Boğaziçi University - Fall'18

MATH 111
Introduction to Mathematical Structures

P.S. & Homeworks & Midterms

Instructor: Alp Bassa
Teaching Assistant: Mehmet Akif YILDIZ

Contents

1 Problem Sessions

PS 1

September 26, Wednesday

Problem 1 In each case say whether or not the given statement is a proposition. If it is a proposition, indicate its truth value. If it is not proposition, explain why it is not.

(a) $\frac{x}{x} = 1$

> It is not a proposition since there is no numeric value assigned in x.

(b) $13 + 24 = 25$

> Clearly it is a false proposition.

(c) x is positive, negative, or zero.

> It is not a proposition since we cannot decide whether x is a real number or not without further information.

(d) If x is a real number, then x is positive, negative, or zero.

> Clearly it is a true proposition.

Problem 2 Suppose H stands for "James is handsome" and T stands for "James is tall". What English sentences are represented by the following expressions?

(a) $(\sim H \wedge T) \vee H$

> Either James is not handsome and he is tall, or he is handsome.

(b) $\sim H \wedge (T \vee H)$

> James is not handsome, and either he is tall or he is handsome.

(c) $\sim (H \wedge T) \vee H$

> Either James is not both handsome and tall, or he is handsome.

Problem 3 Suppose P stands for "Celtics won the last night" and Q stands for "Lakers won the last night". Determine what English sentences are represented by $\sim (P \wedge Q)$ and $\sim P \vee \sim Q$. Then, conclude that the truth values of those two expressions are the same.

> Observe the statement $\sim (P \wedge Q)$ means that "Celtics and Lakers did not both win last night" while $(\sim P \vee \sim Q)$ means that "Either Celtics or Lakers lost last night". These statements clearly convey the same information. Note that this equivalence is called one of DeMorgan's Laws.

Problem 4 Analyze the logical forms of the following statements:

(a) Either John went to the store, or we are out of eggs.

> If we let P stands for the statement "John went to the store" and Q stands for "We are out of eggs", then this statement could be represented symbolically as $P \vee Q$.

(b) Joe is going to leave home and not come back.

> If we let P stands for the statement "Joe is going to leave home" and Q stands for "Joe is going to come back", then we could represent this statement symbolically as $P \wedge \sim Q$.

(c) Either Bill is at work and Jane is not, or Jane is at work and Bill is not.

> Let B stand for the statement "Bill is at work" and J for the statement "Jane is at work". Then the first half of the statement can be represented as $B \wedge \sim J$ while similarly the second half can be represented as $J \wedge \sim B$. Therefore, the entire statement can be represented as $(B \wedge \sim J) \vee (J \wedge \sim B)$.

Problem 5 Represent the statement "I will study Math 111 on Saturday or Sunday, but not on both days" by a sentential form.

> Make the assignments "P: I will study Math 111 on Saturday" and "Q: I will study Math 111 on Sunday". Then the first clause of the given statement is represented by $P \vee Q$, and the remaining part is given by $\sim (P \wedge Q)$. Therefore, the complete answer is $(P \vee Q) \wedge (\sim (P \wedge Q))$.

Problem 6 Make a truth table for the formula $\sim(P \vee Q) \wedge \sim R$.

P	Q	R	$P \vee Q$	$\sim(P \vee Q)$	$\sim R$	$\sim(P \vee Q) \wedge \sim R$
T	T	T	T	F	F	F
T	T	F	T	F	T	F
T	F	T	T	F	F	F
T	F	F	T	F	T	F
F	T	T	T	F	F	F
F	T	F	T	F	T	F
F	F	T	F	T	F	F
F	F	F	F	T	T	T

Problem 7 Find a formula involving the connectives $\sim$, $\vee$, and $\wedge$ that has the following truth table:

P	Q	?
F	F	T
F	T	F
T	F	T
T	T	T

There are three true statements. So we can write $(\sim P \wedge \sim Q) \vee (P \wedge \sim Q) \vee (P \wedge Q)$. Observe that this can be written as $((\sim P \wedge P) \vee \sim Q)) \vee (P \wedge Q)$ by using distributive law. Since $(\sim P \wedge P)$ is a false statement, we can reduce it to $\sim Q \vee (P \wedge Q)$. Alternatively, recall that $X \wedge T$ is equivalent to X for any X if T is a tautology. Now, we must get a false statement only if P is false and Q is true. Hence we can say that $P \vee \sim Q$ works. To involve the connection $\wedge$, we can write $(P \vee \sim Q) \wedge (P \vee \sim P)$.

Problem 8 Determine which of the following formulas are equivalent to each other:

(a) $(P \wedge Q) \vee (\sim P \wedge \sim Q)$

(b) $\sim P \vee Q$

(c) $(P \vee \sim Q) \wedge (Q \vee \sim P)$

(d) $\sim (P \vee Q)$

(e) $(Q \wedge P) \vee \sim P$

P	Q	$part(a)$	$part(b)$	$part(c)$	$part(d)$	$part(e)$
T	T	T	T	T	F	T
T	F	F	F	F	F	F
F	T	F	T	F	F	T
F	F	T	T	T	T	T

$(P \wedge Q) \vee (\sim P \wedge \sim Q) \equiv (P \vee \sim Q) \wedge (Q \vee \sim P)$ $\quad$ $\sim P \vee Q \equiv (Q \wedge P) \vee \sim P$.

Problem 9 Analyze the logical forms of the following statements:

(a) The lecture will be given only if at least ten people are there.

> Let T stand for the statement "At least ten people are there" and L for "The lecture will be given". The given statement means that if there are not at least ten people there, then the lecture will not be given, or in other words $\sim T \Rightarrow \sim L$. By the contrapositive law, this is equivalent to $L \Rightarrow T$.

(b) Having at least ten people there is a necessary and sufficient condition for the lecture being given.

> Let T and L be the same with part (a). From the necessary condition we can say that the lecture will be given only if at least ten people are there, in other words $L \Rightarrow T$. On the other hand, from the sufficient condition we can say that T implies L, in other words $T \Rightarrow L$. Hence we have $(L \Rightarrow T) \wedge (L \Rightarrow T)$, which is equivalent to $L \Leftrightarrow T$.

(c) If John went to the store then we have some eggs, and if he did not then we do not.

> Let S stand for the statement "John went to the store" and E stand for "We have some eggs". From the sentence we have $(S \Rightarrow E) \wedge (\sim S \Rightarrow \sim E)$. By using the contrapositive law, we can write $(S \Rightarrow E) \wedge (E \Rightarrow S)$, again which is equivalent to $E \Leftrightarrow S$.

Problem 10 Show that $(P \Rightarrow Q) \wedge (R \Rightarrow Q)$ and $\sim Q \Rightarrow \sim (P \vee R)$ are equivalent.

> Recall that $P \Rightarrow Q$ is equivalent to $\sim P \vee Q$ (conditional law).
>
> $$\begin{aligned} (P \Rightarrow Q) \wedge (R \Rightarrow Q) &\equiv (\sim P \vee Q) \wedge (\sim R \vee Q) \\ \text{(distributive law)} &\equiv (\sim P \wedge \sim R) \vee Q \\ \text{(De Morgan's law)} &\equiv \sim (P \vee R) \vee Q \\ \text{(conditional law)} &\equiv (P \vee R) \Rightarrow Q \\ \text{(contrapositive law)} &\equiv \sim Q \Rightarrow \sim (P \vee R) \end{aligned}$$

Problem 11 Write a sentential form logically equivalent to $P \Rightarrow (Q \Rightarrow R)$ in which the only logical connectives are $\sim$ and $\wedge$.

From the conditional law, we have $P \Rightarrow (Q \Rightarrow R) \equiv \sim P \vee (\sim Q \vee R)$. Hence we can write $\sim P \vee (\sim Q \vee R) \equiv \sim P \vee \sim Q \vee R \equiv \sim (P \wedge Q \wedge \sim R)$ by using De Morgan's laws.

Problem 12 Show that $(P \Rightarrow Q) \vee (Q \Rightarrow R)$ is a tautology.

Recall that $X \vee T$ is a tautology for any X if T is a tautology.

$$\begin{aligned}(P \Rightarrow Q) \vee (Q \Rightarrow R) &\equiv (\sim P \vee Q) \vee (\sim Q \vee R)\\ &\equiv \sim P \vee (Q \vee \sim Q) \vee R\\ &\equiv \sim P \vee (\text{tautology}) \ \vee R\\ &\equiv (\sim P \vee R) \vee (\text{tautology})\\ &\equiv \text{tautology}\end{aligned}$$

PS 2

October 3, Wednesday

Problem 1 Let n be an odd number. Prove that $n^3 - n$ is divisible by 24.

Suppose n is an odd integer. Observe that $n^3 - n$ is divisible by 24 if and only if $n^3 - n$ is divisible by 3 and $n^3 - n$ is divisible by 8.

- *$n^3 - n$ is divisible by 3:* Since $n^3 - n = (n-1)n(n+1)$, it is the product of three consecutive integers. There are three cases:

  1. If the remainder of n when dividing by 3 is equal to 0, then n is divisible by 3.
  2. If the remainder of n when dividing by 3 is equal to 1, then $n-1$ is divisible by 3.
  3. If the remainder of n when dividing by 3 is equal to 2, then $n+1$ is divisible by 3.

  As a result, in all cases, $n^3 - n = n(n-1)(n+1)$ is divisible by 3.

- *$n^3 - n$ is divisible by 8:* Since n is odd, we can find an integer k such that $n = 2k+1$. Hence $n^3 - n = 2k(2k+1)(2k+2) = 4k(k+1)(2k+1)$. Observe that one of k and $k+1$ is even. Therefore, $k(k+1) = 2m$ for some integer m and then $n^3 - n = 8m(2k+1)$, which is divisible by 8.

Problem 2 If n is an odd integer greater than 1, prove that sum of odd positive integers less than n is $\frac{(n-1)^2}{4}$.

We must show that for any natural number k, the sum of odd positive integers less than $2k+1$ is k^2. We will prove the claim by induction on k.

Base Case: For $k = 1$, we need $2 \cdot 1 - 1 = 1^2$, which is clearly true.

Induction Hypothesis: Assume the claim holds for $k = s$, in other words assume $1 + 3 + ... + (2s-1) = s^2$ some natural number $s \geq 1$.

