S18 MA 274: Exam 3 Study Questions - Partial Solutions

(1) Know the definitions on the website. Any other definitions that you need will be given to you.

(2) When you write a proof, focus on getting the organization clear and correct. If you have to skip some steps or make an assumption that you don't know how to prove, clearly state that that is what you are doing.

(3) Know the theorems we've proved in class and the more significant theorems from the homework.

(4) Don't try to memorize proofs. Instead remember the structure of the proof (proof by contradiction, proof of uniqueness, element argument, etc.) and two or three key steps of the proof. Then at the exam recreate the proof.

(5) At the exam, leave time to write up a nicely written version of each proof. You should have enough time to sketch your ideas out on scratch paper before writing a final version of the proof.

(6) Study the previous study guides and exams as well as your homework, class notes, and the sections of the text we covered.

Prove the following:

(1) The number $\sqrt{2}$ is irrational.

Proof. We assume that a natural number is a multiple number is a multiple of two if and only if its square is. We also assume that every rational can be written in lowest terms.

Suppose, for a contradiction, that $\sqrt{2}$ is rational. Thus, by definition, there exist $a, b \in \mathbb{Z}$ such that $\sqrt{2} = a/b$. By our assumption we may assume that a and b have no common factor other that ± 1. Thus,

$$b\sqrt{2} = a.$$

Squaring both sides:

$$2b^2 = a^2.$$

Thus a^2 is a multiple of 2. B our assumption, this means that a is a multiple of 2. Thus, $a = 2k$ for some integer k. Consequently,

$$2b^2 = 4k^2.$$

Dividing by 2:

$$b^2 = 2k^2.$$

Hence, b^2 is a multiple of 2 and so, by our assumption, b is as well. This contradicts our assumption that a and b have no common factor other than ± 1. Thus, $\sqrt{2}$ is irrational. □

(2) There are infinitely many prime numbers.

Here's a proof which is slightly different from the one we saw before.

Proof. Suppose, for a contradiction, that there are only finitely many prime numbers. Call them:

$$p_1, p_2, \ldots, p_n.$$

Observe that $N = p_1 p_2 \cdots p_n$ is a multiple of every prime. Consider $N+1$ and suppose it is a multiple of a prime. By changing our numbering of the primes we may, without loss of generality, assume that the prime is p_n.

$$N + 1 = p_n \ell$$

for some positive integer ℓ. Subtracting N from $N+1$ we have:

$$1 = p_1 p_2 \cdots p_{n-1}(\ell - 1).$$

But 1 is a multiple only of itself and -1. Thus, being positive, we have each $p_i = 1$ for all $i \in \{1, \dots, n-1\}$. But, by definition, 1 is not a prime. Thus, $n = 1$ and there is only one prime number p_1. However, both 2 and 3 are prime numbers, so we have a contradiction. □

(3) There is no set U such that $A \in U$ if and only if A is a set. (Russell's Paradox)

Here are two proofs.

Proof. To establish a contradiction, suppose there is such a set U. Let $R = \{A \in U : A \notin A\}$. R is a set by the axiom of subset selection. Either $R \in R$ or $R \notin R$. If $R \in R$, then R fulfills its own entrance criterion and so $R \notin R$, a contradiction. If $R \notin R$ then, again, R fulfills its own entrance criterion and so $R \in R$, another contradiction. Thus, U cannot be a set. □

Proof. To establish a contradiction, suppose there is such a set U. By the axiom of power sets, $\mathcal{P}(U)$ is a set. Every element of $\mathcal{P}(U)$ is a set and so is also an element of U. Thus, $\mathcal{P}(U) \subset U$. In particular, $\operatorname{card} \mathcal{P}(U) \leq \operatorname{card} U$. However, this contradicts our previously proved fact that $\operatorname{card} U < \operatorname{card} \mathcal{P}(U)$. □

(4) The Halting Problem

(5) DeMorgan's Laws

(6) Suppose G is a group with operation $\circ$ and that $a \in G$. If $f, g \in G$ have the properties that $f \circ a = a \circ f = a$ and $g \circ a = a \circ g = a$, then $f = g$. (That is, the identity in a group is unique.)

