Math 322
Assignment #1
Nicholas Rees
11848363

1. Let X be the complement of the origin $(0,0)$ in $\mathbb{R}^2$. Define a relation on X by saying points $p, q \in X$ satisfy $p \sim q$ if and only if the line passing through p, q also passes through the origin. Show that $\sim$ is an equivalence relation, and describe the quotient set $X/\sim$.
   We check that the relation satisfies the three conditions for an equivalence relation. By the Canvas page, we can assume $p \sim p$. For $p \sim q$ implies $q \sim p$, note that fixing two points on $\mathbb{R}^n$ uniquely fixes a line that passes through them. Thus, if $p \sim q$, the unique line that passes through p and q also passes through the origin, and so the line passing through q and p is the same line that also passes through the origin, and thus $q \sim p$. Finally we show transitivity. Let $p \sim q$ and $q \sim s$ (where $s \in X$). We know that two points that lie on the same line that passes through the origin are scalar multiples of each other. So we have that $p = aq$ and $q = bs$ where $a, b \in \mathbb{R}$. But then $p = abs$, and so p and s are scalar multiples of each other, and as we just said, this means p and s are on the same line that passes through an origin. Thus, $p \sim s$.

   Each equivalence class corresponds to a different line through the origin, so the quotient set $X/\sim$ is just the set of all lines through the origin.

2. Let $\mathbb{C}^*$ denote the set of nonzero complex numbers. Describe the set $\mathbb{C}^*/\sim$, where $\sim$ is the relation $a \sim b$ if and only if $a/|a| = b/|b|$. How is this quotient set related to the quotient set in Problem 1?
   By dividing a, b by their magnitude, the $\sim$ only cares about the argument of the complex number. $a \sim b$ if and only if $\arg(a) = \arg(b)$. Thus, each equivalence class corresponds to a different argument. Visualizing $\mathbb{C}$ as $\mathbb{R}^2$, each equivalence class is the set of points along the line that extends from 0 and makes an angle equal to the argument with the positive real line. The quotient set $\mathbb{C}^*/\sim$ looks similar then to the quotient set from question 1., however now the rays of the lines on either side of the origin are different equivalence classes, rather than the same one.

3. How many distinct binary relations are there on a set of n elements? How many of these are equivalence relations? (For the second part, a recursive formula is an acceptable answer.)
   We claim there are 2^{n^2} distinct binary relations on a set of n elements, S_n. Note that a binary relation $\sim$ is an element of of the power set of $S_n \times S_n$, $\mathcal{P}(S_n \times S_n)$. The number of binary relations is just the cardinality of this set. We know that the cardinality of the power set of a set with cardinality $k \in \mathbb{N}$ is 2^k. But there are just n^2 elements in $S_n \times S_n$, and so we recover that there are 2^{n^2} distinct binary relations on S_n.

   We know consider how many binary relations in S_n are equivalence relations. Recall that an equivalence relation on a set corresponds to a unique partition of a set, and any partition of that seet corresponds to a unique equivalence relation (via Jacobson). Thus, we can resort to considering how many distinct partionings there are of S_n. Consider the base case $S_0 = \emptyset$. There is only one way to partition this set, namely the empty set. Let's call this $P_0 = 1$. Now, consider the arbitrary case, S_n, and assume that $P_0, \ldots, P_{n-1}$ are given as the number of ways to partition the sets $S_0, \ldots, S_{n-1}$. To form a partition of S_n, fix some element in $s \in S_n$. Consider creating an initial equivalence class with with s with k other elements in it, where $0 \leq k \leq n-1$. There are $\binom{n-1}{k}$ ways to choose these elements. We also have P_{n-1-k} ways to partition the remaining $n-1-k$ elements (where we are given P_{n-1-k} from our assumption). Thus there are $\binom{n-1}{k} P_{n-1-k}$ ways to partion n elements when s is in an equivalence class of size $k+1$. k can take on any value from 0 to $n-1$, thus we can add up all of the possible partitions for all k, which gives the recursive formula for P_n:
   $$P_n = \sum_{k=0}^{n-1} \binom{n-1}{k} P_{n-1-k}$$

