{y}^q$. Then, $p|(y-x)$, and $q|(y-z)$, which means $pm = y-x$ and $qk = y-z$ for $m, k \in \mathbb{Z}$. Rearranging these gets us $x = y-pm$ and $z = y-qk$. Since $\overline{y}^p = \overline{c}^p$ and $\overline{y}^q = \overline{d}^q$, $p|(y-c)$, and $q|(y-d)$, which means $pa = y-c$ and $qb = y-d$ for $a, b \in \mathbb{Z}$. Rearranging these gets us $c = y - pa$ and $d = y - qb$. Then, $x - c = (y - pm) - (y - pa) = (pa - pm) = p(a-m)$, and $z - d = (y - qk) - (y - qb) = (qb - qk) = q(b-k)$. Since $a, m, b, k \in \mathbb{Z}$, $(a-m) \in \mathbb{Z}$ and $(b-k) \in \mathbb{Z}$. Then, $p|(x-c)$, and $q|(z-d)$. Therefore, $\overline{x}^p = \overline{c}^p$, $\overline{z}^q = \overline{d}^q$, and $\overline{c}^p$ and $\overline{d}^q$ are unique. Therefore, given $\bar{y}^{pq} \in \mathbb{Z}_{pq}$, there exist unique $\bar{c}^p \in \mathbb{Z}_p$ and $\bar{d}^q \in \mathbb{Z}_q$ such that $\bar{y}^p = \bar{c}^p$ and $\bar{y}^q = \bar{d}^q$.

4 Problem 2b

Let $p, q \in \mathbb{N}$ be relatively prime. Prove that there is a bijection $f : \mathbb{Z}_{pq} \to \mathbb{Z}_p \times \mathbb{Z}_q$.

Proof:

Let $p, q \in \mathbb{N}$ be relatively prime. We want to show that there exists a bijection $f : \mathbb{Z}_{pq} \to \mathbb{Z}_p \times \mathbb{Z}_q$. Let $f : \mathbb{Z}_{pq} \to \mathbb{Z}_p \times \mathbb{Z}_q$, and define $f(\overline{y}^{pq}) = (\overline{c}^p, \overline{d}^q)$ such that $\bar{y}^p = \bar{c}^p$ and

$\bar{y}^q = \bar{d}^q$. We will show that f is well-defined, f is surjective, and f is injective.

Let $\overline{y}^{pq} \in \mathbb{Z}_{pq}$. By the Chinese Remainder Theorem, there exist $\bar{c}^p \in \mathbb{Z}_p$ and $\bar{d}^q \in \mathbb{Z}_q$ such that $\bar{y}^p = \bar{c}^p$ and $\bar{y}^q = \bar{d}^q$. Therefore, $(\overline{y}^{pq}, (\bar{c}^p, \bar{d}^q)) \in f$, and $dom(f) = \mathbb{Z}_{pq}$. Suppose that $f(\overline{y}^{pq}) = (\overline{x}^p, \overline{z}^q)$. By the Chinese Remainder Theorem, $\bar{c}^p$ and $\bar{d}^q$ are unique solutions such that $\bar{y}^p = \bar{c}^p$ and $\bar{y}^q = \bar{d}^q$. Therefore, $(\overline{x}^p, \overline{z}^q) = (\bar{c}^p, \bar{d}^q)$, and f is well-defined in that there is one $f(\overline{y}^{pq})$ for all $\overline{y}^{pq}$.

We now want to show that f is surjective. Let $(\bar{c}^p, \bar{d}^q) \in \mathbb{Z}_p \times \mathbb{Z}_q$. Based on the first part of the Chinese Remainder Theorem proved in class, there exists an unique $\overline{y}^{pq} \in \mathbb{Z}_{pq}$ such that $\bar{y}^p = \bar{c}^p$ and $\bar{y}^q = \bar{d}^q$. Therefore, there exists a $\overline{y}^{pq} \in \mathbb{Z}_{pq}$ such that $f(\overline{y}^{pq}) = (\bar{c}^p, \bar{d}^q)$. Therefore, f is surjective.

We finally want to prove that f is injective. Let $\overline{x}^{pq}, \overline{y}^{pq} \in \mathbb{Z}_{pq}$. Assume that $f(\overline{x}^{pq}) = f(\overline{y}^{pq}) = (\bar{c}^p, \bar{d}^q)$. Using the definition of f, $\overline{x}^p = \overline{c}^p$, $\overline{y}^p = \overline{c}^p$, $\overline{x}^q = \overline{d}^q$, and $\overline{y}^q = \overline{d}^q$. This means $p|x-c$, $p|y-c$, $q|x-d$, and $q|y-d$, which means $pm = x-c$, $pn = y-c$, $qk = x-d$, and $ql = y-d$ for $m, n, k, l \in \mathbb{Z}$. Then, we get $p(m-n) = x-c-y+c = x-y$ and $q(k-l) = x-d-y+d = x-y$. Let $m-n = a$ and $k-l = b$. Since $m, n, k, l \in \mathbb{Z}$, $a, b \in \mathbb{Z}$, and $p|x-y$ and $q|x-y$. Since p and q are relatively prime, $gcd(p,q) = 1$, and $pq|x-y$. Therefore, $\overline{x}^{pq} = \overline{y}^{pq}$, and f is injective.

Since we have shown that there exists a $f : \mathbb{Z}_{pq} \to \mathbb{Z}_p \times \mathbb{Z}_q$ that surjective and injective, we have shown that there exists a bijection $f : \mathbb{Z}_{pq} \to \mathbb{Z}_p \times \mathbb{Z}_q$.