Proof. Since $f \circ a = a$ and $g \circ a = a$, we have

$$f \circ a = g \circ a.$$

By the inverse axiom for groups, there exists an element $a^{-1} \in G$ such that

$$a \circ a^{-1} = \mathbf{1},$$

where $\mathbf{1}$ is the identity in the group.

By the closure axiom for groups,

$$(f \circ a) \circ a^{-1} = (g \circ a) \circ a^{-1}.$$

By associativity,

$$f \circ (a \circ a^{-1}) = g \circ (a \circ a^{-1}).$$

By the properties of a^{-1},

$$f \circ \mathbf{1} = g \circ \mathbf{1}.$$

By the properties of the identity,

$$f = g.$$

□

(7) Suppose that G is a graph and that a, b, and c are vertices. Then if there is a path from a to b and a path from b to c, then there is a path from a to c.

Proof. Let $v_0, v_1, \dots, v_n$ be a path from a to b. This means that $v_0 = a$, $v_n = b$, and for each i, the vertices v_i and v_{i+1} are the endpoints of an edge in G. Similarly, let $w_0, w_1, \dots, w_m$ be a path from b to c. This means that $w_0 = b$, $w_m = c$, and for each i, the vertices w_i and w_{i+1} are the endpoints of an edge in G.

Consider the sequence:

$$v_0, v_1, \dots, v_n, w_1, w_2, \dots, w_m.$$

Observe that $v_0 = a$ and $w_m = c$. Also, for each i, v_i and v_{i+1} are the endpoints of an edge in G and for each j, w_j and w_{j+1} are the endpoints of an edge in G. Finally, since $v_n = w_0$, the vertices v_n and w_1 are the endpoints of an edge in G, since w_0 and w_1 are. Thus, we have a path in G from a to c. □

(8) The intersection of subgroups is a subgroup

(9) The intersection of convex sets is convex

(10) The intersection of event spaces is an event space.

Proof. We refer to the textbook for the definition of event space. Suppose that $\mathbb{E}$ is a non-empty set such that each $\mathcal{E} \in \mathbb{E}$ is an event space on a set X. We will show that $\bigcap\limits_{\mathcal{E}\in\mathbb{E}} \mathcal{E}$ is an event space on X.

Since each $\mathcal{E} \in \mathbb{E}$ is an event space, by definition, $\varnothing \in \mathcal{E}$ for all $\mathcal{E} \in \mathbb{E}$. Thus, $\varnothing \in \bigcap\limits_{\mathcal{E}\in\mathbb{E}} \mathcal{E}$, by definition of intersection.

Now suppose that $A \in \bigcap\limits_{\mathcal{E}\in\mathbb{E}} \mathcal{E}$. By definition of intersection, $A \in \mathcal{E}$ for all $\mathcal{E} \in \mathbb{E}$. Since each $\mathcal{E}$ is an event space, $A^C \in \mathcal{E}$ for all $\mathcal{E} \in \mathbb{E}$. Hence, $A^C \in \bigcap\limits_{\mathcal{E}\in\mathbb{E}} \mathcal{E}$.

Finally, suppose that for each $n \in \mathbb{N}$, $A_n \in \bigcap\limits_{\mathcal{E}\in\mathbb{E}} \mathcal{E}$. Then, for each $n \in \mathbb{N}$, $A_n \in \mathcal{E}$ for all $\mathcal{E} \in \mathbb{E}$. Thus, for all $\mathcal{E} \in \mathbb{E}$ and for all $n \in \mathbb{N}$, $A_n \in \mathcal{E}$. Since each $\mathcal{E}$ is an event space,

$$\bigcup_{n\in\mathbb{N}} A_n \in \mathcal{E}$$

for all $\mathcal{E} \in \mathbb{E}$. Consequently,

$$\bigcup_{n\in\mathbb{N}} A_n \in \bigcap_{\mathcal{E}\in\mathbb{E}} \mathcal{E}.$$

Since $\bigcap\limits_{\mathcal{E}\in\mathbb{E}} \mathcal{E}$ satisfies the axioms for an event space, it is one! □

(11) $X \times Y = Y \times X$ if and only if either $X = Y$ or one of X or Y is empty.