4. Show that if p is a prime number and a, b are integers such that $p \mid ab$ then $p \mid a$ or $p \mid b$.
   We know that the gcd of integers a, b can be written as $\gcd(a,b) = ma + nb$ where $m, n \in \mathbb{Z}$ (bottom of page 23 in Jacobonson). Note that this implies that if $p \nmid c$ where $n \in \mathbb{Z}$ and p is prime, then there exists $m, n \in \mathbb{Z}$ such that $pm + cn = 1$, since p's only factors are 1 and itself and so $p \nmid n$ implies that $gcd(p, n) = 1$.

   Returning to the statement we are trying to prove, we either have $p \mid a$ or $p \nmid a$. If it is the first case, we are done. If it is the second, we know that there exists $m, n \in \mathbb{Z}$ such that $pm + an = 1$ from above. Multiplying both sides of the equation by b, we get
   $$pmb + anb = b$$

$$mb + \frac{ab}{p}n = \frac{b}{p}$$

But $mb \in \mathbb{Z}$ since they are both integers, and $\frac{ab}{p}n \in \mathbb{Z}$ since $p \mid ab$ and $\in \mathbb{Z}$. Thus the LHS is an integer, so the RHS is an integer, and so $p \mid b$. So in either case, $p \mid a$ or $p \mid b$.

5. Show that if n, k are positive integers, and n is not a perfect k-th power, then $n^{1/k}$ is irrational.
We prove the contrapositive. Assume n, k are positive integers, and $n^{1/k}$ is rational. That is, there exists $a, b \in \mathbb{Z}$ such that $n^{1/k} = a/b$. Taking the k-th power of both sides, we get $n = (a/b)^k = a^k/b^k$. So $nb^k = a^k$, but we assume $n \in \mathbb{Z}^+$, thus $b^k \mid a^k$. We can write a^k and b^k as their unique prime factorization decomposition (since taking a k-power of an integer is also an integer when $k \in \mathbb{Z}^+$), $b^k = p_1^{ke_1} p_2^{ke_2} \ldots p_m^{ke_m}$ and $a^k = p_1^{kf_1} p_2^{kf_2} \cdots p_m^{kf_m} p_{m+1}^{kf_{m+1}} \cdots p_d^{kf_d}$ where $d \geq n$ and $f_i k \geq e_i k$ for $1 \leq i \leq n$ since $b^k \mid a^k$. But we can just divide k out in the second inequality, so $f_i \geq e_i$ for all $1 \leq i \leq n$. But then, since $b = p_1^{e_1} \cdots p_n^{e_n}$ and $a = p_1^{f_1} \cdots p_d^{f_d}$, we get that $b \mid a$. Thus, $a/b \in \mathbb{Z}$, and so n is a perfect k-power, as desired.

6. Show that if $\alpha \colon S \to T$ and $\beta \colon T \to U$, then $(\beta\alpha)^{-1}(U_1) = \alpha^{-1}(\beta^{-1}(U_1))$, for any $U_1 \subset U$.
Given $u \in U_1$, let $t \in T$ such that $\beta^{-1}(u) = t$ and let $s \in S$ such that $\alpha^{-1}(t) = \alpha^{-1}(\beta^{-1}(u)) = s$. (which we can presumebly assume they exist, or the expression is undefined). Note then, that $\alpha(s) = t$ by the definition of an inverse, and $\beta(t) = \beta(\alpha(s)) = (\beta\alpha)(s) = u$. But by the definition of an inverse, this is the same as saying $(\beta\alpha)^{-1}(u) = s$. Thus, both the right-hand side and left-hand side of the equation are both equal to s, and since $u \in U_1$ was arbitrary, we are done.