CS 280 - Homework 2
Solutions

1. Suppose that $f : A \mapsto B$ is an "onto" function, and define a relation $\sim$ on A by $a \sim a'$ iff $f(a) = f(a')$. Show that $\sim$ is an equivalence relation. If we let $C = A/\sim$ and $\eta : a \mapsto C$ by $\eta(a) = [a]$, show that there exists a bijection $g : C \mapsto B$ such that $f = g \circ \eta$.

□ To show that a relation is an equivalence relation, we must show that it is a) reflexive, b) symmetric, and c) transitive.

a) Show that $a \sim a$. To do this, we must show that $f(a) = f(a)$. This is true, since equality is reflexive.

b) Show that $a \sim b \Rightarrow b \sim a$. Given that $f(a) = f(b)$, we must show that $f(b) = f(a)$. This is true, since equality is symmetric.

c) Show that $a \sim b \wedge b \sim c \Rightarrow a \sim c$. Given that $f(a) = f(b)$ and that $f(b) = f(c)$, we can conclude that $f(a) = f(c)$, since equality is transitive.

We now show that g exists and is bijective. Let $g([a]) = f(a)$.

Show that g is well-defined. Note that if $f(a) = b$, then for any a' such that $\eta(a') = [a]$, $f(a') = b$. So, for any a' such that $[a'] = [a]$, $f(a') = f(a)$, and thus $g([a']) = f(a') = f(a) = g([a])$. So, g is well-defined.

Show that g is one-to-one. If we have $g([a]) = g([a'])$, then by definition $f(a) = f(a')$. But this means that $a \sim a'$, so $[a] = [a']$, and g is one-to-one.

Show that g is onto. Since f is onto, we know that for all $b \in B$, there exists $a \in A$ such that $f(a) = b$. Also, since η is a function, for any a, there exists $\eta(a) = [a]$. So, for any b, and given that $f(a) = b$, take $g([a]) = f(a) = b$. Thus for any b, there exists $[a]$ such that $g([a]) = b$, and g is onto. So, g is a bijection and $f = q \circ \eta$. ■

For this question, many people claimed that $f(a) = f(a)$ because f is a function. This does not make much sense; if f were not a function, we could not talk about $f(a)$. The reason that $f(a) = f(a)$ is that equality is an equivalence relation, and thus is reflexive. Also, many people did not prove that g was onto and one-to-one, instead just giving an intuitive argument. While this was accepted, a more formal argument is preferred.

2. Prove that $(1+a)^p \equiv (1+a^p) \bmod p$ if p is prime and a is an integer, $0 \leq a < p$.

□ $(1+a)^p \equiv (1+a^p) \bmod p$ is equivalent to $p \big| (1+a)^p - (1+a^p)$. We now use the binomial theorem to expand the right side:

$$\begin{aligned}(1+a)^p - (1+a^p) &= \left(\sum_{k=0}^{p} \binom{p}{k} a^k\right) - (1+a^p) \\ &= \left(\sum_{k=1}^{p-1} \binom{p}{k} a^k\right) \\ &= \left(\sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} a^k\right) = \sum_{k=1}^{p-1} x_k\end{aligned}$$

Now, if $p \big| x_k$, then $p \big| \sum_{k=1}^{p-1} x_k$. To show that $p \big| x_k$, we use the fact that p is prime. The largest factor in the denominator of x_k will be $(p-k)$ or k, whichever is larger, and since p is prime, there is no way to compose p from smaller factors. Thus, whenever $0 < k < p$, $x_k = \frac{p!}{(p-k)!k!}$ is divisible by p. Thus, since $p \big| x_k$, $p \big| \sum_{k=1}^{p-1} x_k$. Since this is what we sought to prove, we have shown that $(1+a)^p \equiv (1+a^p) \bmod p$. ■

Note that if p is not prime, this proof does not work. Since it is possible for numbers less than p to multiply to p, there is no guarantee that p will not divide $(p-k)!k!$. If it does, then $\frac{p!}{(p-k)!k!}$ may not be divisible by p, and thus the proof is invalid. Note that $(1+1)^4 = 16 \equiv 0 \bmod 4$, while $(1+1^4) = 2 \equiv 2 \bmod 4$. Thus the statement is not true when p is not prime.

