ANSWERS TO HOMEWORK 1

All solutions should be with proofs, you may quote from the book

(1) Decide which of the following are equivalence relations and describe the set of equivalence classes in a familiar form if it is an equivalence relation. (For example, in problem (b) below, the equivalence classes can be identified with $f(S)$, the image of f.)

(a) Let $S = \mathbb{R}^2$ and If $p, q \in S$, we say $p \sim q$ if the distance between them is less than one.

Solution. As usual, we write $\|p - q\|$ to denote the distance between p, q. Clearly, $\|p - p\| = 0 < 1$ and if $\|p - q\| < 1$, so is $\|q - p\|$. So, this relation satisfies reflexivity and symmetry. But this does not satisfy transitivity and hence not an equivalence relation. To see this one just needs a single example, so take $p = (0,0), q = (3/4, 0), r = (3/2, 0)$. Then $\|p - q\| = 3/4 = \|q - r\|$, but $\|p - r\| = 3/2 > 1$. Thus, $p \sim q, q \sim r$ but $p \not\sim r$. $\square$

(b) Let $f : S \to T$ be a mapping. For $s_1, s_2 \in S$, we say $s_1 \sim s_2$ if $f(s_1) = f(s_2)$.

Solution. For any $s \in S$, we have $f(s) = f(s)$ and thus $s \sim s$. If $s \sim t$, $f(s) = f(t)$ and thus $t \sim s$. Finally, if $s \sim t, t \sim u$, we have $f(s) = f(t)$ and $f(t) = f(u)$ and thus $f(s) = f(u)$. So $s \sim u$. So, we have checked all the three properties necessary for an equivalence relation.
The set of equivalence classes as I said earlier, can be identified with $f(S)$. (If you think about it, all equivalence relations on a set S lead to a picture like this with T the set of equivalence classes.) $\square$

(c) Let $S = \mathbb{R}$. We say for $a, b \in S$, $a \sim b$ if $a - b \in \mathbb{Z}$.

Solution. I will leave you to check that this is indeed an equivalence relation (and it is easy). I claim that the set of equivalence classes can be identified with the unit circle $S^1 \subset \mathbb{R}^2$, with center the origin and radius 1. For this, consider the map, $f : \mathbb{R} \to S^1$, $f(a) = (\cos 2\pi a, \sin 2\pi a)$. $\square$

(d) Let S be the set of non-zero complex numbers. If $a, b \in S$, $a \sim b$ if there is a positive real number r such that $a = rb$.

Solution. Again, checking this is an equivalence relation is easy. For example, $a \sim a$ since $a = 1 \cdot a$. If $a \sim b$ and thus $a = rb$ with $r > 0$, then $b = \frac{1}{r}a$ (and $\frac{1}{r} > 0$). So, $b \sim a$. Similarly, if $a \sim b, b \sim c$, we have $a = rb, b = sc$ with r, s positive. Then $a = rsc$ with $rs > 0$ and thus $a \sim c$.
Again, I claim that the set of equivalence classes can be identified with the unit circle. For this consider the map $f : S \to S^1$, given by $f(a) = \frac{a}{|a|}$. $\square$

(2) Let S be a finite set of n elements and let $\mathcal{P}(S)$ be the power set (i.e. the set of all subsets of S). Show that it is finite and has 2^n elements. (In particular, there can not be a one-to-one, onto mapping from $S \to \mathcal{P}(S)$. The last statement is also true if S is infinite. Have you seen a proof?)

Solution. We use induction on n. If $n = 1$, then S has exactly two subsets, itself and the empty set, so $\mathcal{P}(S)$ has 2 elements.

Now assume the result proved for $n - 1$ and let S be a set with n elements. We pick one element $a \in S$. We can divide the subsets of S in two groups, the ones containing a and the ones not containing a. If A is a subset containing a, then $A - \{a\} \subset S - \{a\} = T$ and given a subset of T, by adding a to it we get a subset of S containing A. So these are in one-to-one correspondence with $\mathcal{P}(T)$ and since T has $n - 1$ elements, by induction hypothesis, this collection has 2^{n-1} elements.