(12) If (x_n) is a sequence in a set X such that $\operatorname{range}(x_n)$ is infinite, then (x_n) has a subsequence (x_{n_k}) which is injective and such that $\operatorname{range}(x_{n_k}) = \operatorname{range}(x_n)$.

Proof. Assume that (x_n) is a sequence in a set X such that $\operatorname{range}(x_n)$ is infinite. We will show that it has an injective subsequence with the same range. We construct the subsequence recursively.

Let $n_1 = 1$. Assume that we have defined $n_1, \dots, n_k$ for some $k \in \mathbb{N}$ such that:

(a) $n_1 < n_2 < \cdots < n_k$.
(b) $x_{n_1}, x_{n_2}, \ldots, x_{n_k}$ are all distinct.
(c) There is an $m \in \mathbb{N}$ such that $\{x_1, \ldots, x_{n_k}\} = \{x_1, \ldots, x_m\}$.

Since the range of (x_n) is infinite, the set

$$Z = \big\{m' \in \mathbb{N} : x_{m'} \notin \{x_1, \ldots, x_m\}\big\}$$

is non-empty.

Let n_{k+1} be its minimal element, which exists by the well-ordering principle. Observe that

$$x_{n_{k+1}} \notin \{x_1, \ldots, x_m\} = \{x_1, \ldots, x_{n_k}\}$$

Thus, $x_{n_1}, \ldots, x_{n_{k+1}}$ are all distinct.

By the choice of n_{k+1} to be minimal, for all j with $1 \leq j < n_{k+1}$, we have $x_j \in \{x_1, \ldots, x_{n_k}\}$. Thus, $n_{k+1} > n_k$ and

$$\{x_{n_1}, x_{n_2}, \ldots, x_{n_k}, x_{n_{k+1}}\} = \{x_1, x_2, \ldots, x_{n_{k+1}-1}, x_{n_{k+1}}\}.$$

Consequently, by recursion we have our desired subsequence (x_{n_k}). □

(13) Suppose that (x_n) is a sequence in $\mathbb{R}$ with the property that for all $N \in \mathbb{N}$, there exists $m \in \mathbb{N}$ such that $x_m < \min\{x_1, \ldots, x_N\}$. Prove that (x_n) has a subsequence (x_{n_k}) which is strictly decreasing.

Proof. Suppose that (x_n) is a sequence in $\mathbb{R}$ with the property that for all $N \in \mathbb{N}$, there exists $m \in \mathbb{N}$ such that $x_m < \min\{x_1, \ldots, x_N\}$. We will construct a strictly decreasing subsequence.

Let $n_1 = 1$. Assume that we have defined $n_1, \ldots, n_k$ for some k so that

$$x_{n_1} > x_{n_2} > \ldots > x_{n_k}$$

and

$$n_1 < n_2 < \cdots < n_k.$$

By hypothesis, the set

$$S = \{m' \in \mathbb{N} : x_{m'} < \min\{x_1, x_2, \ldots, x_{n_k}\}\}$$

is non-empty. Let n_{k+1} be the least element of S. It exists by the Well-Ordering Principle. Observe $n_{k+1} \notin \{1, \ldots, n_k\}$ since

$$n_{k+1} \notin \{x_1, x_2, \ldots, x_{n_k}\}.$$

Thus, $n_{k+1} > n_k$. Also, since $x_{n_{k+1}} \in S$, we have $x_{n_{k+1}} < x_{n_k}$.

Thus, by recursion, we have a strictly decreasing subsequence (x_{n_k}).

□

(14) Prove that if G is a finite, connected, non-empty planar graph, then the number of vertices minus the number of edges plus the number of faces equals 2.

Proof Hint. Use complete induction and the fact that taking an edge away from a graph (but leaving its vertices) results in at most two connected components. Some algebra is required. □

(15) Prove that for every natural number $n \geq 2$, there exist prime numbers $p_1, p_2, \ldots, p_k$ such that $n = p_1 p_2 \cdots p_k$.

Proof. We use complete induction on n. If $n = 2$, since n is prime, set $p_1 = 2$. Then $n = p_1$ and the result holds.

