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 $i \in \{1, \ldots, n-1\}$. 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 $v_0, v_1, \ldots, v_n$ 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 $w_0, w_1, \ldots, w_m$ 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:

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

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 $\bigcap_{\mathcal{E}\in\mathbb{E}} \mathcal{E}$ 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, $\varnothing \in \bigcap_{\mathcal{E}\in\mathbb{E}} \mathcal{E}$, by definition of intersection.

Now suppose that $A \in \bigcap_{\mathcal{E}\in\mathbb{E}} \mathcal{E}$. 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, $A^C \in \bigcap_{\mathcal{E}\in\mathbb{E}} \mathcal{E}$.

Finally, suppose that for each $n \in \mathbb{N}$, $A_n \in \bigcap_{\mathcal{E}\in\mathbb{E}} \mathcal{E}$. 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 $\bigcap_{\mathcal{E}\in\mathbb{E}} \mathcal{E}$ 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 $\mathrm{range}(x_n)$ is infinite, then (x_n) has a subsequence (x_{n_k}) which is injective and such that $\mathrm{range}(x_{n_k}) = \mathrm{range}(x_n)$.

Proof. Assume that (x_n) is a sequence in a set X such that $\mathrm{range}(x_n)$ 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 $n_1, \ldots, n_k$ 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

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

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) Be able to prove that something is or is not an equivalence relation. For example, if $\equiv_7$ is defined on $\mathbb{Z}$ by $x \equiv_7 y$ if and only if $x - y$ is a multiple of 7, prove that $\equiv_7$ is an equivalence relation.

(15) Be able to prove that if $\sim$ is an equivalence relation on X and if f is a given function with domain $X/\sim$ then f is well-defined. For example, if we define $f\colon\ \mathbb{Z}/\sim \to \mathbb{Z}/\sim$ by $f([x]) = [2x]$ then f is well-defined.

(16) Addition of equivalence classes in $\mathbb{Z}/\equiv_p$ is well-defined. That is, define $x \equiv_p y$ if and only $x - y$ is a multiple of p. Define $[x] + [y] = [x + y]$. Prove that $[x] + [y]$ is well-defined.

Proof. Suppose that $[x'] = [x]$ and $[y'] = [y]$. We prove that $[x] + [y] = [x'] + [y']$.

Since $[x'] = [x]$, we have $x \equiv_p x'$. Similarly, $y \equiv_p y'$. By definition, there exist integers k and ℓ such that

$$x' = x + pk$$

and

$$y' = y + p\ell$$

Hence,

$$x' + y' = (x + y) + p(k + \ell).$$

Thus, $x' + y' \equiv_p (x + y)$. Hence, $[x' + y'] = [x + y]$. By definition, this implies $[x'] + [y'] = [x] + [y]$. □

(17) Addition on $\mathbb{Q}^+ = (\mathbb{N} \times \mathbb{N})/\sim$ is well-defined where pairs $(x, y) \sim (a, b)$ if and only if $xb = ya$.

Proof. Recall that we define

$$[(x, y)] + [(z, w)] = [(xw + yz, yw)].$$

Suppose that $[(x', y')] = [(x, y)]$ and $[(z', w')] = [(z, w)]$. We will show:

$$[(x, y)] + [(z, w)] = [(x', y')] + [(z', w')].$$

By the definition of addition, we are required to show:

$$[(xw + yz, yw)] = [(x'w' + y'z', y'w')]$$

Equivalently, we must show:

$$(xw + yz)y'w' = (x'w' + y'z')yw.$$

By the definition of the equivalence relation and the fact that two equivalence classes are equal if and only if their elements are related, we have

$$\begin{aligned} x'y &= y'x, \text{ and} \\ z'w &= w'z \end{aligned}$$

Thus,

$$\begin{aligned} (xw + yz)y'w' &= xwy'w' + yzy'w' \\ &= (xy')ww' + (zw')yy' \\ &= x'yww' + z'wyy' \\ &= (x'w' + z'y')yw \\ &= (x'w' + y'z')yw, \end{aligned}$$

as desired. □

(18) If $\sim$ is an equivalence relation on X, then for all $x, y \in X$, if $[x] \cap [y] \neq \varnothing$ then $[x] = [y]$.

(19) If $\sim$ is an equivalence relation on X, then $x \sim y$ if and only if $[x] = [y]$.

(20) If $\sim$ is an equivalence relation on X, then $X/\sim$ is a partition of X.

(21) 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.

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

(23) 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.

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

(25) 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. □

(26) 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.
(e) $\mathbb{N}^k = \underbrace{\mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}}_{k}$

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

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

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

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

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

(32) 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.)
(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.
(c) The sequence (x_n) is not surjective.
(d) If $\theta \notin \pi\mathbb{Q}$, then there exists a subsequence (x_{n_k}) converging to x_0.

(33) 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.

(34) 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. □

(35) State and prove LaGrange's theorem.