F22 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) Suppose that (x_n) is a sequence in a set X such that for all $N \in \mathbb{N}$ there exists $m \geq N$ with $x_m \notin \{x_1, \ldots, x_N\}$. Prove that there exists an *injective* sequence (a_k) in X such that $\text{range}(a_k) = \text{range}(x_n)$. BONUS: Show that we may define the sequence (a_k) in such a way that there is a strictly increasing sequence (n_i) in $\mathbb{N}$ with $a_k = x_{n_k}$ for all $k \in \mathbb{N}$.

Proof. Assume that (x_n) is a sequence in a set X such that for all $N \in \mathbb{N}$ there exists $m \geq N$ with $x_m \notin \{x_1, \ldots, x_N\}$. We will show that there is an injective sequence with the same range. We construct it recursively.

Let $a_1 = x_1$. Assume we have defined $a_1, \ldots, a_k$ such that:

(a) All of $a_1, \ldots, a_k$ are distinct
(b) There exists $n_k \in \mathbb{N}$ such that

$$\{a_1, \ldots, a_k\} = \{x_1, x_2, \ldots, x_{n_k}\}.$$

By our hypothesis, the set $S_k = \{m \in \mathbb{N} : x_m \notin \{x_1, \ldots, x_{n_k}\}$ is non-empty. By the well-ordering principle, there is a least element; let n_{k+1} be that least element and set $a_{k+1} = x_{n_{k+1}}$. Since $a_{k+1} = x_{n_{k+1}} \in S_k$, all of $a_1, \ldots, a_{k+1}$ are distinct. If $n_k \leq j < n_{k+1}$, by our choice of n_{k+1} to be the minimal element of S_k, we must have $x_j \in \{x_1, \ldots, x_{n_k}\}$. (In particular, if $j < n_{k+1}$, then $x_j \in \{x_1, \ldots, x_{n_k}\}$. Thus,

$$\{a_1, \ldots, a_{k+1}\} = \{x_1, x_2, \ldots, x_{n_k}, x_{n_k+1}, \ldots, x_{n_{k+1}}\}.$$

By recursion we have a sequence (a_k). For the BONUS, notice that $n_1 < n_2 < \cdots < n_k$ for all k and that $(a_k) = (x_{n_k})$.

If (a_k) were not injective, there would be k, ℓ such that $a_k = a_\ell$, but $k \neq \ell$. Without loss of generality, we may assume $k < \ell$. Then,

$$a_\ell \in \{a_1, \ldots, a_k, \ldots, a_{\ell-1}\},$$

contradicting our construction of the sequence. Thus, (a_k) is injective.

For each $k \in \mathbb{N}$, there exists $n_k \in \mathbb{N}$ such that

$$\{a_1, \ldots, a_k\} = \{x_1, \ldots, x_{n_k}\}$$

and $a_k = x_{n_k}$. Since $a_{k+1} = x_{n_{k+1}}$ is distinct from each of $x_1, \ldots, x_{n_k}$, we must have $n_{k+1} > n_k$ (as we already observed.) Since these are integers,

$$n_{k+1} \geq n_k + 1.$$

Thus, (by induction) $n_k \geq k$. Thus,

$$x_k \in \{x_1, \ldots, x_{n_k}\} = \{a_1, \ldots, a_k\}.$$

So each x_k is in the range of (a_n), as desired. □

(2) 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 $x_m < \min\{x_1, \ldots, x_N\}$. Recursively define a sequence (n_k) in $\mathbb{N}$ such that $n_{k+1} > n_k$ for all $k \in \mathbb{N}$ and $x_{n_{k+1}} < x_{n_k}$ for all $k \in \mathbb{N}$.

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

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

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}).

□

(3) If P is a (convex) polygon with $n \geq 3$ sides, then P has a triangulation with $n - 2$ triangles and all vertices of the triangulation are also vertices of P.

Proof Hint. For the convex case you can use regular induction. For the nonconvex case, use complete induction. In both cases, for the inductive step break a polygon with $k + 1$ sides into two polygons with fewer sides. In the convex case, you can guarantee that one of these polygons is a triangle. Apply the inductive hypothesis to the smaller polygons and then glue back together to get a triangularion of the larger polygon. □

(4) 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. Consider two cases, depending on whether or not there are one or two components. Some algebra is required. □

(5) Prove that if T is a tree with at least one edge, then T has at least two leaves (i.e. vertices that are each incident to a single edge of T).

