Kris Harper
MATH 25700
Homework 1 October 2, 2009

Problem 1. *Determine whether the following functions f are well-defined:*
(a) $f : \mathbb{Q} \to \mathbb{Z}$ defined by $f(a/b) = a$.
(b) $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(a/b) = a^2/b^2$.

Proof. (a) Here f is not well defined. Note that $f(1/2) = 1$ and $f(2/4) = 2$ yet $1/2 = 2/4$.

(b) Now f is well defined. Let $a/b, c/d \in \mathbb{Q}$ such that $a/b = c/d$. We wish to show that $f(a/b) = f(c/d)$. Note that since $a/b = c/d$, squaring both sides gives $a^2/b^2 = c^2/d^2$ which is the desired equality. □

Problem 2. *Let $f : A \to B$ be a surjective map of sets. Prove that the relation*

$$a \sim b \text{ if and only if } f(a) = f(b)$$

is an equivalence relation whose equivalence classes are the fibers of f.

Proof. Clearly $\sim$ is reflexive since $f(a) = f(a)$ for all $a \in A$. Similarly if $a \sim b$ for $a, b \in A$ then $f(a) = f(b)$ and so $f(b) = f(a)$. Thus $b \sim a$ and $\sim$ is symmetric. Finally if $a \sim b$ and $b \sim c$ for $a, b, c \in A$, then $f(a) = f(b)$ and $f(b) = f(c)$. But then $f(a) = f(c)$ and so $a \sim c$. Thus $\sim$ is an equivalence relation.

Consider $\overline{a}$, the equivalence class of a, and let $b \in \overline{a}$. Then $f(b) = f(a)$ and so $b \in f^{-1}(a)$. Thus $\overline{a} \subseteq f^{-1}(a)$. Conversely, let $b \in f^{-1}(a)$. Then $f(b) = f(a)$ and $b \sim a$. Thus $b \in \overline{a}$ and $f^{-1}(a) \subseteq \overline{a}$. Therefore the equivalence classes of $\sim$ are precisely the fibers of f. □

Problem 3. *For each of the following pairs of integers a and b, determine their greatest common divisor, their least common multiple, and write the greatest common divisor in the form $ax + by$ for some integers x and y.*
(a) $a = 20$, $b = 13$.
(b) $a = 69$, $b = 372$.

(a) $(20, 13) = 1$. The least common multiple of 20 and 13 is 260. $1 = (2)20 + (-3)13$.

(b) $(69, 372) = 3$. The least common multiple of 69 and 372 is 8556. $3 = (27)69 + (-5)372$.

Problem 4. *Prove that if n is composite, then there are integers a and b such that n divides ab but n does not divide either a or b.*

Proof. Let n be composite. Then $n = p_1^{q_1} p_2^{q_2} \dots p_s^{q_s}$ for primes $p_1, \dots, p_s$ such that there exists i and j where $q_i \geq 1$ and $q_j \geq 1$ (if $i = j$ then $q_i > 1$). We can assume $i \leq j$. If $i < j$ let $a = p_1^{q_1} p_2^{q_2} \dots p_i^{q_i}$ and $b = p_{i+1}^{q_{i+1}} p_{i+2}^{q_{i+2}} \dots p_s^{q_s}$. Otherwise if $i = j$ let $a = p_1^{q_1} p_2^{q_2} \dots p_i^{q_i - 1}$ and $b = p_i p_{i+1}^{q_{i+1}} p_{i+2}^{q_{i+2}} \dots p_s^{q_s}$. Note that since a and b are multiples of prime numbers, both are greater than 1. Clearly $n \mid ab$ since n will divide itself. But since $n = ab$ and $a > 1$, $b > 1$ and $n > 1$, it cannot be that $n \mid a$ or $n \mid b$. □

Problem 5. *Determine the value $\varphi(n)$ for each integer $n \leq 30$ where ϕ denotes the Euler φ-function.*

$\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, $\varphi(9) = 6$, $\varphi(10) = 4$, $\varphi(11) = 10$, $\varphi(12) = 4$, $\varphi(13) = 12$, $\varphi(14) = 6$, $\varphi(15) = 8$, $\varphi(16) = 8$, $\varphi(17) = 16$, $\varphi(18) = 6$, $\varphi(19) = 18$, $\varphi(20) = 8$, $\varphi(21) = 12$, $\varphi(22) = 10$, $\varphi(23) = 22$, $\varphi(24) = 8$, $\varphi(25) = 20$, $\varphi(26) = 12$, $\varphi(27) = 18$, $\varphi(28) = 12$, $\varphi(29) = 28$, $\varphi(30) = 8$.