The most common problem was that students neglected to show that the statement was false for p non-prime. Also, a few students relied on Fermat's Theorem, which states $a^p \equiv a \bmod p$ for p prime. On this assignment, since some consultants had suggested that this theorem be used, no credit was lost if it was correctly applied. In general, though, you should not rely on external results unless you can prove them yourself.

3. How many binary operations are there on a set A with n elements? List all of them for the set $\{a, b\}$ and indicate which are commutative, associative, have identity elements, and have zero divisors.

□ A binary operation on a set takes two elements and returns one; let our generic operation be $* : A \times A \mapsto A$. Since in general, the number of functions from $X \mapsto Y$ is $|\,Y|^{|X|}$, and since $|\,A \times A| = |\,A|^2$, the total number of binary operations on a set of size n is $n^{(n^2)}$. We represent the possible binary operations in a table; each column corresponds to one possible operation:

		I					I	I		I						
	C	C					C	C	C	C					C	C
a * a =	a	a	a	a	a	a	a	a	b	b	b	b	b	b	b	b
a * b =	a	a	a	a	b	b	b	b	a	a	a	a	b	b	b	b
b * a =	a	a	b	b	a	a	b	b	a	a	b	b	a	a	b	b
b * b =	a	b	a	b	a	b	a	b	a	b	a	b	a	b	a	b
	A	A		A		A	A	A		A						A
	Z															Z

Columns marked with C correspond to commutative operations; those marked with A correspond to associative operations; those marked with I correspond to those with identity elements, and those marked with Z to those with zero divisors. From this, we see that there are 8 commutative operations, 8 associative operations, 4 operations with identity elements, and 2 operations with zero divisors. ■

Definitions: Given an operation $*$, it:

– is commutative if: for all x, y, $x * y = y * x$.
– is associative if: for all x, y, z, $x * (y * z) = (x * y) * z$.
– has an identity element if: there exists e such that for all x, $e * x = x * e = x$.
– has a zero divisor if: there exists an annihilator a (for all x, $a * x = x * a = a$) and there exist b, c such that $b * c = a$.

One common problem was trying to relate this problem to the binary operators you know, or even just listing some binary operators. (These included +, ×, ∪, ∩, ∧, ∨, and others) This is totally incorrect, and resulted in no credit being given. Binary operators can be defined on any set, and although we happen to be familiar with many of them over integers, sets, logical propositions, and other domains, the definition of a binary operator f over a set X is just a function $f : X \times X \mapsto X$. Be careful in general of applying a familiar concept to an unfamiliar problem.

Also, many people wrote that the number of operations was $(n^2)^n = n^{2n}$. This is incorrect, but since this answer was given to some people in consulting, no points were deducted if it was given.

4. Let G be a group (written multiplicatively) and A a non-empty set. We say that G "acts on" A if there is a function $f : G \times A \mapsto A$ (where we write $f(g, a) = g.a$) satisfying:

(a) $g.(h.a) = (gh).a \qquad \forall\, g, h \in G, a \in A$
(b) $1.a = a \qquad \forall\, a \in A$
Prove that:

`i)` Given $g \in G$, the function $p_g : A \mapsto A$ given by $p_g(a) = g.a$ is a bijection.

□ Show that p_g has an inverse. Let us guess that $p_{g^{-1}}$ is its inverse. Check:

$$\begin{aligned} p_{g^{-1}}\big(p_g(a)\big) &= p_{g^{-1}}\big(g.a\big) && \text{[by def. of } p_g\text{]} \\ &= g^{-1}.(g.a) && \text{[by def. of } p_{q^{-1}}\text{]} \\ &= (g^{-1}g).a && \text{[by (a)]} \\ &= 1.a && \text{[by } A4\text{]} \\ &= a && \text{[by (b)]} \end{aligned}$$

Thus, since p_g has an inverse, it is a bijection. ■ Common problems:

$p_g : A \mapsto A$ does not imply that p_g is an identity function.