Proof. Use complete induction on the number of edges and the definition of a "tree" as a connected graph such that removing any edge keeps the graph connected. For the inductive step, choose an edge e in a tree having $k+1$ edges. Take it away to get two trees T_1 and T_2. Let $L(T)$, $L(T_1)$, and $L(T_2)$ be the number of leaves of each of the trees. Explain why $L(T) \geq L(T_1) + L(T_2) - 2$ and consider separetely the cases when one or both of $L(T_1)$ or $L(T_2)$ has only one leaf. □

(6) Suppose that $f\colon \mathbb{N} \to \mathbb{N}$ is a permutation such that there exists $N \in \mathbb{N}$ with $f(n) = n$ for all $n > N$. Prove that there exist transpositions $\tau_1, \cdot, \tau_k$ such that

$$f = \tau_1 \circ \cdots \circ \tau_k$$

Proof. For a permutation $f\colon \mathbb{N} \to \mathbb{N}$, let $N(f) = \min\{N : f(n) = n \text{ for all } n > N\}$ if it exists. By our assumption, $N(f)$ exists for all the permutations we care about. Induct on $N(f)$. If $N(f) = 1$, then f is the identity which counts as a transposition. Assume that there exists $k \in \mathbb{N}$ such that for any permutation $f'\colon \mathbb{N} \to \mathbb{N}$ with $N(f') \leq k$, then f' is the composition of tranpositions. Let f be a permutation of $\mathbb{N}$ with $N(f) = k+1$.

Since f is a bijection, $f(j) \leq k+1$ for all $j \leq k+1$. If $f(k+1) = k+1$, then $N(f) \leq k$, contradicting our choice of f. Thus, $f(k+1) = m$ for some $m \leq k$. Let $\tau\colon \mathbb{N} \to \mathbb{N}$ be the transposition such that $\tau(m) = k+1$ and $\tau(k+1) = m$. Notice that $\tau \circ f\colon \mathbb{N} \to \mathbb{N}$ is a bijection and that $\tau \circ f(n) = n$ for all $n > k+1$. In fact,

$$\tau \circ f(k+1) = \tau(f(k+1)) = \tau(m) = k+1.$$

Thus, $N(\tau \circ f) \leq k$. By our inductive hypothesis, there exist transpositions $\tau_1, \ldots, \tau_p$ such that

$$\tau \circ f = \tau_1 \circ \cdots \circ \tau_p.$$

Since τ is a transposition, $\tau \circ \tau$ is the identity function. Thus,

$$f = \tau \circ \tau \circ f = \tau \circ \tau_1 \circ \cdots \circ \tau_p.$$

Consequently, f is also a composition of transpositions.

By complete induction, we have our theorem. □

(7) 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 $n \geq 2$.

□

(8) 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. □

(9) 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. You can use induction on b or the Well Ordering Principle problem. To do it with the well-ording principle, set

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

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

Here is the proof by induction on b. If $b = 0$, then $b = a(0) + 0$. Since $a \geq 1$, we can set $q = 0$ and $r = 0$ to get our result. Assume, therefore, that there is a b' such that there exists $q', r' \in \mathbb{N}^*$ such that $r' < a$ and $b' = aq' + r'$. Let $b = b' + 1$. We prove that there exists $q, r \in \mathbb{N}^*$ with $r < a$ so that $b = aq + r$.

If $r' < a - 1$, then $r' + 1 < a$. In which case, let $r = r' + 1$ and $q = q'$ and note that $b = aq + r$, as desired. Suppose, therefore, that $r' = a - 1$. Then:

$$b = b' + 1 = aq' + r' + 1 = aq' + a = a(q' + 1) + 0$$

Setting $q = q' + 1$ and $r = 0$, we again obtain our result. By induction, the statement holds for all a, b.

□

(10) 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. □

(11) 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. □

(12) 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. □

(13) 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. Suppose that α is a path from vertex a to vertex b. We write α as:

$$v_0, v_1, \ldots, v_n$$

where $v_0 = a$, $v_n = b$ and for $i \in \{0, \ldots, n\}$, the vertices v_i and v_{i+1} are the endpoints of an edge.

If no vertex in the list is repeated, we are done. so suppose that $v_i = v_j$ for some $i < j$. Then consider:

$$v_0, \ldots, v_{i-1}, v_j, v_{j+1}, \ldots, v_n$$

If $i = 0$, then this means: $v_j, v_{j+1}, \ldots v_n$. Since $j - i > 0$, this list has fewer vertices than α. Futhermore, if $i = 0$, then $a = v_0 = v_j$ and if $i > 0$, then since $v_i = v_j$, the vertices v_{i-1} and v_j are the endpoints of an edge. Thus, this list is a path from a to b with fewer vertices than α. □

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

proof idea. Create an injective sequence by letting $x_0 \in X \setminus B$ 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. □

(15) 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.)