Suppose the result holds for all natural numbers j with $2 \leq j \leq k$ for some k. If $k + 1$ is prime, let $p_1 = k + 1$. As in the base case, the result holds. If $k + 1$ is not prime, then there exist a, b such that $2 \leq a, b \leq k$ and $k + 1 = ab$. By the inductive hypothesis applied to a and b, there exist primes $u_1, \ldots, u_m$ and $v_1, \ldots, v_p$ such that $a = u_1 u_2 \cdots u_m$ and $b = v_1 v_2 \cdots v_p$. Thus,

$$k + 1 = v_1 v_2 \cdots v_p u_1 u_2 \cdots u_p$$

and the result again holds. By complete induction the result holds for all $n \geq 2$.

□

(16) Prove that for every rational number $r \in \mathbb{Q}$, there exist $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ such that $r = a/b$ and a and b have no common factor other than ±1.

Proof. Let $r \in \mathbb{Q}$. Let $S = \{a \in \mathbb{N}^* : \exists b \in \mathbb{N} \text{ s.t. } r = \pm a/b\}$. Since $r \neq 0$ is rational, $S \neq \varnothing$. By the well-ordering principle S has a minimal elements. Call it a. Let b be the corresponding denominator such that $r = \pm a/b$. If a and b have a common factor $m \geq 1$, then $a = km$ and $b = \ell m$ for some $k, \ell \in \mathbb{N}$. In which case, notice that $0 \leq k \leq a$ and $r = k/\ell$. Thus, $k \in S$. Since a is the minimal element of S, $a \leq k$. Since also $k \leq a$, we have $a = k$. Thus, $m = 1$. If some $m < 0$ is a common factor, then $-m > 0$ is as well. So ± 1 are the only common factors of a and b. □

(17) Prove that if a and b are natural numbers, then there exist $q, r \in \mathbb{N}^*$ such that $b = aq + r$ and $r < a$.

proof hint. This is another Well Ordering Principle problem. Set

$$S = \{r' \in \mathbb{N}^* : \exists q' \in \mathbb{N}^* \text{ s.t. } b = aq' + r'\}.$$

Argue that $S \neq 0$ and choose r to be the minimal element of S. Show that the result holds for that r and its corresponding q. □

(18) Prove that if α is a path from a vertex a to a different vertex b in a graph G, then either α does not pass through any vertex twice or there is a path from a to b which contains fewer vertices than α.

Proof. Let a and b be distinct vertices in a graph G. Assume that there is a path in G from a to b. Let S be the set of all $n \in \mathbb{N}$ such that there is a path from a to b containing exactly n vertices. Assume that S is non-empty; that is, assume that there is a path from a to b. Let n be the minimal element of S, which exists by the well-ordering principle. Let α be a path from a to b containing exactly n vertices. Write:

$$\alpha = v_0, v_1, \ldots, v_{n-1}$$

where $v_0 = a$, $v_{n-1} = b$, and v_i and v_{i+1} are endpoints of an edge in G for all i. Suppose, for a contradiction, that $i < j$ and that $v_i = v_j$. Consider the path:

$$\beta = v_0, v_1, \ldots, v_i, v_{j+1}, \ldots, v_{n-1}$$

obtained by removing the vertices $v_{i+1}, \ldots, v_j$ from α. To see that β is a path, recall that $v_i = v_j$ and so v_i and v_{j+1} are the endpoints of an edge in G. Since $i < j$, β has fewer vertices than α and is still a path from a to b. This contradicts our choice of α, and so α has no repeated vertices. □

(19) Prove that if e is an edge of a connected graph then $G - e$ has at most two connected components.

Proof. Let a, b be the endpoints of e. Suppose that v is any vertex of G. Let S be the set of all $n \in \mathbb{N}^*$ such that there is a path from v to either a or b having length n. Since G is connected, S is non-empty. By the well-ordering principle, there exists a least element of S. Let α be a path from v to either a or b having the least length among all such paths.

Suppose α is the sequence

$$v = v_0, v_1, \ldots, v_n$$

where v_n is either a or b. If α traverses e, there exists an $i < n$ such that $v_i = a$ and $v_{i+1} = b$ or vice versa. Then

$$v_0, v_1, \ldots, v_i$$

would be a path from v to either a or b of shorter length than α. This contradicts the choice of α, so α must not traverse e. Thus, α is a path in $G - e$ from v to one of the endpoints of e.