Induction Step: We must show $1 + 3 + ... + (2s-1) + (2s+1) = (s+1)^2$. From induction hypothesis, we have $1 + 3 + ... + (2s-1) + (2s+1) = s^2 + (2s+1)$ and clearly the right hand side is equal to $(s+1)^2$, so we are done.

Problem 3 Prove by induction that $7^n - 4^n$ is divisible by 3 for all natural numbers n.

Base Case: For $n = 1$, we need $7^1 - 4^1$ is a multiple of 3, which is clearly true.

Induction Hypothesis: Assume the claim holds for $n = k$, in other words assume $7^k - 3^k$ is a multiple of 3 for some natural number $k \geq 1$.

Induction Step: We must show $7^{k+1} - 4^{k+1}$ is a multiple of 3. We must build a relation between $7^{k+1} - 4^{k+1}$ and $7^k - 4^k$. Observe that $7^{k+1} - 4^{k+1} = 7 \cdot (7^k - 4^k) + 3 \cdot 4^k$. From induction hypothesis, we know $7^k - 4^k$ is divisible by 3 and trivially $3 \cdot 4^k$ is a multiple of 3. Clearly, if two integers are divisible by 3, then their difference will be divisible by 3, too. Hence $7^{k+1} - 4^{k+1}$is a multiple of 3 and we are done.

Problem 4 Prove that if a and b are positive integers with $a > b$, then we can find two integers q and r such that $a = qb + r$ where $0 \leq r < b$ and $q \geq 0$.

If a is a multiple of b, then we can find a positive integer q such that $a = qb$. Then by choosing $r = 0$, we can express a as $qb + r$. Hence assume a is not a multiple of b. Define $I_n = (nb, (n+1)b)$ for $n \geq 0$. Then the union of the intervals I_n gives the set of positive integers that are not divisible by b. Therefore there exists an integer q such that $a \in I_q$. If $a \in I_q$, we have $qb < a < (q+1)b$ and so $0 < a - qb < b$. Let $a - qb = r$. Since $0 < r < b$ and $a = qb + r$, we are done.

Alternatively, consider the set $A = \{|a - qb| : q \in \mathbb{N}\}$. Observe that A is a subset of nonnegative integers. If $0 \in A$, then $|a - qb| = 0$ for some integer q, which implies $a = qb + r$ where $r = 0$ and we are done. Suppose $0 \notin A$. Then A is a nonempty subset of positive integers. Hence A has a minimum element, say r, by well-ordering principle. Suppose $r \geq b$. Then for some integer q either $a - qb = r$ or $a - qb = -r$. If $a - qb = r$ then $|a - (q+1)b| = r - b < r$, and similarly if $|a - (q-1)b| = |b - r| = r - b < r$. In both cases, we can find an element in A that is smaller than r, which contradicts with the minimality of r. As a result, we have $0 < r < b$. Now, for some integer q either $a - qb = r < b$ or $a - qb = -r > -b$. Hence either $a = qb + r$ with $0 < r < b$ or $a = (q-1)b + (b - r)$ with $0 < b - r < b$, which completes the proof.

Problem 5 The favorite number of Cristiano is seven and he want to show that it is the largest integer. To prove his claim, he uses the following reasoning:

Assume that the claim is false. Then let $n > 7$ be the largest integer. Multiplying both sides of this inequality by n gives us $n^2 > 7n$. Since $7n > n$, we can conclude that $n^2 > n$, which contradicts to the being largest of n. Hence the assumption is wrong and so the number 7 is the largest integer.

Discuss the proof of Cristiano, where is the mistake?

The falsity of the claim is "*there exists an integer larger than* 7", not "*there exists a largest integer which is greater than* 7". Therefore, assumption of existence of largest integer makes the proof false.

Problem 6 As a hardworking Math 111 student, John has started to examine reference books and he realized that all of them have the same number of pages. From this inspiration, he concluded that all math books have the same number of pages. Then he claimed that "All sets of n math books have the same number of pages." and this can be proven by induction on n as follows:

- *Let $n = 1$. If X is a set of one math book, then all math books in X have the same number of pages.*
- *Assume that in every set of n math books all the books have the same number of pages.*
- *Now suppose that X is a set of $n + 1$ math books. It is sufficient to show that, if a and b are any two books in X, then a has the same number of pages as b. Let Y be the collection of n books in X except a and similarly let Z be the collection of n books in X except b. By the inductive hypothesis, all books in Y have the same number of pages, and all books in Z have the same number of pages. Therefore, if c is a book in both Y and Z, it will have the same number of pages as a and b. As a result, a has the same number of pages as b and we are done.*

Discuss the proof of John, where is the mistake?

In the induction step, we must ensure that such a book c exists. Since the intersection of the sets Y and Z consists of exactly $n - 1$ books, we can select a book c only if $n - 1 \geq 1$, in other words $n \geq 2$. However, to apply the induction, we have only $n \geq 1$. Therefore, we cannot pass from the case $n = 1$ to the case $n = 2$ by using above argument, which makes the proof false.

Problem 7 Show that the sum of the cubes of three consecutive integers is divisible by nine.

Let P_n stands for the statement $p_n = (n - 1)^3 + n^3 + (n + 1)^3$ is divisible by 9. We must show that P_n is true for all integers n. Firstly observe that P_0 is clearly true since $p_0 = 0$. On the other hand, for any integer k, observe that

$$p_{k+1} - p_k = (k+2)^3 - (k-1)^3 = k^3 + 6k^2 + 12k + 8 - k^3 + 3k^2 - 3k + 1 = 9 \cdot (k^2 + k + 1)$$

From the observation, we can conclude that if P_k is true then P_{k-1} and P_{k+1} are true statements. Now assume that the claim is false, in other words, assume that there exists some integer n such that p_n is not divisible by 9. Now consider the set $A = \{|n| : n \in \mathbb{Z} \text{ and } P_n \text{ is false.}\}$. Since $0 \notin A$, A is a subset of positive integers and A is nonempty due to our assumption. From well-ordering principle, there exists a minimal element in A, say r. Hence either P_r or P_{-r} is false. If P_r is false, then we have P_{r-1} is true due to the minimality, but this is a contradiction because $p_r - p_{r-1}$ is divisible by 9. Similarly, if P_{-r} is false, then we have P_{-r+1} is true due to the minimality but this is a contradiction because $p_{-r} - p_{-r+1}$ is divisible by 9. As a result, P_n is true for any integer n.

Problem 8 Prove that there are infinitely many prime numbers.

Assume the contrary, say there are only finitely many prime numbers. Suppose there are n primes and let $P = \{p_1, p_2, ..., p_n\}$ be the set of all primes. Consider the natural number $M = p_1 p_2 ... p_n + 1$. Observe that M is larger than every element in P, so M is not a prime number. Hence M must have a prime divisor. Since P is the set of all primes, there exists $k \in \{1, 2, ..., n\}$ such that M is divisible by p_k. On the other hand, the number $M - 1$ is the product of all primes, then clearly $M - 1$ is divisible by p_k. Now, both of M and $M - 1$ are divisible by p_k, therefore their difference should be divisible by p_k. However, $M - (M - 1) = 1$ and we need 1 is divisible by p_k, which is a contradiction. As a result, there are infinitely many prime numbers.

Problem 9 Prove that $F_n < 2^n$ for all natural numbers where $F_0, F_1, F_2, ..., F_n, ...$ is the Fibonacci sequence defined as $F_0 = F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$.

Firstly, observe that all elements in the Fibonacci sequence are positive integers. Moreover, since $F_{k+2} = F_{k+1} + F_k$ and $F_k \geq 0$, we have $F_{k+2} \geq F_{k+1}$ for any k. We will prove the claim $F_n < 2^n$ by induction on n.

Base Case: For $n = 1$, we need $1 = F_1 < 2^1 = 2$, which is clearly true.

Induction Hypothesis: Assume the claim holds for $n = k$, in other words assume $F_k < 2^k$ some natural number $k \geq 1$.

Induction Step: We must show $F_{k+1} < 2^{k+1}$. Observe that $F_{k+1} = F_k + F_{k-1}$ implies $F_{k+1} \leq 2 \cdot F_k$ because $F_{k-1} \leq F_k$. On the other hand, from induction hypothesis, $F_k < 2^k$. Hence $F_{k+1} \leq 2 \cdot F_k < 2 \cdot 2^k = 2^{k+1}$ and we are done.

PS 3

October 10, Wednesday

Problem 1 Prove that if $n = ab$ where n, a, and b are positive integers, then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Let $P : a \leq \sqrt{n}$ and $Q : b \leq \sqrt{n}$. We must show that $P \vee Q$ is a true statement. Assume the contrary, in other words say $P \vee Q$ is false. Hence we have P and Q are false statements. Then $a > \sqrt{n}$ and $b > \sqrt{n}$ give us $ab > \sqrt{n} \cdot \sqrt{n} = n$, which is a contradiction. As a result, either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Problem 2 Let n be an integer larger than 4. Prove that the next to the last digit from the right of 3^n is even.

Let $3^n = ...x_n y_n$ for $n > 4$. We must show that x_n is an even integer for $n \geq 5$. Firstly, since 3^n is an odd integer and y_n is the last digit of 3^n, we have $y_n \in \{1, 3, 5, 7, 9\}$. Moreover, $y_n = 5$ implies 3^n is divisible by 5. Therefore, $y_n \in \{1, 3, 7, 9\}$. Now, we will prove that x_n is even for $n \geq 5$ by induction on n.

Base Case: For $n = 5$, $3^5 = 243$ and so $x_5 = 4$, which is even.

Induction Hypothesis: Assume the claim holds for $n = k$, in other words assume x_k is even for some natural number $k \geq 5$.

Induction Step: We must show x_{k+1} is even.

- *If* $y_k = 1$ *or* $y_k = 3$, then x_{k+1} is the remainder of $(3x_k)$ when dividing by 10.

$$x_{k+1} = \begin{cases} 3x_k, & \text{if } x_k = 0 \text{ or } x_k = 2 \\ 3x_k - 10, & \text{if } x_k = 4 \text{ or } x_k = 6 \\ 3x_k - 20, & \text{if } x_k = 8 \end{cases}$$

- *If* $y_k = 7$ *or* $y_k = 9$, then x_{k+1} is the remainder of $(3x_k + 2)$ when dividing by 10.

$$x_{k+1} = \begin{cases} 3x_k + 2, & \text{if } x_k = 0 \text{ or } x_k = 2 \\ 3x_k - 8, & \text{if } x_k = 4 \\ 3x_k - 18, & \text{if } x_k = 6 \text{ or } x_k = 8 \end{cases}$$

In all cases, x_{k+1} is even and so we are done.