The notation $p_g : A \mapsto A$ just signifies that p_g is a function that maps from a domain A back to the range A. It does not mean that p_g is an identity function. For example, $f : \mathbb{Z} \mapsto \mathbb{Z}, f(n) = n+1$ clearly maps from the integers to the integers, and just as clearly it is not the identity function.

The fact that p_g is one-to-one and maps from A to A does not imply onto.

Just because you have proved that a function is one-to-one and maps from set $X \mapsto X$ does not prove that it is onto. For example, the function $f : \mathbb{Z} \mapsto \mathbb{Z}, f(n) = 2n$ is one-to-one and maps from $\mathbb{Z} \mapsto \mathbb{Z}$, but it is not onto.

The fact that p_g is onto and maps from A to A does not imply 1-1.

Just because you have proved that a function is onto and maps from set $X \mapsto X$ does not prove that it is one-to-one. For example, the function $f : \mathbb{Z} \mapsto \mathbb{Z}, f(n) = \lfloor n/2 \rfloor$ is onto and maps from $\mathbb{Z} \mapsto \mathbb{Z}$, but it is not one-to-one. Both these confusions arise from the fact that A can be infinite. For a finite set X, if $f : X \mapsto X$, then f is onto if and only if f is one-to-one. This is not true for infinite sets, as shown.

p_g determines g, so you cannot choose $g = 1$.

For any given p_g, g is fixed. It is one specific element of the group, and you cannot make any assumptions about it. In particular, you cannot assume that $g = 1$.

`ii)` The relation on A given by $a \sim b$ iff $\exists\, g \in G$ s.t. $g.a = b$ is an equivalence relation.

□ To show that a relation is an equivalence relation, we must show that it is a) reflexive, b) symmetric, and c) transitive.

a) Show that $a \sim a$. To show $a \sim a$, we must show that $\exists\, g \in G$ s.t. $g.a = a$. So let $g = 1$, and $1.a = a$ by (b). Thus the relation is reflexive.

b) Show that $a \sim b \Rightarrow b \sim a$. If $a \sim b$, then $\exists\, g \in G$ s.t. $g.a = b$. Consider $g^{-1}.b$. Substituting, we get:

$$\begin{aligned} g^{-1}.b &= g^{-1}.(g.a) && \text{[assumed]} \\ &= (g^{-1}g).a && \text{[by (a)]} \\ &= 1.a && \text{[by A4]} \\ &= a && \text{[by (b)]} \end{aligned}$$

Thus, given that $\exists\, g \in G$ s.t. $g.a = b$, we can show that $\exists\, h = g^{-1} \in G$ s.t. $h.b = a$. Thus the relation is symmetric.

c) Show that $a \sim b \wedge b \sim c \Rightarrow a \sim c$. If $a \sim b \wedge b \sim c$, then $\exists\, g, h \in G$ s.t. $g.a = b$ and $h.b = c$. Substituting:

$$\begin{aligned} c &= h.b && \text{[assumed]} \\ &= h.(g.a) && \text{[assumed]} \\ &= (hg).a && \text{[by (a)]} \end{aligned}$$

Thus, given that $\exists\, g, h \in G$ s.t. $g.a = b$ and $h.b = c$, we can show that $\exists\, i = (hg) \in G$ s.t. $i.a = c$. Thus the relation is transitive, and thus it is an equivalence relation. ■ Common problems:

When g is determined, you cannot choose $g = 1$.