We conclude that every vertex of $G - e$ is in the same connected component of $G - e$ as one (or both!) of the endpoints of e. Since e has two endpoints, $G - e$ can have at most two components. □

(20) Prove that a connected nonempty graph where every vertex has even degree has an Euler circuit.

idea of proof. Let G be a connected graph with every vertex of even degree.

Case 1: Suppose that every vertex of G has degree 2.

We induct on the number of edges. If G has no edges it consists of a single vertex. The path consisting of only that vertex is an Euler circuit. Suppose therefore that the result holds when G has $k \geq 0$ edges. We show it has $k + 1$ edges. If G has an edge that is a loop based at a vertex v, then remove it to get a graph G'. Every vertex of G' still has even degree (since loops contribute two to degree), so G' has an euler circuit. At the first moment in the Euler circuit when we arrive at v, insert the loop into the Euler circuit. This is then a circuit in G traversing every edge exactly once; hence, and euler circuit. If G does not have any loop, let G' be the graph obtained by removing a vertex v and merging the edges e_- and e_+ into a single edge e. Since neither e_- nor e_+ are a loop, this is possible. G' has every vertex of even degree, so by the inductive hypothesis it has an euler circuit. When e appears in that euler circuit, split it into the two edges e_- and e_+ traversed in the order so that we still have an euler circuit in G. Thus, by induction, every such G has an euler circuit. □(Case 1)

In the general case, let v be a vertex of G having degree at least 4. Split v into the number of vertices corresponding to its degree and pair edges up at each of those. Each connected component of the resulting graph G' has at least one less vertex than G of degree greater than 2, so by induction each has an Euler circuit. By a cyclic shift we may assume each of those circuits starts at the new vertices. Patching them all together gives an Euler circuit in G. By induction the result holds. □

(21) If X is a subset such that there is an injection $f\colon A \to B$ where B is a proper subset of B, then X is infinite.

proof idea. Create an injective sequence by letting $x_0 \in A \setminus B$ and letting $x_{k+1} = f(x_k)$. Show this is an injective sequence. If X were finite, we would have an injection $\{x_1, x_2, \ldots\} \to \{1, 2, \ldots, N\}$ for some $N \in \mathbb{N}$. However, this is impossible since finite sets do not have infinite subsets. □

(22) Recall that the cardinality $|X|$ of a non-empty finite set X is a number n such that there exists a bijection $X \to \{1, \ldots, n\}$. Prove that the number n is unique and prove that if $|X| = |Y|$ then there exists a bijection from X to Y.

Idea Proof of first part. Suppose that $f\colon X \to \{1,\ldots,n\}$ and $g\colon X \to \{1,\ldots,m\}$ are bijections. Then $h = g \circ f^{-1}\colon \{1,\ldots,n\} \to \{1,\ldots m\}$ is a bijection. We induct on n.

If $n = 1$, then $\{1,\ldots,n\}$ has a unique element and since h is a bijection, $\{1,\ldots,m\}$ must as well. Thus $m = 1 = n$.

Assume the result for $n = k$ for some fixed k and prove it for $n = k+1$. Remove $k+1$ from $\{1,\ldots,k+1\}$ and $h(k+1)$ from $\{1,\ldots,m\}$ and restrict the domain and codomain of h to get a bijection. Show that there is a bijection $\alpha\colon \{1,\ldots,m\} \setminus \{h(k+1)\} \to \{1,\ldots,m-1\}$. Then $\alpha \circ h\colon \{1,\ldots,k\} \to \{1,\ldots,m-1\}$ is a bijection. By the induction hypothesis, $k = m-1$, so $m = k+1$, as desired.

□

(23) Prove that if n is a natural number, then there exists $m \in \mathbb{N}$ and digits $d_i \in \{0,1,2\}$ for $i \in \{0,\ldots,m\}$ such that

$$n = \sum_{i=0}^{m} d_i 3^i$$

(In other words, natural numbers can be written in ternary notation.)

(24) Prove that a subset of a countable set is countable.