Problem 3 If the product of n positive real numbers is equal to 1, then prove that their sum is greater than or equal to n. Moreover, show that their sum can be equal to n only if all of them are equal to 1.

We will prove the claim by induction on n.

Base Case: For $n = 1$, we have a positive real number which is equal to 1. Therefore, the claim is trivially true.

Induction Hypothesis: Assume the claim holds for $n = k$, in other words the sum of k positive real numbers is greater than or equal to k if their product is equal to 1, and equality occurs only if all of them are equal to 1.

Induction Step: Take $k + 1$ positive real numbers whose product is equal to 1. We must show that their sum is greater than or equal to $k + 1$ and the equality occurs only if all of them are equal to 1. Let $a_1, a_2, ..., a_{k+1}$ be some positive real numbers with $a_1 a_2 ... a_{k+1} = 1$. If all of these numbers are equal to 1, then their sum is equal to $k + 1$, which implies the sum is greater than or equal to $k + 1$ and so there is nothing to prove. Now suppose at least one of them is different from 1, in other words, suppose that at least one of the statements $a_1 \neq 1$, $a_2 \neq 1$, ..., $a_{k+1} \neq 1$ is true. Since all of these statements will give us completely same procedures, without loss of generality we can assume that $a_1 \neq 1$. Now we must prove that $a_1 + a_2 + ... a_{k+1} > k + 1$ since at least one of them is different from 1. There are two cases:

- If $a_1 > 1$, then we have $a_2 a_3 ... a_{k+1} < 1$ since the whole product is equal to 1. Then, at least one of the statements $a_2 < 1$, $a_3 < 1$, ..., $a_{k+1} < 1$ is true because their product is strictly less than 1. Again, without loss of generality, we can assume that $a_2 < 1$ and so we have $(a_1 - 1)(a_2 - 1) < 0$.

- If $a_1 < 1$, then we have $a_2 a_3 ... a_{k+1} > 1$ since the whole product is equal to 1. Then, at least one of the statements $a_2 > 1$, $a_3 > 1$, ..., $a_{k+1} > 1$ is true because their product is strictly greater than 1. Again, without loss of generality, we can assume that $a_2 > 1$ and so we have $(a_1 - 1)(a_2 - 1) < 0$.

In both cases we have $(a_1 - 1)(a_2 - 1) < 0$, which implies $a_1 a_2 - a_1 - a_2 + 1 < 0$ and so $a_1 + a_2 > a_1 a_2 + 1$.

On the other hand, define $y_1 = a_1 a_2$, $y_2 = a_3$, $y_3 = a_4$, ..., $y_k = a_{k+1}$. Since the product $y_1 y_2 ... y_k = a_1 a_2 ... a_{k+1} = 1$, we can say that the sum $y_1 + y_2 + ... + y_k \geq k$ due to the induction hypothesis. Therefore we have $1 + y_1 + y_2 + ... + y_k \geq k + 1$. From the definition of those numbers, we can write $1 + a_1 a_2 + a_3 + a_4 + ... + a_k + a_{k+1} \geq k + 1$. Hence by using the fact that $a_1 + a_2 > a_1 a_2 + 1$, we have

$$a_1 + a_2 + a_3 + a_4 + ... + a_{k+1} > 1 + a_1 a_2 + a_3 + a_4 + ... a_{k+1} \geq k + 1$$

As a result, $a_1 + a_2 + a_3 + ... + a_{k+1} > k + 1$ and so we are done.

Problem 4 Let a, b and c be positive real numbers. Show that $(a+b+c)\cdot(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}) \geq 9$.

Observe that $(a+b+c)\cdot(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}) = 3+\frac{a}{b}+\frac{a}{c}+\frac{b}{a}+\frac{b}{c}+\frac{c}{a}+\frac{c}{b}$. Now we have six positive real numbers whose product is equal to 1. Indeed, if define $y_1 = \frac{a}{b}$, $y_2 = \frac{a}{c}$, $y_3 = \frac{b}{a}$, $y_4 = \frac{b}{c}$, $y_5 = \frac{c}{a}$, and $y_6 = \frac{c}{b}$, then $y_1y_2y_3y_4y_5y_6 = 1$. Hence $y_1+y_2+y_3+y_4+y_5+y_6 \geq 6$ from the previous question. Then $(a+b+c)\cdot(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}) = 3+y_1+y_2+y_3+y_4+y_5+y_6 \geq 3+6 = 9$, which completes the proof.

Problem 5 Six non-collinear points in the plane has marked and each line segment between two points has colored in either blue or red. Show that one can always find a triangle whose edges have the same color.

Let A, B, C, D, E, and F be six non-collinear points in the plane. Consider the edges AB, AC, AD, AE, and AF. Let P and Q be the statements "*At least three of these five edges are red.*" and "*At least three of these five edges are blue.*", respectively. If both of P and Q are false, then we would have *there are at most two red edges* and *there are at most two blue edges*, which implies there are at most four edges since we have exactly two colors, which is a contradiction. Hence, at least one of P and Q is true. Without loss of generality, say P is true. Moreover, assuming any three of AB, AC, AD, AE, and AF are red will give completely symmetric procedures. Therefore, without loss of generality, we can assume that AB, AC, and AD are red. Then,

- If BC, BD, and CD are blue, then BCD will be a blue triangle.
- If at least one of BC, BD, and CD is red, without loss of generality say BC is red, then ABC will be a red triangle.

In all cases, we have a triangle whose edges have the same color.

Problem 6 Let P be a polynomial of degree $n \geq 1$ with real coefficients. Show that P can have at most n real zeros, not all necessarily distinct.

We will prove the claim by induction on n.

Base Case: For $n = 1$, let $P(x) = ax + b$ for some real number a, b with $a \neq 0$. Hence P has a unique root $\frac{-b}{a}$, so the claim holds.

Induction Hypothesis: Assume the claim holds for $n = k$, in other words assume any polynomial of degree k has at most k real zeros.

Induction Step: Take a polynomial P of degree $k+1$, we must show that P has at most $k+1$ real zeros. If P has no real zeros, then there is nothing to prove. If P has at least one real root, say c, then we can write $P(x) = (x-c)\cdot Q(x)$ for some polynomial Q of degree k. From induction hypothesis, Q can have at most k real zeros, so P can have at most $k+1$ real zeros, which completes the proof.

Problem 7 Prove that $\sqrt{2}+\sqrt{3}$ is an irrational number.

Let $r = \sqrt{2}+\sqrt{3}$ and assume the contrary, say r is a rational number. Since $r > 0$, we have $\sqrt{3}-\sqrt{2} = \frac{1}{r}$ is rational, too. Then $r - \frac{1}{r}$ would be a rational number, which implies $2\sqrt{2}$ is rational. As a result, we have $\sqrt{2}$ is rational. Then we can find two positive integers a, b which are relatively prime and $\sqrt{2} = \frac{a}{b}$. Then, $a^2 = 2b^2$ implies a^2 is even, so is a. Let $a = 2k$ for some integer k. Hence, $4k^2 = 2b^2$ implies $2k^2 = b^2$ and so b^2 is even. As a result, we have both of a and b are even, which contradicts to the being relatively prime of a and b. Therefore, r is irrational.

Problem 8 Prove that for every natural number $n \geq 13$, we can always find two natural numbers a and b satisfying $n = 3a + 4b$.

Assume the contrary, say there exists an integer $n \geq 13$ for which we cannot find natural numbers a and b satisfying $n = 3a + 4b$. Hence, if we define the set A as $A = \{n \in \mathbb{N} : n \geq 13,$ there are no natural numbers a, b satisfying $n = 3a + 4b\}$, A will be a nonempty subset of positive integers. From well-ordering principle, there exists a minimum element in A, say r. Observe that $13 \notin A$, $14 \notin A$, and $15 \notin A$ since $13 = 3\cdot 3 + 4\cdot 1$, $14 = 3\cdot 2 + 4\cdot 2$, and $15 = 3\cdot 1 + 4\cdot 3$, which implies $r \geq 16$. However, if $r \geq 16$ then we have $r - 3 \geq 13$ and the minimality of r gives us $r - 3 \notin A$. Hence we can find two natural numbers a and b satisfying $r - 3 = 3\cdot a + 4\cdot b$, which implies $r = 3\cdot(a+1) + 4\cdot b$ and so $r \in A$, which is a contradiction. As a result, for every natural number $n \geq 13$, we can always find two natural numbers a and b satisfying $n = 3a + 4b$.

PS 4

October 17, Wednesday

Problem 1 The followings are called as Zarmelo-Fraenkel axioms in set theory. Express each of them by using quantifiers and logical connectives.

- *Extensionality Axiom:* Two sets are equal if and only if they have the same elements.

$$\forall A, \forall B(A = B \Leftrightarrow \forall x(x \in A \Leftrightarrow x \in B))$$

- *Empty Set Axiom:* There is a set with no elements.

$$\exists A, \forall x(x \notin A)$$

- *Subset Axiom:* Let $P(x)$ be a formula. For every set A there is a set S that consists of all the elements of $x \in A$ such that $P(x)$ holds.

$$\forall A, \exists S, \forall x(x \in S \Leftrightarrow (x \in A \wedge P(x)))$$

- *Pairing Axiom:* For every u and v there is a set that consists of just u and v.

$$\forall u, \forall v, \exists A, \forall x(x \in A \Leftrightarrow (x = u \vee x = v))$$

- *Union Axiom:* For every family F of sets there exists a set U that consists of all the elements that belong to at least one set in F.

$$\forall F, \exists U, \forall x(x \in U \Leftrightarrow \exists C(x \in C \wedge C \in F))$$

- *Power Set Axiom:* For every set A there is a family P of sets that consists of all the sets that are subsets of A.

$$\forall A, \exists P, \forall x(x \in P \Leftrightarrow \forall y(y \in x \Rightarrow y \in A))$$

- *Infinity Axiom:* There is a set I that contains the empty set as an element and whenever $x \in I$, then $x \cup \{x\} \in I$.

$$\exists I(\emptyset \in I \wedge \forall x(x \in I \Rightarrow x \cup \{x\} \in I))$$

- *Replacement Axiom:* Let $P(x, y)$ be a formula. For every set A, if for each $x \in A$ there is a unique y such that $P(x, y)$ holds, then there is a set S that consists of all the elements y such that $P(x, y)$ holds for some $x \in A$.

$$\forall A[(\forall x \in A, \exists! y(P(x, y))) \Rightarrow \exists S, \forall y(y \in S \Leftrightarrow (\exists x \in A(P(x, y))))]$$

- *Regularity Axiom:* Every nonempty set A has an element that is disjoint from A.

$$\forall A(A \neq \emptyset \Rightarrow \exists x(x \in A \wedge x \cap A = \emptyset))$$

Problem 2 Let $A = \{1, 2, 3, 4, 5\}$, $B = \mathbb{N}$ and $C = \mathbb{Z}$. Discuss the truth values of the following statements:

(a) $\forall x \in A, \exists y \in B(y = x + 1)$

For any $x \in A$, $x + 1$ is a natural number and so $x + 1 \in B$. Therefore the statement is true.