If some quality already determines g, (for example, that $g.a = b$) you cannot say anything about g. In particular, you cannot choose $g = 1$. This means that when showing symmetricity and transitivity, you cannot use $g = 1$. Note that to show reflexivity, you can (and must) let $g = 1$, but this is allowable, since we are trying to *find* g.

g **and** h **can be different.** In showing symmetricity, we have that $a \sim b \Rightarrow b \sim a$ is equivalent to saying that $g.a = b \Rightarrow h.b = a$. Note that g and h can and will be different. Many people said that $g.a = b \Rightarrow g.b = a$, and from this somehow concluded that g was 1. This is incorrect — the statement itself is wrong, and it does not even imply that $g = 1$. Similarly, when proving transitivity, we seek to show that $g.a = b \wedge h.b = c \Rightarrow i.a = c$. All of g, h, and i will be different, and you need to prove that i exists in terms of g and h.

`iii)` NOTE: This problem was very difficult; no totally correct solutions were turned in. This proof is one way of showing the desired fact, but you were not expected to come up with it.

□ We define two concepts:

$aG = \{g.a \,|\, g \in G\}$ is called the orbit of a on G.

$G_a = \{g \,|\, g \in G, g.a = a\}$, a subgroup of G, is called the *isotropy group* or *stabilizer* of a.

If we define equivalence according to the relation above, we see that $[a] = \{g.a \,|\, g \in G\}$, which is aG, the orbit of a. We now show that there exists a bijection $\beta : G_a \backslash G \mapsto aG$, where $G_a \backslash G$ denotes $\{G_a x \,|\, x \in G\}$, the set of right cosets of G_a. (Here $G_a x = \{gx \,|\, g \in G_a\}$.) We assert that $\beta : G_a x \mapsto x.a$ is a bijection. We first need to check that this is well defined, so assume we have two definitions of the coset: $G_a x = G_a y$ for $x, y \in G$. Thus $G_a y^{-1} x = G_a$, $y^{-1}x \in G_a$, and $(y^{-1}x).a = a$:

$$\begin{aligned} (y^{-1}x).a &= a \\ y.\big((y^{-1}x).a\big) &= y.a \\ (yy^{-1}x).a &= y.a \\ x.a &= y.a \end{aligned}$$

Thus β is well defined. Now define $\gamma : aG \mapsto G_a \backslash G$ as $a.x \mapsto G_a x$. Again, we need to show that γ is well defined. Suppose that $x.a = y.a$ for $x, y \in G$.

$$\begin{aligned} x.a &= y.a \\ y^{-1}(x.a) &= y^{-1}(y.a) \\ (y^{-1}x).a &= (y^{-1}y).a \\ (y^{-1}x).a &= a \end{aligned}$$

Thus $y^{-1}x \in G_a$, thus $G_a x = G_a y$ and γ is well defined. Since β and γ are mutually inverse, they are both bijections, so we have proved that β is a bijection.

The cardinality of $G_a \backslash G$ is denoted $|\, G : G_a|$; when G is finite this is $\frac{|\,G|}{|\,G_a|}$. Since there exists a bijection from $G_a \backslash G$ to aG, they must have the same cardinality, and thus the cardinality of the orbit of a over a finite group G is $\frac{|\,G|}{|\,G_a|}$. The orbit of A is just $[a]$, and thus $|\,[a]| = \frac{|\,G|}{|\,G_a|}$. ■

Common problems:

$g.a = a$ does not mean that $g = 1$.

The fact that g fixes a (that is, that $g.a = a$) does not imply that g is an identity element. It says nothing about the behavior of g in general; for example, we could have $g.b = c$.

It is meaningless to talk about $[1]$ or $[g]$.

It doesn't make sense to talk about $[1]$ or $[g]$. $\mathbf{1}$ is an element of the group G, and $\sim$ is a relation defined on A. Thus, only elements of A can have equivalence classes. This is why we can talk about $[a]$, but not $[g]$.