(25) Prove that the following sets are countable:

(a) $\mathbb{Z}$

(b) $\mathbb{N} \times \mathbb{N}$

(c) $\mathbb{Q}_+ = \{q \in \mathbb{Q} : q > 0\}$

(d) $\bigcup\limits_{\lambda\in\Lambda} A_\lambda$ where Λ is a non-empty countable set and each A_λ is non-empty and countable.

Proof. Recall that we proved that a non-empty set X is countable if and only if there is a surjection $\mathbb{N} \to X$. Equivalently, X is countable if and only if there is a surjective sequence (x_n) in X. Since Λ is countable and non-empty, there is a surjective sequence (λ_n) in Λ. Since A_{λ_n} is non-empty and countable, there is a surjective sequence $(a_{n,k})_k$ in A_{λ_k}. Thus, a_{n_k} is the kth element of the nth set. Since every element of $\bigcup\limits_{\lambda\in\Lambda} A_\lambda$ is in at least one of the sets A_{λ_k}, the function

$$f\colon \mathbb{N} \times \mathbb{N} \to \bigcup_{\lambda\in\Lambda} A_\lambda$$

defined by $f(n,k) = a_{n,k}$ is surjective.
Since $\mathbb{N} \times \mathbb{N}$ is countable (by the Cantor snake), there is a bijection $g\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$. Thus,

$$f \circ g\colon \mathbb{N} \to \bigcup_{\lambda\in\Lambda} A_\lambda$$

is a surjection. Consequently, $\bigcup\limits_{\lambda\in\Lambda} A_\lambda$ is countable. □

(e) $\mathbb{N}^k = \underbrace{\mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}}_{k}$

Proof Idea. There are (at least) two ways to do this. Notice that when $k = 1$ we have $\mathbb{N} = \mathbb{N}^1$ and that is countable by definition. If $k = 2$, we have $\mathbb{N} \times \mathbb{N}$ which is countable by the Cantor Snake. Induct on k and use the fact that $\mathbb{N}^{k+1}$ is in bijection with $\mathbb{N} \times (\mathbb{N}^k)$. □

(26) Prove that for every set X, $\operatorname{card} X < \operatorname{card} \mathcal{P}(X)$.

(27) The interval $(0, 1)$ is uncountable.

(28) If X is an infinite set, then there exists an infinite injective sequence in X

Proof. Assume X is an infinite set. We will construct an injective sequence in X recursively.

Since X is infinite, it is not finite. Thus it is non-empty and no function $X \to \{1, \ldots, n\}$ is a bijection, for any $n \in \mathbb{N}$. Since X is not empty, there exists $x_1 \in X$. Suppose that there exists $k \in \mathbb{N}$ such that we have defined $x_1, \ldots, x_k \in X$ all distinct. Notice that $\{x_1, \ldots, x_k\} \to \{1, \ldots, k\}$ defined by $x_i \mapsto i$ is a bijection since $x_1, \ldots, x_k$ are all distinct. Thus, $\{x_1, \ldots, x_k\} \subsetneq X$. Therefore, there exists $x_{k+1} \in X \setminus \{x_1, \ldots, x_k\}$. Observe that $x_1, \ldots, x_{k+1}$ are all distinct. By recursion, we have a sequence (x_n) in X.

We show that (x_n) is injective. Suppose that $x_i = x_k$ with $i \leq k$. By construction, however, $x_1, \ldots, x_k$ are all distinct and so $i = k$, as desired. □

(29) If X has an infinite injective sequence in X, then for any element $a \in X$, $\operatorname{card} X = \operatorname{card} X \setminus \{a\}$.

Proof. Let (x_n) be an injective sequence in X. If $a \neq x_m$ for any $m \in \mathbb{N}$, let $y_1 = a$ and $y_{k+1} = x_k$ for $k \geq 1$. Notice that (y_n) is an injective sequence whose first term is a.

If $a = x_m$ for some $m \in \mathbb{N}$, let $y_n = x_{n+(m-1)}$ for all $n \in \mathbb{N}$. Notice that (y_n) is still an injective sequence and that $y_1 = a$.