(b) $\forall x \in A, \exists y \in B(x^3 - 2 = y)$

If $x = 1$ then $x \in A$ but $x^3 - 2 = -1 \notin B$. Hence the statement is false.

(c) $\exists x \in B, \exists y \in C(x^2 + x + 1 = y^2)$

Observe that $x^2 < x^2 + x + 1 < x^2 + 2x + 1 = (x + 1)^2$ for any natural number x. Since $x^2 + x + 1$ lies between the squares of two consecutive integers, it cannot be a perfect square. Therefore, the statement is false.

(d) $\forall x \in C, \exists y \in A, \exists z \in B(x^3 - y = 5z)$

If x is a negative integer, then $x^3 - y$ will be a negative integer for all $y \in A$. Therefore, we cannot find a natural number z so that $5z = x^3 - y$. Hence the statement is false.

(e) $\forall x \in B, \exists y \in A, \exists z \in C(x^3 - y = 5z)$

For any natural number x, the remainder of x^3 when divisible by 5 can be equal to $0, 1, 2, 3, 4$. Therefore, $x^3 - y$ is divisible by 5 for some $y \in \{1, 2, 3, 4, 5\}$ and so we can find an integer z satisfying $x^3 - y = 5z$. As a result, the statement is true.

(f) $\forall x \in C, \exists y \in B, \forall z \in A(x^3 + y \geq z)$

> For any integer x, there is a natural number y that is bigger than $5 - x^3$. Therefore, we can find $y \in B$ such that $y > 5 - x^3 \geq z - x^3$ for all $z \in A$, which implies $x^3 + y \geq 5$. Hence the statement is true.

(g) $\forall x \in C, \exists y \in B, \exists z \in A(x^3 + y = z)$

> If x is a positive integer bigger than 1, then $x^3 + y$ will be greater than 5 for any natural number y. Hence the statement is false.

Problem 3 Write the following sentences and their negations by using quantifiers and logical connectives:

(a) For all positive real numbers ϵ, we can always find a positive real number δ such that $|f(x) - 7| < \epsilon$ holds whenever $|x| < \delta$.

> **Statement:** $\forall \epsilon > 0, \exists \delta > 0, \forall x(|x| < \delta \Rightarrow |f(x) - 7)| < \epsilon)$
> **Negation:** $\exists \epsilon > 0, \forall \delta > 0, \exists x(|x| < \delta \wedge |f(x) - 7| \geq \epsilon)$

(b) There exists an integer q such that for all real numbers $x > 0$, there exists a positive integer k such that $(q - x)^2 > 5$ and that if $x \leq k$ then q is nonnegative.

> **Statement:** $\exists q \in \mathbb{Z}, \forall x > 0, \exists k \in \mathbb{N}[((q - x)^2 > 5) \wedge (x \leq k \Rightarrow q \geq 0)]$
> **Negation:** $\forall q \in \mathbb{Z}, \exists x > 0, \forall k \in \mathbb{N}[((q - x)^2 \leq 5) \vee (x \leq k \wedge q < 0)]$

(c) There is a real number that is not the square of a real number, but the cube of a real number.

> **Statement:** $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \exists z \in \mathbb{R}(x \neq y^2 \wedge x = z^3)$
> **Negation:** $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, \forall z \in \mathbb{R}(x = y^2 \vee x \neq z^3)$

PS 5

October 31, Wednesday

Problem 1 Express the following relations and their negations for the sets A, B and C in terms of quantifiers and logical connectives.

(a) $A \neq \emptyset$

> **Statement:** $\exists x(x \in A)$
> **Negation:** $\forall x(x \notin A)$

(b) $A \neq B$

> **Statement:** $\exists x((x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B))$
> **Negation:** $\forall x(x \in A \Leftrightarrow x \in B)$

(c) $A \subseteq B$

> **Statement:** $\forall x(x \in A \Rightarrow x \in B)$
> **Negation:** $\exists x(x \in A \wedge x \notin B)$

(d) $A \backslash B = \emptyset$

> **Statement:** $\forall x(\sim (x \in A \wedge x \notin B)) \equiv \forall x(x \notin A \vee x \in B)$
> **Negation:** $\exists x(x \in A \wedge x \notin B)$

(e) $A \cap B \neq C$

> **Statement:** $\exists x((x \in A \wedge x \in B \wedge x \notin C) \vee ((x \notin A \vee x \notin B) \wedge x \in C))$
> **Negation:** $\forall x((x \notin A \vee x \notin B \vee x \in C) \wedge ((x \in A \wedge x \in B) \vee x \notin C))$

Problem 2 Prove that $A \cap B \cap C = \emptyset$ if $A \cap B \subseteq B \backslash C$.

> Assume the contrary, say $A \cap B \cap C \neq \emptyset$. Then there exists an element x such that $x \in A \cap B \cap C$, in other words $x \in A$, $x \in B$ and $x \in C$. However, $x \in A \wedge x \in B$ implies $x \in A \cap B$. Since $A \cap B \subseteq B \backslash C$ we have $x \in B \backslash C$, which implies $x \in B$ and $x \notin C$, and this contradicts with $x \in C$.

Problem 3 Prove that if A and $B\backslash C$ are disjoint, then $A \cap B \subseteq C$.

Let $x \in A \cap B$. We must show that $x \in C$. On the other hand,

$$\begin{aligned} A \cap (B\backslash C) = \emptyset \quad &\Leftrightarrow \quad \forall x(x \notin A \cap (B\backslash C)) \\ &\Leftrightarrow \quad \forall x(\sim (x \in A \wedge (x \in B \wedge x \notin C))) \\ &\Leftrightarrow \quad \forall x(x \notin A \vee x \notin B \vee x \in C) \end{aligned}$$

Since $x \notin A$ and $x \notin B$ are false statements, we have $x \in C$ is true and the result follows.

Problem 4 Prove that $A \cap (B\backslash C) = (A \cap B)\backslash C$.

For any x, we can get the following equivalences by using associativity of the logical connective "$\wedge$"

$$x \in A \cap (B\backslash C) \Leftrightarrow x \in A \wedge (x \in B \wedge x \notin C) \Leftrightarrow (x \in A \wedge x \in B) \wedge x \notin C \Leftrightarrow (x \in A \cap B)\backslash C$$

Hence $\forall x(x \in A \cap (B\backslash C) \Leftrightarrow (x \in A \cap B)\backslash C)$ and the result follows.

Problem 5 Prove that $(A \cap B) \cup C = A \cap (B \cup C) \Leftrightarrow C \subseteq A$.

($\Rightarrow$) Assume $(A \cap B) \cup C = A \cap (B \cup C)$ and take an element x from C. We must show that $x \in A$. Observe that $x \in C$ implies $x \in (A \cap B) \cup C$. Then, by using the equality, we can get $x \in A \cap (B \cup C)$ and this implies $x \in A$.

($\Leftarrow$) Assume $C \subseteq A$. From the distributive law, we have $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$. Since $C \subseteq A$ implies $A \cup C = A$, we have $(A \cup C) \cap (B \cup C) = A \cap (B \cup C)$. Hence, $(A \cap B) \cup C = (A \cup C) \cap (B \cup C) = A \cap (B \cup C)$ and we are done.

Problem 6 For each part, determine whether the relation R is symmetric, transitive or reflexive on the set X. Also if R is an equivalence relation, determine equivalence classes.

(a) $X = \mathbb{R}$ and $xRy \Leftrightarrow xy < 0$ for all $x, y \in X$.

R is not reflexive: Observe that xRx implies $x^2 < 0$, which is false for any $x \in \mathbb{R}$.
R is symmetric: Since $xy < 0 \Leftrightarrow yx < 0$, we can say that $xRy \Leftrightarrow yRx$ for all $x, y \in \mathbb{R}$.
R is not transitive: Assume xRy and yRz for some $x, y, z \in \mathbb{R}$. Then we have $xy < 0$ and $yz < 0$, which implies $xy^2z > 0$ and so $xz > 0$. Therefore if xRy and yRz then y does not have a relation with z.

(b) $X = \mathbb{Z}$ and $xRy \Leftrightarrow x^2 = y^2$ for all $x, y \in X$.

> R ***is reflexive:*** $xRx \Leftrightarrow x^2 = x^2$, which is clearly true for all $x \in \mathbb{Z}$
> R ***is symmetric:*** Since $x^2 = y^2 \Leftrightarrow y^2 = x^2$ for all $x, y \in \mathbb{Z}$, it is trivially true.
> R ***is transitive:*** If $x^2 = y^2$ and $y^2 = z^2$, then clearly we have $x^2 = z^2$.
> Hence R is an equivalence relation. Since x and y are in the same equivalence class if and only if $|x| = |y|$, we can list the equivalence classes as follows: $\{[n] : n \in \mathbb{N} \cup \{0\}\}$ where $[n] = \{n, -n\}$ for $n \in \mathbb{N}$ and $[0] = \{0\}$.

(c) $X = \{1, 2, 3, 4\}$ and $R = \{(1, 2), (1, 1), (3, 3), (2, 2), (2, 3), (1, 3), (4, 4)\}$.