Problem 6. *If p is a prime prove there do not exist nonzero integers a and b such that $a^2 = pb^2$ (i.e. $\sqrt{p}$ is not a rational number).*

Kris Harper
MATH 25700
Homework 1 October 2, 2009

Proof. Let p be prime and assume nonzero integers a and b exist such that $a^2 = pb^2$. Then $p \mid a^2$ or equivalently $p \mid a \cdot a$. Thus $p \mid a$ and so there exists $c \in \mathbb{Z}$ such that $pc = a$. Then $p^2c^2 = a^2 = pb^2$ and $pc^2 = b^2$. Consequently $p \mid b^2$ and so $p \mid b$ as well. Then $a_1 = a/p$ and $b_1 = b/p$ are both integers and we have $a_1^2 = pb_1^2$. But the same argument holds and so $p \mid a_1$ and $p \mid b_1$. We can let the integers $a_2 = a_1/p$ and $b_2 = b_1/p$ and continue in this fashion until $b_n^2 = 1$. This forces $a_n^2 = p$, but p is prime and clearly not a perfect square. This is a contradiction and so a and b cannot exist. $\square$

Problem 7. *Let $f : A \to B$. The map f is injective if and only if f has a left inverse.*

Proof. Suppose that f is injective. Let $g : B \to A$ be the function such that for $b \in f(A) \subseteq B$, $g(b) = a$ where a is the unique element of A such that $f(a) = b$. We know a is unique because f is injective and that such an a exists because b is in the image of A. Define $g(c)$ for $c \in B \backslash f(A)$ to be anything. Then for $a \in A$ we have $g \circ f(a) = g(f(a)) = a$.

Conversely suppose that f has a left inverse. Then there exists $g : B \to A$ such that $g \circ f : A \to A$ is the identity. Consider $x, y \in A$ such that $x \neq y$. Then $g \circ f(x) = g(f(x)) \neq g(f(y)) = g \circ f(y)$ which implies $f(x) \neq f(y)$ (otherwise $g(f(x))$ would equal $g(f(y))$). Thus f is injective. $\square$

Problem 8. *If A and B are finite sets with the same number of elements then $f : A \to B$ is bijective if and only if f is injective if and only if f is surjective.*

Proof. Suppose f is bijective, then it is clearly injective. Now suppose f is injective. Let $|A| = |B| = n$. Since f is injective, two distinct elements of A are mapped by f to two distinct elements of B. There are n distinct elements of A and so $|f(A)| = n$. But $|B| = n$ as well and so f is surjective. Finally suppose that f is surjective. Then for each $b \in B$ there exists $a \in A$ such that $f(a) = b$. Since $|B| = n$ there must be at least n distinct elements of A which map to unique values of B. But $|A| = n$, therefore if $x \neq y$ in A, then $f(x) \neq f(y)$ in B. Thus f is both surjective and injective and so f is a bijection. $\square$

Problem 9. *Write out the multiplication table for D_6.*

$\times$	$\mathbf{I}$	$\mathbf{R_{120}}$	$\mathbf{R_{240}}$	$\mathbf{F_T}$	$\mathbf{F_L}$	$\mathbf{F_R}$
$\mathbf{I}$	I	R_{120}	R_{240}	F_T	F_L	F_R
$\mathbf{R_{120}}$	R_{120}	R_{240}	I	F_R	F_T	F_L
$\mathbf{R_{240}}$	R_{240}	I	R_{120}	F_L	F_R	F_T
$\mathbf{F_T}$	F_T	F_L	F_R	I	R_{120}	R_{240}
$\mathbf{F_L}$	F_L	F_R	F_T	R_{240}	I	R_{120}
$\mathbf{F_R}$	F_R	F_T	F_L	R_{120}	R_{240}	I

Problem 10. *Write out the multiplication table for D_8.*

$\times$	$\mathbf{I}$	$\mathbf{R_{90}}$	$\mathbf{R_{180}}$	$\mathbf{R_{270}}$	$\mathbf{V}$	$\mathbf{H}$	$\mathbf{D_L}$	$\mathbf{D_R}$
$\mathbf{I}$	I	R_{90}	R_{180}	R_{270}	V	H	D_L	D_R
$\mathbf{R_{90}}$	R_{90}	R_{180}	R_{270}	I	D_L	D_R	H	V
$\mathbf{R_{180}}$	R_{180}	R_{270}	I	R_{90}	H	V	D_R	D_L
$\mathbf{R_{270}}$	R_{270}	I	R_{90}	R_{180}	D_R	D_L	V	H
$\mathbf{V}$	V	D_R	H	D_L	I	R_{180}	R_{270}	R_{90}
$\mathbf{H}$	H	D_L	V	D_R	R_{180}	I	R_{90}	R_{270}
$\mathbf{D_L}$	D_L	V	D_R	H	R_{90}	R_{270}	I	R_{180}
$\mathbf{D_R}$	D_R	H	D_L	V	R_{270}	R_{90}	R_{180}	I