Proof. We use complete induction on n. If $n = 1$, set $d_0 = 1$ and notice that $n = d_0 \cdot 3^0$. Assume there is a $k \in \mathbb{N}$ such that for all $j \leq k$, j can be written in ternary notation. We show that $k + 1$ can be written in ternary notation.

Case 1: $k + 1$ is not a multiple of 3.

By IH, there exist $d_0, \ldots, d_m$ so that

$$k = d_m \cdot 3^m + \cdots + d_1 \cdot 3 + d_0 \cdot 3^0.$$

Thus,

$$k + 1 = d_m \cdot 3^m + \cdots + d_1 \cdot 3 + (d_0 + 1) \cdot 3^0.$$

If $d_0 = 2$, then

$$k + 1 = 3\big(d_m \cdot 3^{m-1} + \cdots + d_1 \cdot 3^0 + 1\big)$$

would be a multiple of 3, contradicting the case we are in. Thus, $d_0 \neq 2$. By definition, $d_0 \in \{0, 1\}$ and so $(d_0 + 1) \in \{0, 1, 2\}$. Thus, $k + 1$ can be written in ternary notation.

Case 2: $k + 1$ is a multiple of 3.

In this case, there exists $j \in \mathbb{N}$ such that $k + 1 = 3j$. By the IH, m can be written as

$$j = d_m \cdot 3^m + \cdots + d_1 \cdot 3 + d_0 \cdot 3^0$$

with each $d_i \in \{0, 1, 2\}$. Thus,

$$k + 1 = 3j = d_m \cdot 3^{m+1} + \cdots + d_1 \cdot 3^2 + d_0 \cdot 3^1$$

can also be written in ternary. □

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

Proof Sketch 1. If A is finite it is countable by definition, so assume that A is infinite. Every subset of a finite set is finite, so X is also infinite. By assumption X is countable, so there is a bijective sequence (x_n) in X. Since A is non-empty, the set $S_0 = \{n \in \mathbb{N} : x_n \in A\}$ is nonempty. By the well-ordering principle it has a minimum n_0. Assume we have defined $x_{n_0}, \ldots, x_{n_k}$ so that they are all distinct, $n_0 < n_1 < \cdots < n_k$ and for every i, j such that $n_i < j < n_{i+1}$, $x_j \notin A$.

Let $S_{k+1} = \{n > n_k : x_n \in A \text{ and } x_n \neq x_{n_1}, x_{n_2}, \ldots, x_{n_k}\}$. Since A is infinite, S_{k+1} is nonempty. Let $n_{k+1} = \min S_{k+1}$; it exists by the well-ordering principle. Then $x_{n_{k+1}} \in A$ and is different from $x_{n_1}, \ldots, x_{n_k}$ and $n_{k+1} > n_k$. Furthermore, since n_{k+1} was the minimum of S_{k+1}, each x_j with $n_k < j < n_{k+1}$ is not an element of A. By recursion we have a sequence (x_{n_k}) in A.

That sequence is injective since if $x_{n_i} = x_{n_k}$ for some $i < k$, then when we defined x_{n_k} it would have been equal to one of the previous terms of the sequence, but it was not. Similarly, the sequence is injective, since the sequence (x_n) is surjective in X, so if $a \in A$, then there exists n such that $a = x_n$. Since there is a k such that $n < n_k$, and since for each i any term of (x_n) between x_{n_i} and $x_{n_{i+1}}$ is not in A, x_n must be one of the terms of (x_{n_i}). Since A contains a bijective sequence, it is countable.

□

Proof Sketch 2. We begin by showing that every subset of $\mathbb{N}$ is countable. Let $A \subset \mathbb{N}$. If A is finite, it is countable by definition, so assume that A is infinite. In particular, $A \neq \varnothing$. Let $a_1 = \min A$. It exists by the well-ordering principle. Assuming we have defined distinct $a_1, \ldots, a_k$, define

$$a_{k+1} = \min A \setminus \{a_1, \ldots, a_k\}.$$

It exists by the well ordering principle and the fact that $i \mapsto a_i$ is a bijection $\{1, \ldots, k\} \to \{a_1, \ldots, a_k\}$ and so $A \neq \{a_1, \ldots, a_k\}$ because it is infinite. Notice that $a_1, \ldots, a_{k+1}$ are all distinct. By recursion we have an infinite sequence (a_k) which must be injective. In fact,

$$a_1 < a_2 < \cdots < a_k < \cdots$$

for all $k \geq 3$, since if B, C are subsets of $\mathbb{N}$ such that $B \subset C$, then $\min C \leq \min B$. Setting $B = A \setminus \{a_1, \ldots, a_{k+1}\}$ and $C = A \setminus \{a_1, \ldots, a_k\}$ produces the desired inequality.