> R ***is reflexive:*** Observe that $(1, 1), (2, 2), (3, 3), (4, 4) \in R$.
> R ***is not symmetric:*** Observe that $(1, 2) \in R$ but $(2, 1) \notin R$.
> R ***is transitive:*** We need to check whether "If xRy and yRz then xRz" for all $x, y, z \in X$. However, we can reduce this control to the examination of the cases where $x \neq y$ because if $x = y$ then clearly once we have yRz then automatically we would have xRz. Therefore, in this question we need to consider only whether $(1, 2) \in R \wedge (2, 3) \in R \Rightarrow (1, 3) \in R$, which is true.

(d) $X = [0, \frac{\pi}{2}]$ and $xRy \Leftrightarrow \sin^2 x + \cos^2 y = 1$ for all $x, y \in X$.

> Observe that $\sin^2 x + \cos^2 y = 1 \Leftrightarrow \sin^2 x = \sin^2 y$ since $\sin^2 y + \cos^2 y = 1$ for any y. Moreover, $\sin^2 x = \sin^2 y \Leftrightarrow x = y$ on the interval $[0, \frac{\pi}{2}]$ because the sine function is strictly increasing and nonnegative in this interval. Therefore, we have $xRy \Leftrightarrow x = y$ for all $x, y \in [0, \frac{\pi}{2}]$. Then clearly R ***is reflexive***, R ***is symmetric*** and R ***is transitive***. Hence R is an equivalence relation and the equivalence classes are just singletons, in other words $[x] = \{x\}$ for all $x \in [0, \frac{\pi}{2}]$.

(e) $X = \{1, 2, 3\}$ and $R = \{(1, 2), (2, 1), (1, 1)\}$.

> R ***is not reflexive:*** Observe that $(3, 3) \notin R$.
> R ***is symmetric:*** Observe that $(1, 2) \in R$ and $(2, 1) \in R$. Since there are no pairs (a, b) with $a \neq b$ other than $(1, 2)$ and $(2, 1)$, the claim is clearly true.
> R ***is not transitive:*** Observe that $(2, 1) \in R$ and $(1, 2) \in R$, but $(2, 2) \notin R$.

(f) $X = \{a, b, c\}$ and $R = \{(a, a), (b, b), (c, c)\}$.

> Observe that we have $xRy \Leftrightarrow x = y$ for all $x, y \in X$. As similar to the part (d), R ***is reflexive***, R ***is symmetric*** and R ***is transitive***. Hence R is an equivalence relation and the equivalence classes are just singletons, in other words there are three equivalence classes as $[a] = \{a\}$, $[b] = \{b\}$ and $[c] = \{c\}$.

(g) $X = \mathbb{Z}$ and $xRy \Leftrightarrow |x - y| \leq 7$ for all $x, y \in X$.

> R ***is reflexive:*** Since $|x - x| = 0 \leq 7$, we have xRx for all $x \in \mathbb{Z}$.
> R ***is symmetric:*** Since $|x - y| = |y - x|$, we have $xRy \Leftrightarrow yRx$.
> R ***is not transitive:*** Observe that $1R7$ and $7R14$, but 1 does not have a relation with 14.

(h) $X = \mathbb{N}$ and $xRy \Leftrightarrow x|y$ for all $x, y \in X$.

> R ***is reflexive:*** Since $x|x$ for any natural number, we have xRx for all $x \in \mathbb{N}$.
> R ***is not symmetric:*** Observe that 1 divides 2, but 2 does not divide 1.
> R ***is transitive:*** Observe that if $x|y$ and $y|z$ for some natural numbers, then $\frac{y}{x} \in \mathbb{N}$ and $\frac{z}{y} \in \mathbb{N}$, which implies $\frac{z}{x} = \frac{y}{x} \cdot \frac{z}{y} \in \mathbb{N}$. Hence $(x|y) \wedge (y|z)$ implies $x|z$.

(i) $X = \mathbb{Z}$ and $xRy \Leftrightarrow 3|x - y$ for all $x, y \in X$.

> R ***is reflexive:*** $xRx \Leftrightarrow 3|x - x$, which is clearly true for all $x \in \mathbb{Z}$
> R ***is symmetric:*** Since $3|x - y \Leftrightarrow 3|y - x$ for all $x, y \in \mathbb{Z}$, it is trivially true.
> R ***is transitive:*** If $3|x - y$ and $3|y - z$, then $3|(x - y) + (y - z)$, which implies $3|x - z$.
> Hence R is an equivalence relation. Observe that a natural number x lies in the equivalence class $[0]$ if and only if x is divisible by 3. Similarly, x lies in the equivalence class $[1]$ if and only if the remainder of x when dividing by three is equal to 1 and x lies in the equivalence class $[2]$ if and only if the remainder of x when dividing by three is equal to 2. Therefore, we have three equivalence classes:
> $[0] = \{n \in \mathbb{Z} : n = 3k$ for some integer k$\}$
> $[1] = \{n \in \mathbb{Z} : n = 3k + 1$ for some integer k$\}$
> $[2] = \{n \in \mathbb{Z} : n = 3k + 2$ for some integer k$\}$

(j) $X = \mathbb{Z} \times \mathbb{Z}$ and $(x_1, y_1)R(x_2, y_2) \Leftrightarrow y_1 = y_2$ for all $(x_1, y_1), (x_2, y_2) \in X$.

> R ***is reflexive:*** Observe $(x_1, y_1)R(x_1, y_1)$ since $y_1 = y_1$ for any $(x_1, y_1) \in \mathbb{Z} \times \mathbb{Z}$.
> R ***is symmetric:*** Since $y_1 = y_2 \Leftrightarrow y_2 = y_1$, we can get the equivalence $(x_1, y_1)R(x_2, y_2) \Leftrightarrow (x_2, y_2)R(x_1, y_1)$ trivially.
> R ***is transitive:*** If we have $(x_1, y_1)R(x_2, y_2)$ and $(x_2, y_2)R(x_3, y_3)$ for some $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{Z} \times \mathbb{Z}$, then we have $y_1 = y_2$ and $y_2 = y_3$, which implies $y_1 = y_3$ and so $(x_1, y_1)R(x_3, y_3)$.
> Hence R is an equivalence relation. Since two elements are in the same equivalence class if and only if their second component are equal, the classes can be thought as the lines $y = n$ in the coordinate plane where $n \in \mathbb{Z}$. As a result, we can list the equivalence classes as follows:
> $\{[(0, n)] : n \in \mathbb{Z}\}$ where $[(0, n)] = \{(x, n) : x \in \mathbb{Z}\}$.

PS 6

November 7, Wednesday

Problem 1 Suppose R is a relation on a nonempty set A and let $\mathcal{P}(A)$ be the power set of A. Define a relation S on $\mathcal{P}(A)$ as follows:

$$S = \{(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) : \forall x \in X, \exists y \in Y(xRy)\}$$

(a) If R is reflexive, must S be reflexive?

> **YES** Take an element $X \in \mathcal{P}(A)$. We must show that $(X, X) \in S$. Since R is reflexive, $(x, x) \in R$ for any $x \in X$. Therefore, $\forall x \in X, \exists y \in X(xRy)$ is a true statement because we can choose $y = x$. Hence $(X, X) \in S$ for any $X \in \mathcal{P}(A)$.

(b) If R is symmetric, must S be symmetric?

> **NO** In general, for a formula $P(x, y)$, we cannot say $[\forall x \exists y(P(x, y))]$ implies $[\forall y \exists x(P(y, x))]$ because there can be some y values not working for all x values while some y values work for multiple x values. For example, if $T = \{1, 2, 3\}$ and $L = \{2, 4\}$, for all elements $t \in T$ there exists an element $l \in L$ such that $t < l$, however for $4 \in L$, we cannot find an element $t \in T$ satisfying $4 < t$.
>
> From this intuition, we will construct a counter example. Let $A = \{1, 2, 3\}$ and $R = \{(1, 2), (2, 1)\}$. Clearly R is symmetric. On the other hand, $(\{1\}, \{2, 3\}) \in S$ since $(1, 2) \in R$, but $(\{2, 3\}, \{1\}) \notin S$ since $(3, 1) \notin R$.

(c) If R is transitive, must S be transitive?

> **YES** Suppose $(X, Y), (Y, Z) \in S$. We must show that for any $x \in X$, we can find $z \in Z$ such that $(x, z) \in R$. Let $x \in X$. Since $(X, Y) \in S$, there exists $y \in Y$ such that $(x, y) \in R$. Moreover, since $(Y, Z) \in S$ and $y \in Y$, we can find $z \in Z$ such that $(y, z) \in R$. Now, $(x, y), (y, z) \in R$ and R is transitive, so $(x, z) \in R$.

Problem 2 Suppose R is a relation on a nonempty set A. Let $\mathcal{P}(A)$ be the power set of A and $\mathcal{F}(A) = \mathcal{P}(A) \backslash \{\emptyset\}$. Define relations S_1, S_2 on $\mathcal{P}(A)$ and S_3 on $\mathcal{F}(A)$ as follows:

- $S_1 = \{(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) : \exists x \in X, \exists y \in Y(xRy)\}$
- $S_2 = \{(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) : \forall x \in X, \forall y \in Y(xRy)\}$
- $S_3 = \{(X, Y) \in \mathcal{F}(A) \times \mathcal{F}(A) : \forall x \in X, \forall y \in Y(xRy)\}$

(a) If R is transitive, must S_1 be transitive?

NO In general, for a formula $P(x, y)$, we cannot say $[\exists x \exists y P(x, y)]$ and $[\exists y \exists z P(y, z)]$ imply $[\exists x \exists z P(x, z)]$ because corresponding y values making $P(x, y)$ and $P(y, z)$ true in $[\exists x \exists y P(x, y)]$ and $[\exists y \exists z P(y, z)]$ may be different.

From this intuition, we will construct a counter example. Let $A = \{1, 2, 3\}$ and $R = \{(1, 2), (2, 3), (1, 3), (3, 3)\}$. Firstly R is transitive. On the other hand, observe that $(\{3\}, \{1, 2, 3\}) \in S_1$ since $(3, 3) \in R$, and $(\{1, 2, 3\}, \{2\}) \in S_1$ since $(1, 2) \in R$. However, $(\{3\}, \{2\}) \notin S_1$ since $(3, 2) \notin R$. As a result, S_1 might not be transitive even if R is transitive.

(b) If R is transitive, must S_2 be transitive?