In either case, define $f\colon X \to X \setminus \{a\}$ by $f(x) = y_{n+1}$ if $x = y_n$ for some $n \in \mathbb{N}$ and $f(x) = x$ otherwise. Since (y_n) is injective, f is well-defined and since $a = y_1$ the $X \setminus \{a\}$ is the codomain for f. □

(30) If X and Y are sets such that there is an injection $f\colon X \to Y$, then there exists a surjection $g\colon Y \to X$.

Proof. For this to be true, we need to assume that $X \neq \varnothing$. Assume we have an injection $f\colon X \to Y$. Define $g\colon Y \to X$ as follows. Choose some $x_0 \in X$. If $y \notin \operatorname{range} f$, define $g(y) = x_0$. If $y \in \operatorname{range}(f)$, let $g(y)$ equal that $x \in X$ such that $f(x) = y$. Since f is injective, g is a well-defined function. Since f is a function, g is surjective. □

(31) Let S^1 be the unit circle. For any $\alpha \in \mathbb{R}$, let R_α be the counterclockwise rotation by α radians. (If $\alpha < 0$ this means rotate by $|\alpha|$ radians clockwise.) Suppose that $\theta \in \mathbb{R}$. Let (x_n) be the sequence in S^1 where $x_0 = (1, 0)$ and $x_n = R_\theta(x_{n-1})$ for all $n \in \mathbb{N}$. Prove the following:

(a) The sequence (x_n) is injective if and only if $\theta \notin \pi\mathbb{Q}$ (i.e. θ is not a rational multiple of π.)

Proof idea. We did this very early in the semester. Recall that x_n is obtained by rotating x_0 by an angle $n\theta$. Thus if $x_n = x_0$, we conclude that $n\theta = 2\pi k$ for some $k \in \mathbb{Z}$. Solving for θ shows that θ is a rational multiple of π. □

(b) The sequence (x_n) is periodic (i.e. there exists $n \in \mathbb{N}$ such that $x_n = x_0$) if and only if θ is a rational multiple of π.

Proof idea. Same idea as in the previous one. If $x_n = x_m$, then there exists $k \in \mathbb{Z}$ such that $n\theta = m\theta + 2\pi k$. □

(c) The sequence (x_n) is not surjective.

Proof. Since S^1 is uncountable (remember how to prove this?) no sequence in S^1 can be surjective. □

(d) ~~If $\theta \notin \pi\mathbb{Q}$, then there exists a subsequence (x_{n_k}) converging to x_0.~~

(32) Let $X = \mathcal{P}(\mathbb{R})$ and define $\sim$ on X by $A \sim B$ if and only if there exists a bijection $f\colon A \to B$. Prove that $\sim$ is an equivalence relation.

(33) Let X be a non-empty set and let $\mathcal{F}$ be the set of bijections of X to itself (i.e. permutations of X). For $f, g \in \mathcal{F}$ define $f \sim g$ if and only if there exists a bijection $h \in \mathcal{F}$ such that

$$f = h^{-1} \circ g \circ h.$$

Prove that $\sim$ is an equivalence relation.

Proof. Let $\mathrm{id}\colon X \to X$ be the identity permutation. Recall that $\mathrm{id}^{-1} = \mathrm{id}$. Thus,

$$f = \mathrm{id}^{-1} \circ f \circ \mathrm{id} = \mathrm{id} \circ f \circ \mathrm{id} = f.$$

Thus, $\sim$ is reflexive.

Suppose that $f \sim g$. Thus, there is $h \in \mathcal{F}$ such that $f = h^{-1} \circ g \circ h$. Notice that

$$(h^{-1})^{-1} \circ g \circ h^{-1}.$$

Since h^{-1} is also a permutation of X, $\sim$ is symmetric.

Now suppose that $f \sim g$ and $g \sim k$. Then there are permutations h and j such that

$$f = h^{-1} \circ g \circ h$$

and

$$g = j^{-1} \circ k \circ j.$$

Thus, by associativity we have

$$\begin{aligned} f &= h^{-1} \circ j^{-1} \circ k \circ j \circ h \\ &= (j \circ h)^{-1} \circ k \circ (j \circ h). \end{aligned}$$

Since the composition of bijections is a bijection, $j \circ h$ is a permutation of X. Thus, $f \sim k$. Hence, $\sim$ is transitive. □

(34) State and prove LaGrange's theorem.