Next, we consider subsets not containing a. But these are precisely subsets of T and thus again there are 2^{n-1} of them. Thus the total number of elements in $\mathcal{P}(S)$ is $2^{n-1} + 2^{n-1} = 2^n$. $\square$

(3) Again, let S be a set with n elements. Construct a one-to- one correspondence $f : S \to S$ such that $f^n = \mathrm{Id}$ (composition of f, n times), but $f^m \neq \mathrm{Id}$ for $0 < m < n$.

Solution. Write $S = \{a_1, \dots, a_n\}$ and define f as, $f(a_1) = a_2, f(a_2) = a_3, \dots, f(a_{n-1} = a_n, f(a_n) = a_1$. One can check that this has all the properties. (A better way would be to index the set with elements of $\mathbb{Z}/n\mathbb{Z}$, which is J_n in the book. So, $S = \{a_{[x]} | [x] \in \mathbb{Z}/n\mathbb{Z}\}$. Then $f(a_{[x]}) = a_{[x+1]}$.) $\square$

(4) Again, let S be a set with n elements and $A(S)$, the set of all one-to-one onto maps from S to itself. Show that $A(S)$ has $n!$ elements.

Solution. Let T be another set with n elements. It suffices to show that the set of one-one-one onto maps (called *bijective* maps) from S to T has $n!$ elements. We do this by induction.

If $n = 1$, $S = \{a\}, T = \{b\}$ and then clearly there is only one such map from S to T.

So, assume proved for $n - 1$ and let S, T have n elements. Pick an $a \in S$. For any bijective f, we have $f(a) \in T$, which can be any element in T and thus has n choices. Then, f gives a bijection from $S - \{a\} \to T - \{f(b)\}$ and these are sets with $n - 1$ elements and thus there are $(n-1)!$ possibilities. Thus, the total number is $n \cdot (n-1)! = n!$. $\square$

(5) Let n, m be two positive integers. We will write $\mathbb{Z}/n\mathbb{Z}$ for J_n, used in the book, which is more standard. Let $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the map $\pi_n(a) = [a]$. Consider the map $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $f(a) = (\pi_n(a), \pi_m(a))$. Find a necessary and sufficient condition on n, m so that f is onto.

Solution. Let $\gcd(n, m) = d$. First, let us look at the case $d > 1$. Then, I claim $([1], [d])$ is not in the image. If it were, we should have $a \in \mathbb{Z}$ such that $\pi_n(a) = [1], \pi_m(a) = [d]$. The second gives, $a - d = rm$ and so $a = d + rm$. Since d divides m, we see that d divides a. But the first gives $a - 1 = sn$ and so $a - sn = 1$. But, both a, n are divisible by d which implies d divides 1, a contradiction.

Next, we look at the case $d = 1$. We will show that in this case f is onto. (This is known as Chinese Remainder Theorem.) So, let $[p] \in \mathbb{Z}/n\mathbb{Z}, [q] \in \mathbb{Z}/m\mathbb{Z}$. Since $\gcd(n, m) = 1$, we can find integers r, s such that $rn + sm = 1$. So, we get $p - q = (p-q)rn + (p-q)sm$ and thus $p - (p-q)rn = q + (p-q)sm$, which we call a and then $\pi_n(a) = [p]$ and $\pi_m(a) = [q]$. $\square$

(6) Let $\mathrm{End}(\mathbb{Z}/n\mathbb{Z})$ (End is an abbreviation for *endomorphisms*) be the set of of all maps $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ satisfying $f([a] + [b]) = f([a]) + f([b])$ for all $a, b \in \mathbb{Z}$. Calculate the number of elements (cardinality) in this set.

Solution. Let f be such an endomorphism and let $f([1]) = [x]$. Then we get $f([2]) = f([1]) + f([1]) = [x] + [x] = [2x]$ and i should be clear that similarly, for any $[p]$, $f([p]) = [xp]$. So, $[x]$ determines such a map. Conversely, given any $[x] \in \mathbb{Z}/n\mathbb{Z}$, one can define an endomorphism f by $f([p]) = [xp]$. I will leave you to check that this does indeed define an endomorphism. So, the number of such maps is exactly the number of elements in $\mathbb{Z}/n\mathbb{Z}$, which is n. $\square$