If $a \in A$, then for large enough k, $a_k > a$. In which case, we must have $a \in \{a_1, \ldots, a_k\}$. Thus, (a_k) is a bijective sequence and so A is countable. Thus, every subset of $\mathbb{N}$ is countable.

Now suppose that X is any countable set and that $A \subset X$ is any subset. If $X = \varnothing$, then $A = \varnothing$ and A is countable. Suppose $X \neq \varnothing$. Then, by definition, there exists a subset $X' \subset \mathbb{N}$ (which is either $\{1, \ldots, n\}$ for some n or $\mathbb{N}$ itself) and a bijection $f\colon\ X' \to X$. Let $A' = \{x \in X' : f(x) \in A\}$. Notice that

$$f|_{A'}\colon\ A' \to A$$

defined by $f|_{A'}(x) = f(x)$ is a bijection.

Since $A' \subset X' \subset \mathbb{N}$, by our result above A' is countable. Since it is in bijection with A, A must also be countable. □

(17) (Bonus Solution) 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) $\bigcup_{\lambda \in \Lambda} A_\lambda$ 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 $\bigcup_{\lambda \in \Lambda} A_\lambda$ 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, $\bigcup_{\lambda \in \Lambda} A_\lambda$ 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 $\mathbb{N} \times (\mathbb{N}^k)$.

□

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

(19) The set of sequences in $\{0, 1\}$ is uncountable.

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

(21) 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. □

(22) 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. □

(23) If there exists $a \in X$ such that $\operatorname{card} X = \operatorname{card} X \setminus \{a\}$, then X has an infinite injective sequence.

Hint: Define $a_0 = a$ and $a_{k+1} = f(a_k)$ for $k \geq 0$ where $f\colon X \to X \setminus \{a\}$ is a bijection. □

(24) 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. □

(25) 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.~~

(26) Prove that the set of algebraic numbers is countable and, therefore, that the set of transcendental numbers is uncountable.

(27) 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.

(28) 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. □

(29) Let G be a group and $H \subset G$ a subgroup. Define $\sim_H$ on G by declaring $x \sim_H y$ if and only if there exists $h \in H$ with $x = h \circ y$.

(a) Prove that $\sim_H$ is an equivalence relation.

Proof. Since H is a subgroup, $\mathbb{1} \in H$. Since for all $x \in G$, $x = \mathbb{1} \circ x$, $x \sim_H x$. Thus, $\sim_H$ is reflexive. If $x \sim_H y$, then there exists $h \in H$ such that $x = h \circ y$. Thus, $h^{-1} \circ x = y$. Since H is a subgroup, $h^{-1} \in H$. Thus, $y \sim_H x$, so $\sim_H$ is symmetric. Finally, suppose that $x \sim_H y$ and $y \sim_H z$. Then there exist $h_1, h_2 \in H$ such that $x = h_1 \circ y$ and $y = h_2 \circ z$. Substituting and using associativity, we have:

$$x = (h_1 \circ h_2) \circ z$$

Since H is a subgroup, $h_1 \circ h_2 \in H$, so $x \sim_H z$. Thus, $\sim_H$ is transitive.

□

(b) Let $a \in G$ and let $[a]$ be its equivalence class under h. Define $f\colon H \to [a]$ by $f(h) = h \circ a$. Prove that f is a bijection.

Proof. Define $g\colon [a] \to H$ by $g(x) = x \circ a^{-1}$. If $x \in [a]$, by definition $a \sim_H x$. By symmetry, $x \sim_H a$. Thus, there exists $h \in H$ such that $x = h \circ a$. Thus, $x \circ a^{-1} = h \in H$, so g satisfies the domain condition. It is well-defined, since its definition does not depend on any particular representation of an element of $[a]$. Note that $g \circ f(h) = (h \circ a) \circ a^{-1} = h$ and $f \circ g(x) = (x \circ a^{-1}) \circ a = x$. Thus, f and g are inverse functions and so f is a bijection. □

(c) Explain why H and $[a]$ have the same cardinality.

Proof. There exists a bijection between them. □

(d) Conclude that if G is finite, then $|G/\sim_H| = |G|/|H|$. (This is Lagrange's Theorem in Group Theory)

Proof. Suppose that G is finite and has n elements. (Since G contains $\mathbb{1}$, $n \geq 1$.) The quotient set $G/\sim_H$ is a partition of G. By the previous part, every element of $G/\sim_H$ has $|H|$ elements. Since there are $|G/\sim_H|$ sets in $G/\sim_H$ and each of them contains $|H|$ elements and every element of G is in exactly one of those sets, $|G| = |G/\sim_H||H|$. $\square$