NO Observe that $\forall x \in X \forall y \in \emptyset (xRy)$ is true for any $X \in \mathcal{P}$ since there is no element in the empty set. Hence $(X, \emptyset) \in S_2$ for all $X \in \mathcal{P}$. Similarly, we have $(\emptyset, Y) \in S_2$ for all $Y \in \mathcal{P}$. If S_2 is transitive, then we would have $(X, Y) \in S_2$ for any $X, Y \in \mathcal{P}$ because $(X, \emptyset) \in S_2$ and $(\emptyset, Y) \in S_2$ regardless of the relation R.

Now, finding a counter example will be easy. Let $A = \{1, 2\}$ and $R = \{(1, 1)\}$. Clearly R is transitive. Since $(\{1\}, \emptyset) \in S_2$, $(\emptyset, \{2\}) \in S_2$ and $(\{1\}, \{2\}) \notin S_2$, we have S_2 might not be transitive even if R is transitive.

(c) If R is transitive, must S_3 be transitive?

YES Let $(X, Y), (Y, Z) \in S_3$ for some $X, Y, Z \in \mathcal{F}(A)$. We must show that $(X, Z) \in S_3$, in other words we must have $(x, z) \in R$ for all $x \in X$ and $z \in Z$. Since Y is nonempty, choose an element y from Y. Now we have $(x, y) \in R$ since $(X, Y) \in S_3$ and $(y, z) \in R$ since $(Y, Z) \in S_3$. Moreover, $(x, y) \in R$ and $(y, z) \in R$ imply $(x, z) \in R$ since R is transitive. As a result, if R is transitive, then S_3 must be transitive.

Problem 3 For any set S, define a function $\chi_S : S \to \{0, 1\}$, called the characteristic function of S, as follows:

$$\chi_S(x) = \begin{cases} 1, & \text{if } x \in S \\ 0, & \text{if } x \notin S \end{cases}$$

Show that if A and B are subsets of X then,

(a) $\chi_{A\cap B}(x) = \chi_A(x) \cdot \chi_B(x)$, $\forall x \in X$.

For any $x \in X$, there are four possibilities:

- If $x \in A$ and $x \in B$, then $\chi_{A\cap B}(x) = 1 = 1 \cdot 1 = \chi_A(x) \cdot \chi_B(x)$.
- If $x \in A$ and $x \notin B$, then $\chi_{A\cap B}(x) = 0 = 1 \cdot 0 = \chi_A(x) \cdot \chi_B(x)$.
- If $x \notin A$ and $x \in B$, then $\chi_{A\cap B}(x) = 0 = 0 \cdot 1 = \chi_A(x) \cdot \chi_B(x)$.
- If $x \notin A$ and $x \notin B$, then $\chi_{A\cap B}(x) = 0 = 0 \cdot 0 = \chi_A(x) \cdot \chi_B(x)$.

As a result, $\chi_{A\cap B}(x) = \chi_A(x) \cdot \chi_B(x)$ for any $x \in X$.

(b) $\chi_{A\cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x)$, $\forall x \in X$.

Let $x \in S$. Observe that we have $\chi_S(x) + \chi_{X\setminus S}(x) = 1$ for any $S \subseteq X$. Then,

$$\begin{array}{rcll}
\chi_{A\cup B}(x) & = & 1 - \chi_{X-(A\cup B)}(x) & \textit{from observation} \\
& = & 1 - \chi_{(X-A)\cap(X-B)}(x) & \textit{just set equality} \\
& = & 1 - \chi_{(X-A)}(x) \cdot \chi_{(X-B)}(x) & \textit{from prev. ques.} \\
& = & 1 - (1 - \chi_A(x)) \cdot (1 - \chi_B(x)) & \textit{from observation} \\
& = & 1 - (1 - \chi_A(x) - \chi_B(x) + \chi_A(x) \cdot \chi_B(x)) & \textit{just multiplication} \\
& = & \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x) & \textit{just manipulation}
\end{array}$$

As a result, $\chi_{A\cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x)$ for any $x \in X$.

Problem 4 Suppose $f : A \to B$ and $g : B \to C$ are functions.

(a) Show that if $g \circ f$ is injective then f is injective.

Assume $f(x) = f(y)$ for some $x, y \in A$. Then

$$(g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y)$$

Since $g \circ f$ is injective, $(g \circ f)(x) = (g \circ f)(y)$ implies $x = y$. Hence $f(x) = f(y)$ implies $x = y$ and so f is injective.

(b) Show that if $g \circ f$ is surjective then g is surjective.

Observe that $g \circ f : A \to C$. Hence for any $c \in C$, we can find an element $a \in A$ satisfying $(g \circ f)(a) = c$ since $g \circ f$ is surjective. If we let $f(a) = b$, then we can find $b \in B$ satisfying $g(b) = c$. As a result, for any $c \in C$, we can find $b \in B$ satisfying $g(b) = c$, which implies g is surjective.

Problem 5 Suppose $f : A \to B$ is a function. The image of Z under the function f is defined as $f(Z) = \{b \in B : \exists x \in Z(f(x) = b)\}$ for any $Z \subseteq A$. Prove or disprove:

(a) $f(X \cap Y) = f(X) \cap f(Y)$ if f is injective.

TRUE

($f(X \cap Y) \subseteq f(X) \cap f(Y)$) Suppose $z \in f(X \cap Y)$. Then there exists $x \in X \cap Y$ such that $f(x) = z$. Since $x \in X$ and $x \in Y$, we can get $z \in f(X)$ and $z \in f(Y)$. As a result $z \in f(X) \cap f(Y)$.

($f(X) \cap f(Y) \subseteq f(X \cap Y)$) Suppose $z \in f(X) \cap f(Y)$. Since $z \in f(X)$ and $z \in f(Y)$, we can say there exists $x \in X$ satisfying $f(x) = z$ and there exists $y \in Y$ satisfying $f(y) = z$. On the other hand, $f(x) = z = f(y)$ implies $x = y$ because f is injective. Then $x = y$ implies $x \in Y$ and so $x \in X \cap Y$. As a result $z \in f(X \cap Y)$.

(b) $f(X \backslash Y) = f(X) \backslash f(Y)$ if f is surjective.

FALSE

Let $z \in f(X \backslash Y)$. Then there exists an element $x \in X \backslash Y$ satisfying $f(x) = z$. Since $x \in X$ we have $z \in f(X)$ and then we need $z \notin f(Y)$. However, if f is surjective, we cannot say $z \notin Y$ in general.

Let us try to build a counter example. Let $A = \{1, 2\}$, $B = \{1\}$, $X = A$, $Y = \{2\}$ and $f(1) = f(2) = 1$. Now f is surjective and $f(X \backslash Y) = f(\{1\}) = \{1\} \neq \emptyset = \{1\} \backslash \{1\} = f(X) \backslash f(Y)$

(c) $f(X \cup Y) = f(X) \cup f(Y)$

TRUE

$f(X \cup Y) \subseteq f(X) \cup f(Y)$ Let $z \in f(X \cup Y)$. Then there exists an element $x \in X \cup Y$ satisfying $f(x) = z$. Hence either $x \in X$ or $y \in Y$. Without loss of generality, say $x \in X$. Hence $z \in f(X)$, which implies $z \in f(X) \cup f(Y)$.

$f(X) \cup f(Y) \subseteq f(X \cup Y)$ Suppose $z \in f(X) \cup f(Y)$, then either $z \in f(X)$ or $z \in f(Y)$. Without loss of generality, say $z \in f(X)$, then there exists $x \in X$ satisfying $f(x) = z$. Since $x \in X$ implies $x \in X \cup Y$, we have $z \in f(X \cup Y)$.

Problem 6 Let $F = \{a, b, c\}$ and $G = \{1, 2, 3, 4\}$.

(a) How many functions are there from F to G?

> For any $x \in F$, $f(x)$ can take four different values. Since the values of $f(x)$ and $f(y)$ are independent from each other for any $x, y \in F$, there are $4 \cdot 4 \cdot 4 = 64$ functions from F to G.

(b) How many injective functions are there from F to G?

> We must choose three different elements in G for a, b, c. Since there are four options for a, after assigning the value of $f(a)$, there will be three remaining options because f is injective. Similarly, after assigning the value of $f(b)$, there will be two remaining options for $f(c)$. Hence there are $4 \cdot 3 \cdot 2 = 24$ injective functions from F to G.

(c) How many injective functions are there from G to F?

> We must choose four different elements in F where F contains exactly three elements. Hence, there is no injective function from G to F.

Problem 7 Determine which of the following functions are injective, surjective or bijective.

(a) $a : \mathbb{N} \to \mathbb{N}$, $a(x) = x^2$

> *a is injective:* $a(x) = a(y)$ implies $x^2 = y^2$ and so $x = y$ or $x = -y$. Since the domain of f is natural numbers, $x = -y$ is not the case. Hence $a(x) = a(y)$ implies $x = y$.
>
> *a is not surjective:* Since $2 \in \mathbb{N}$ and there is no natural number x satisfying $a(x) = 2$, a is not surjective.
>
> Then, *a is not bijective* since it is not surjective.

(b) $b : \mathbb{Z} \to \mathbb{Z}$, $b(x) = x + 7$

> *b is injective:* $b(x) = b(y)$ implies $x + 7 = y + 7$ and so $x = y$. Hence $b(x) = b(y)$ implies $x = y$.
>
> *b is surjective:* Since for any $x \in \mathbb{Z}$, $x - 7 \in \mathbb{Z}$ and $b(x - 7) = x$, b is surjective.
>
> Then, *b is bijective* since it is both injective and surjective.

(c) $c : \mathbb{Z} \to \mathbb{Z}$, $c(x) = x^2 + x + 1$

c is not injective: Observe that $c(x) = c(y)$ implies $x^2 + x = y^2 + y$ and then $(x - y)(x + y + 1) = 0$. Therefore, if $x + y = -1$ then we have $c(x) = c(y)$. Indeed, $c(0) = c(-1) = 1$ and so c is not injective.

c is not surjective: Observe that there is no integer x satisfying $x^2 + x + 1 = 0$.

Then, *c is not bijective* since it is not injective.