5. Note on permutations: From the homeworks, it is clear that many people do not have a clear grasp on what a permutation is. This makes it difficult to prove anything about permutations. A permutation is not a list of elements; it is a function. The formal definition of a permuation σ over a set X is just a bijection $\sigma : X \mapsto X$. We can write this in two-row notation, with the members of X in the first row, and what they are mapped to below them:

$$\sigma : \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \sigma(x_3) & \cdots & \sigma(x_n) \end{pmatrix}$$

In this notation, it is easy to compose two permutations. Simply write the last permutation, and then the first permutation below it — but arrange the columns of the second permutation so it matches with the one above it:

$$\sigma : \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \sigma(x_3) & \cdots & \sigma(x_n) \end{pmatrix} \qquad \pi : \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ \pi(x_1) & \pi(x_2) & \pi(x_3) & \cdots & \pi(x_n) \end{pmatrix}$$

$$\sigma\pi : \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \pi(x_1) & \pi(x_2) & & \pi(x_n) \end{pmatrix} \begin{pmatrix} \pi(x_1) & \pi(x_2) & \cdots & \pi(x_n) \\ \sigma\big(\pi(x_1)\big) & \sigma\big(\pi(x_2)\big) & & \sigma\big(\pi(x_n)\big) \end{pmatrix}$$

$$= \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \sigma\big(\pi(x_1)\big) & \sigma\big(\pi(x_2)\big) & & \sigma\big(\pi(x_n)\big) \end{pmatrix}$$

To write a cycle in this form, just write, below each number, the number after it in the cycle:

$$(x_1 \; x_2 \; x_3 \; \cdots \; x_n) = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_2 & x_3 & x_4 & \cdots & x_1 \end{pmatrix}$$

Some people who came to consulting were told that permutations acted on the position, rather than the elements. This is incorrect. Unfortunately, it is self-consistent — if you interpret things in the wrong way every time, your answers will still make sense. For the same reason, it is very dangerous to think about permutations as lists of elements, or rearrangements thereof. To be safe, always think of permutations as functions.

Show that every permutation of X can be written as a composition of disjoint cycles, that every permutation can be written as a composition of transpositions, and that if p in $S(X)$ can be written using an even number of transpositions, then it cannot be written using an odd number of transpositions, and vice versa.

`i)` For this question, an algorithm was sufficient. □ Take the smallest number in X; call it x. Under the permutation $\sigma \in S(X)$, $\sigma(x) = x', \sigma^2(x) = \sigma(x') = x'', \ldots$. Since $|X| = n$, we know that there exists some number p $(0 < p \leq n)$ such that $\sigma^p(x) = x^{(p)} = x$.Thus we can construct a cycle by $\big(x \quad x' \quad x'' \quad \ldots \quad x^{(p-1)}\big)$. Now, if $p = n$, then the above cycle is σ, and we are done. If $p < n$, choose the smallest element of X that does not yet appear in a cycle, and repeat the above argument. The resulting cycle must be disjoint from all others, because since σ is a bijection, for any b there can only be one unique a such that $\sigma(a) = b$. If b appeared in two cycles, it would be the image of two different numbers, and thus σ would not be one-to-one. Now simply repeat the above method until all elements of X have been paritioned into cycles. Take their composition, and by the definition of cycles, we have σ again. Thus any permutation can be written as the composition of disjoint cycles. ■

A few people claimed that since their solution to part `ii` proved that any permutation could be written as a composition of transpositions, their solution to `ii` also solved `i`. This is not true; in general, the transpositions from part `ii` will not be disjoint, and `i` specifically requires that the permutation be composed of *disjoint* cycles.

`ii)` □ By part `i`, any permutation can be written as the composition of disjoint cycles. Thus it suffices to show that any cycle C can be written as the composition of transpositions. Proof by induction on the length of C. $P(n)$: we can represent any cycle of length n as the composition of transpositions.

Base case: when the length of C is 1, it is of the form (x_i). This is the identity, and thus can be represented as the composition of 0 transpositions. So $P(1)$ is true.

Inductive step: Assume $P(n-1)$ — a cycle of length $n-1$ can be written as the composition of transpositions. Note that $\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \end{pmatrix} = \begin{pmatrix} x_1 & x_n \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_{n-1} \end{pmatrix}$. If C is of length n, then by our inductive hypothesis, $\begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_{n-1} \end{pmatrix}$ can be written as a composition of transpositions. Let the corresponding sequence of transpositions be $t_k \cdots t_3 t_2 t_1$. Substituting in this sequence of transpositions, we have that $\begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_n \end{pmatrix} = \begin{pmatrix} c_1 & c_n \end{pmatrix} t_k \cdots t_3 t_2 t_1$. But this is itself a composition of transpositions, and thus $P(n-1) \Rightarrow P(n)$. Thus, since $P(1)$ is also true, $P(n)$ is true for all $n > 0$, and so any cycle can be written as the composition of transpositions.