(d) $d : \mathbb{R} \to \mathbb{R}$, $d(x) = x^3$

d is injective: $d(x) = d(y)$ implies $x^3 = y^3$ and so $(x - y)(x^2 + y^2 + xy) = 0$. Observe that $x^2 + y^2 + xy = 0$ leads $(x + \frac{y}{2})^2 + \frac{3y^2}{4} = 0$ and the last equality can occur only if $x = y = 0$. As a result $d(x) = d(y)$ implies $x = y$.

d is surjective: Since for any $x \in \mathbb{R}$, $\sqrt[3]{x} \in \mathbb{R}$ and $d(\sqrt[3]{x}) = x$, d is surjective.

Then, *d is bijective* since it is both injective and surjective.

(e) $e : \mathbb{R}\backslash\{-1\} \to \mathbb{R}$, $e(x) = \frac{2x}{x+1}$

e is injective: Observe that $e(x) = e(y)$ implies $2x(y + 1) = 2y(x + 1)$ and then $x = y$.

e is not surjective: For all x, $e(x) \neq 2$ since $e(x) = 2$ implies $2x = 2x + 2$.

Then, *e is not bijective* since it is not surjective.

(f) $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f(x, y) = (x + 2y, x - y)$

f is injective: $f(x_1, y_1) = f(x_2, y_2)$ implies $(x_1+2y_1, x_1-y_1) = (x_2+2y_2, x_2-y_2)$. Hence we have $x_1 + 2y_1 = x_2 + 2y_2$ and $x_1 - y_1 = x_2 - y_2$. From the first equality we can get $x_1 - x_2 = 2(y_1 - y_2)$, while the second leads $x_1 - x_2 = y_2 - y_1$. Then $2(y_1 - y_2) = y_2 - y_1$ and so $y_1 = y_2$. Moreover, $y_1 = y_2$ implies $x_1 = x_2$. As a result, $f(x_1, y_1) = f(x_2, y_2)$ implies $(x_1, y_1) = (x_2, y_2)$ and then f is injective.

f is surjective: Take an element $(x, y) \in \mathbb{R} \times \mathbb{R}$. We must find $(u, w) \in \mathbb{R} \times \mathbb{R}$ satisfying $f(u, w) = (x, y)$. Then we need $u + 2w = x$ and $u - w = y$. We can choose $u = \frac{x+2y}{3}$ and $w = \frac{x-y}{3}$ in order to conclude $f(\frac{x+2y}{3}, \frac{x-y}{3}) = (x, y)$ for any $(x, y) \in \mathbb{R} \times \mathbb{R}$. Hence f is surjective.

Then, *f is bijective* since it is both injective and surjective.

(g) $g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $g(x, y) = x^2 + y$

g is not injective: Observe that $g(x_1, y_2) = g(x_2, y_2)$ implies $(x_1)^2 + y_1 = (x_2)^2 + y_2$. Hence $g(-x, y) = g(x, y)$ for all $(x, y) \in \mathbb{R} \times \mathbb{R}$. Since $g(1, 0) = g(-1, 0)$, g in not injective.

g is surjective: Take an element $x \in \mathbb{R}$. Clearly $g(0, x) = x$. Hence g is surjective.

Then, g *is not bijective* since it is not injective.

Problem 8 Let $f : \mathbb{R} \to \mathbb{N}$ be a function where f maps the real number m to the smallest natural number n satisfying $m^2 < n$, and $g : \mathbb{N} \to \mathbb{R}$ be a function given by $g(x) = \sqrt{x - 1}$. Find a formula of $g \circ f$ and prove that $f \circ g$ is a restriction of $g \circ f$ to $\mathbb{N}$.

Firstly, for a real number m, $f(m) = \lfloor m^2 \rfloor + 1$ where $\lfloor . \rfloor$ is the floor function. Hence $(g \circ f)(x) = \sqrt{\lfloor x^2 \rfloor + 1 - 1} = \sqrt{\lfloor x^2 \rfloor}$ and $(f \circ g)(x) = \lfloor (\sqrt{x - 1})^2 + 1 \rfloor = \lfloor x \rfloor$. Moreover, observe that $g \circ f : \mathbb{R} \to \mathbb{R}$ and $f \circ g : \mathbb{N} \to \mathbb{N}$. Then $(f \circ g)(x) = x$. Hence $f \circ g$ is a restriction of $g \circ f$ to $\mathbb{N}$ if and only if $(f \circ g)(n) = (g \circ f)(n)$ for all natural numbers n. Therefore, we need $\sqrt{\lfloor n^2 \rfloor} = n$ for all natural numbers n, which is clearly true.

PS 7

November 14, Wednesday

Problem 1 Let $X = \mathbb{N} \times \mathbb{N}$. Define a relation $\sim$ on X such that $(a, b) \sim (c, d) \Leftrightarrow ad = bc$.

(a) Prove that $\sim$ is an equivalence relation. Hence $\sim$ defines equivalence classes, let Y be the set of those classes.

> $\sim$ is clearly reflexive and symmetric due to the commutativity of multiplication on natural numbers. Moreover, assume $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. We need to show that $(a, b) \sim (e, f)$ by using $ad = bc$ and $cf = ed$. Since $ad = bc$ implies $adf = bcf$ and $cf = ed$ implies $bcf = bed$, we have $adf = bed$ or $d \cdot af = d \cdot be$. Since the last equality implies $af = be$, we can conclude that $(a, b) \sim (e, f)$.

(b) For any class C in Y, prove that there exists a unique element $a \in \mathbb{N}$ satisfying $(x, y) \in C \Rightarrow x \geq a$ and $(a, y) \in C$ for some $y \in X$. Denote this element a by $N(C)$.

> Consider the set of first components of pairs lying in the class C. By well-ordering principle, there exists a smallest element, say $N(C)$. Moreover, if $(N(C), b_1), (N(C), b_2) \in C$ then we would have $N(C)b_1 = N(C)b_2$, which clearly implies $b_1 = b_2$.

(c) For any class C in Y, prove that there exists a unique element $b \in \mathbb{N}$ satisfying $(x, y) \in C \Rightarrow y \geq b$ and $(x, b) \in C$ for some $x \in X$. Denote this element b by $D(C)$.

> Consider the set of second components of pairs lying in the class C. By well-ordering principle, there exists a smallest element, say $D(C)$. Moreover, if $(a_1, D(C)), (a_2, D(C)) \in C$ then we would have $D(C)a_1 = D(C)a_2$, which clearly implies $a_1 = a_2$.

(d) For any class C in Y, prove that if $(N(C), y) \in C$ for some $y \in X$ then $y = D(C)$, and if $(x, D(C)) \in C$ for some $x \in X$ then $x = N(C)$. Hence $(N(C), D(C)) \in C$.

> From the definitions of $N(C), D(C)$, $(x, D(C)) \in C$ and $(N(C), y) \in C$ imply $x \geq N(C)$ and $y \geq D(C)$. Moreover, $(x, D(C)) \sim (N(C), y)$ implies $xy = N(C)D(C)$. By combining the last equality with inequalities $x \geq N(C)$ and $y \geq D(C)$, we can conclude $x = N(C)$ and $y = D(C)$.

(e) Assign the symbol $\frac{N(C)}{D(C)}$ into the class C for any $C \in Y$, and then write $[\frac{N(C)}{D(C)}]$ for the class C. Prove that this assignment is meaningful by showing

$$(N(U), D(U)) = (N(V), D(V)) \Rightarrow U = V \text{ for all } U, V \in Y$$

Notice that this representation gives the set of positive rational numbers.

Suppose $(N(U), D(U)) = (N(V), D(V))$. From part (c), we can say $(N(U), D(U)) \in U$ and $(N(V), D(V)) \in V$. Hence the equivalence classes U and V have a common element, so they are equal.

(f) For any $U, V \in Y$, prove that there exists unique element $S \in Y$ satisfying

$$N(U)D(V)D(S) + N(V)D(U)D(S) = D(U)D(V)N(S)$$

Moreover, for any $(a, b) \in U$ and $(c, d) \in V$, show that $(ad + bc)D(S) = bdN(S)$. ***Notice that the class S corresponds to the sum of two positive rational numbers.***

Firstly, since equivalence classes form a partition, there exists a unique class S containing the pair $(N(U)D(V) + N(V)D(U), D(U)D(V))$. Clearly, S satisfies the equation. Moreover, if S' also satisfies the equation, we would have $(N(S), D(S)) = (N(S'), D(S')$, which implies $S = S'$ from part (e).

On the other hand, if we take $(a, b) \in U$ and $(c, d) \in V$, we must prove that $(ad + bc, bd) \in S$. To do this, we must show

$$(ad + bc)D(U)D(V) = bd(N(U)D(V) + D(U)N(V))$$

This equality holds since $aD(U) = bN(U)$ implies $adD(U)D(V) = bdN(U)D(V)$, and $cD(V) = dN(U)$ implies $bcD(U)D(V) = bdD(U)N(V)$.

(g) For any $U, V \in Y$, prove that there exists unique element $M \in Y$ satisfying

$$N(U)N(V)D(M) = D(U)D(V)N(M)$$

Moreover, for any $(a, b) \in U$ and $(c, d) \in V$, show that $acD(M) = bdN(M)$. ***Notice that the class M corresponds to the multiplication of two positive rational numbers.***

Firstly, since equivalence classes form a partition, there exists a unique class M containing the pair $(N(U)N(V), D(U)D(V))$. Clearly, M satisfies the equation. Moreover, if M' also satisfies the equation, we would have $(N(M), D(M)) = (N(M'), D(M')$, which implies $M = M'$ from part (e).

On the other hand, if we take $(a, b) \in U$ and $(c, d) \in V$, we must prove that $(ac, bd) \in M$. To do this, we must show $acD(U)D(V) = bdN(U)N(V)$. Then the result follows by using $aD(U) = bN(U)$ and $cD(V) = dN(U)$.

Problem 2 Let $f : \mathbb{N} \to \mathbb{Q}^+$ be a function satisfying the followings:

- $f(1) = 1$.
- $f(2n) = f(n) + 1$ for all $n \in \mathbb{N}$.
- $f(2n+1) = \frac{1}{1+f(n)}$ for all $n \in \mathbb{N}$.

Prove that f is a bijection. Discuss whether the number of natural numbers is equal to the number of positive real numbers by inspiration having a bijection between two sets.

Firstly, it can be observed that $f(n) > 1 \Leftrightarrow n$ is even and $f(n) < 1 \Leftrightarrow n$ is odd, $n > 1$.