Since any permutation can be written as the composition of cycles, by `i`, and any cycle can be written as the composition of transpositions, any permutation can be written as the composition of transpositions. ■ The sequence that results from applying the above algorithm will be $\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \end{pmatrix} = \begin{pmatrix} x_1 & x_n \end{pmatrix} \cdots \begin{pmatrix} x_1 & x_3 \end{pmatrix} \begin{pmatrix} x_1 & x_2 \end{pmatrix}$, but this is actually irrelevant to our proof.

`iii)` Let any transposition be even if it can be written as the composition of an even number of transpositions, and odd if it can be written as the composition of an odd number of transpositions. We seek to prove that no permutation can be both odd and even.

Lemma: e, the identity, is even and not odd. Note that $e = (x_j x_k)(x_k x_j)$ and thus is even. Let us show that e cannot be odd. Let $e = t_1 t_2 \cdots t_k$, where each t is a transposition and k is the number of transpositions. Choose m that occurs somewhere in some t_n, let t_i be the first t (from the right) that contains m, and let t_i be (mx). Notice that $i \neq 1$, because if it did, then t_1 would be the only t that contained m. But then $e(m) = t_1(m) = x$ — but $e(m)$ has to be m, since e is the identity. Thus we can consider $t_{i-1} t_i$. There are four cases:

(i) $t_{i-1} t_i = (mx)(mx) = e$
(ii) $t_{i-1} t_i = (my)(mx) = (mx)(xy)$
(iii) $t_{i-1} t_i = (xy)(mx) = (my)(xy)$
(iv) $t_{i-1} t_i = (yz)(mx) = (mx)(yz)$

Notice that in the alternate expressions for $(ii) - (iv)$, the transposition containing m is one place further to the left. So we replace $t_{i-1} t_i$ with the corresponding expression above. Now either k, the total number of transpositions, is decreased by 2, or the first t containing m is moved one place to the left. But remember that we showed that the first occurence of m cannot be in the first term. Thus eventually m must be eliminated and k reduced by an even number. Repeat this procedure for every number that occurs in $t_1 t_2 \cdots t_k$. Eventually, we have $e = e \cdot e \cdot e \cdots e$. Since the number of transpositions is now 0, and we have reduced it by an even number every time, it follows that k must be even. Thus e is even and cannot be odd.

We now use this result to show that a permutation cannot be both even and odd. Let a permutation σ be represented by two sequences of transpositions, $t_1 t_2 \cdots t_j$ and $u_1 u_2 \cdots u_k$. We can write $t_1 t_2 \cdots t_j = u_1 u_2 \cdots u_k$. But this means that $e = u_1 u_2 \cdots u_k t_j^{-1} \cdots t_2^{-1} t_1^{-1}$. By our lemma, we know that e can only be represented as an even number of transpositions, and thus $j + k$ is even. But this means that either j and k are both even or both odd, and thus σ is either even or odd, but not both. ■

Note that showing that the minimum number of transpositions is even or odd does not prove anything. Every integer is even or odd; I can tell you with certainty that the number of red-headed students at Cornell is even or odd — and not both. Remember that while there is a smallest number of transpositions that a given permutation can be composed of, the number of transpositions in any given decomposition can be as large as you like.

Also, any arguments that relied on the fact that once you have a decomposition, any transposition has to be "undone" were incomplete. For example, saying that from part `ii` a decomposition existed, and it was impossible to add a transposition without "messing it up" was not correct. You need to consider the case that a decomposition has nothing in common with the one that you have already found. Remember that if you think about problems in a specific case, you still need to generalize your answers.