- f **is injective:** Assume the contrary, say f is not injective. Consider the following set $A = \{n \in \mathbb{N} : \exists m \in \mathbb{N}(f(m) = f(n), n < m)\}$. If f is not injective, we have A is a nonempty subset of natural numbers. Then by well-ordering principle there exists a minimum number in A, say k. Firstly, from the definition, there exists $r > k$ with $f(r) = f(k)$. On the other hand, from the initial observation, k and r have the same parity and $k > 1$. Now, from the properties of f, if k and r even then $f(\frac{k}{2}) = f(\frac{r}{2})$, and if k and r are odd then $f(\frac{k-1}{2}) = f(\frac{r-1}{2})$. In both cases, either $\frac{k}{2} \in A$ or $\frac{k-1}{2} \in A$, but this leads to have an element in A which is smaller than A, which is a contradiction.

- f **is surjective:** Assume the contrary, say f is not surjective. Consider the following set $A = \{a + b : \forall n \in \mathbb{N}(f(n) \neq \frac{a}{b})\}$. If f is not surjective, we have A is a nonempty subset of natural numbers. Then by well-ordering principle there exists a minimum number in A, say k. Firstly, from the definition, there exist $r, s \in \mathbb{N}$ such that $f(n) \neq \frac{r}{s}$ for all $n \in \mathbb{N}$ and $k = r + s$. Due to the minimality we have $r \notin A$ and $s \notin A$. Now, if $r > s$, we have $\frac{r-s}{s} = f(m)$ for some $m \in \mathbb{N}$, but in this case we have $f(2m) = \frac{r-s}{s} + 1 = \frac{r}{s}$, which is a contradiction. Similarly, if $r < s$, we have $\frac{s-r}{r} = f(m)$ for some $m \in \mathbb{N}$, but in this case we have $f(2m+1) = \frac{1}{\frac{s-r}{r}+1} = \frac{r}{s}$, which is a contradiction.

PS 8

November 21, Wednesday

Recall the equivalence relation $\sim$ on the set $\mathbb{N} \times \mathbb{N}$ defined as $(a, b) \sim (c, d) \Leftrightarrow ad = bc$.

Problem 1 Let U, V, W be equivalence classes. Prove the followings:

- ***(associativity of addition)*** $(U + V) + W = U + (V + W)$.
- ***(associativity of multiplication)*** $(U \cdot V) \cdot W = U \cdot (V \cdot W)$.
- ***(distributive law)*** $U \cdot (V + W) = (U \cdot V) + (U \cdot W)$.

Let $(a, b) \in U$, $(c, d) \in V$ and $(e, f) \in W$. It can be easily seen that

- From the definition of addition on the equivalence classes, it can be seen that $(ad + bc, bd) \in U + V$. Then we can say $(adf + bcf + bde, bdf) \in (U + V) + W$. Similarly, we can obtain $(adf + bcf + bde, bdf) \in U + (V + W)$ by using $(a, b) \in U$ and $(cf + de, df) \in V + W$. As a result, we have two classes which have a common element, so they are equal.
- From the definition of multiplication on the equivalence classes, it can be easily seen that the pair (ace, bdf) lies in both of classes $(U \cdot V) \cdot W$ and $U \cdot (V \cdot W)$, hence they are equal.
- Firstly, $(a(cf + de), bdf) \in U \cdot (V + W)$. On the other hand, $(ac, bd) \in U \cdot V$ and $(ae, bf) \in U \cdot W$ imply $(acbf + bdae, bdbf) \in (U \cdot V) + (U \cdot W)$. We must prove that $(a(cf + de), bdf) \sim (acbf + bdae, bdbf)$, which is clearly true.

Problem 2 *(definition of the subtraction)* Let U and V be classes with $U > V$. Prove that there exists a unique class S satisfying $U = V + Y$. This class S is called the difference of U and V, and denoted by $U - V$.

Firstly the uniqueness is clear since if $V + Y_1 = U = V + Y_2$, then clearly we have $Y_1 = Y_2$. Hence we only need to show the existence.

Let $(a, b) \in U$ and $(c, d) \in V$. From the definition of ordering, we have $ad > bc$. Then there exists a natural number m satisfying $ad = bc + m$. Let Y be the class of the pair (m, bd). From the definition of the addition, we have $(md+cbd, dbd) \in V+Y$.

On the other hand, $ad = bc + m$ implies $bdad = bdbc + bdm$. Then we can write $b(md + cbd) = a(dbd)$ and so $(a, b) \sim (md + cbd, dbd)$. As a result, $U = V + Y$.

Problem 3 Let U be a class. Prove that there exist two classes V and W satisfying $V < U$ and $U < W$.

Take $(a, b) \in U$. Let W and V be the classes of the pairs $(a, b + b)$ and $(a + a, b)$, respectively. Observe that

- $V < U \Leftrightarrow ab < (b + b)a \Leftrightarrow ab < ba + ba$ which is clearly true.
- $U < W \Leftrightarrow ab < b(a + a) \Leftrightarrow ab < ba + ba$ which is clearly true.

Hence we have $V < U$ and $U < W$.

Problem 4 Let U and V be classes with $U > V$. Prove that there are infinitely many classes W satisfying $U > W$ and $W > V$.

Take $(a, b) \in U$ and $(c, d) \in V$. Let W be the class of the pair $(a + c, b + d)$. Since $U > V$, we have $ad > bc$. Observe that

- $U > W \Leftrightarrow a(b + d) > b(a + c) \Leftrightarrow ab + ad > ba + bc \Leftrightarrow ad > bc$
- $W > V \Leftrightarrow (a + c)d > (b + d)c \Leftrightarrow ad + cd > bc + dc \Leftrightarrow ad > bc$

Hence there exists a rational number between two different rationals. Inductively, it can be easily seen that there are infinitely many rationals W satisfying $U > W > V$.

PS 9

November 30, Friday

Problem 1 Let ξ and ν be cuts. If $\xi < \nu$, then prove that there exists a unique cut μ satisfying $\xi + \mu = \nu$.

Define the set $\mu = \{Y - X : Y \in \nu, X \notin \xi, X < Y\}$. We need to prove two things:

1

- From the definition of ordering, $\xi < \nu$ implies there exists a rational number R such that $R \in \nu$ and $R \notin \xi$. Since there is no greatest element in ν, there exists $S \in \nu$ with $R < S$. Since $R \notin \xi$ and $R < S$, we have $S \notin \xi$. Hence $S - R$ is a rational number and $S - R \in \mu$ from the definition and so $\mu \neq \emptyset$.
- Since ξ and ν are cuts, there are rational numbers $P \in \xi$ and $Q \notin \nu$. Observe that $\xi < \nu$ implies $P \in \nu$ and then we have $P < Q$. We claim $Q - P \notin \mu$. Assume the contrary, say $Q - P \in \mu$. Then there exist $X \notin \xi$ and $Y \in \nu$ with $X < Y$ such that $Q - P = Y - X$, so we have $Q + X = P + Y$. However, $X \notin \xi$ and $P \in \xi$ imply $P < X$ whereas $Q \notin \nu$ and $Y \in \nu$ imply $Y < Q$. As a result, we can conclude $P + Y < Q + X$, which is a contradiction. Therefore, $Q - P \notin \mu$ and so μ is a proper subset of rational numbers.
- Let $Z \in \mu$ and $U < Z$. We need to prove that $U \in \mu$. Since $Z \in \mu$, from the definition of μ, there are rational numbers $X \notin \xi$ and $Y \in \nu$ with $X < Y$ and $Z = Y - X$. Let $Y_1 = U + X$. Observe that $U < Z$ implies $Y_1 < Y$. Since $Y \in \nu$ and ν is a cut, we have $Y_1 \in \nu$. Then, again from the definition of μ, we have $Y_1 - X = U \in \mu$ since $Y_1 \in \nu$ and $X \notin \xi$.
- Let $Z \in \mu$. We need to show that there exists $Z_1 \in \mu$ such that $Z < Z_1$. Since $Z \in \mu$, from the definition of μ, there are rational numbers $X \notin \xi$ and $Y \in \nu$ with $X < Y$ and $Z = Y - X$. Moreover, since Y is not the greatest element of ν, there exists $Y_1 \in \nu$ such that $Y < Y_1$. Since $X < Y$ and $Y < Y_1$, we have $X < Y_1$. Let $Z_1 = Y_1 - X$, then from the definition of μ, we have $Z_1 \in \mu$ and clearly $Z < Z_1$. **Hence $\boldsymbol{\mu}$ is a cut.**

2

- Let $T \in \xi + \mu$. We need to prove that $T \in \nu$. From the definition of $\xi + \mu$, there exist $U \in \xi$ and $Z \in \mu$ such that $T = U + Z$. Moreover, from the definition of μ, there are rationals satisfying $Z = Y - X$, $Y \in \nu$, $X \notin \xi$. Hence we have $T = U + Y - X$. Since $U \in \xi$ and $X \notin \xi$, we have $T < Y$. Then, $Y \in \nu$ and $T < Y$ imply $T \in \nu$.
- Let $T \in \nu$. We need to prove that $T \in \xi + \mu$. If $T \notin \xi$, take $U \in \xi$. Also, since T is not the greatest in ν, there exists $L \in \nu$ with $T < L$. Then there exists a natural number n such that $N = U + (n-1)(L - T) \in \xi$ and $M = U + n(L - T) \notin \xi$. Hence $L - T = M - N$ implies $L - M = T - N$ and so $T = N + (T - N) = N + (L - M)$. Observe $N \in \xi$ and $L - M \in \mu$ since $L \in \nu$ and $M \notin \xi$. As a result, we have show that if $T \notin \xi$ then $T \in \xi + \mu$. On the other hand, we know $R \notin \xi$ and $R \in \nu$, which implies $R \in \xi + \mu$. Therefore, if $T \in \xi$, $T < R$ leads $T \in \xi + \mu$. **Hence $\boldsymbol{\xi + \mu = \nu}$.**

The uniqueness is trivial since $\xi + \mu_1 = \nu = \xi + \mu_2$ clearly implies $\mu_1 = \mu_2$.

Problem 2 Let ξ be a cut. If $\xi^n = \xi$ for some natural number $n \geq 2$, then prove that ξ consists of all rational numbers smaller than 1.

Let $x \geq 1$ be a rational number. We need to show that $x \notin \xi$. Assume the contrary. Suppose $x \in \xi$. Since x is not the greatest element, there is a rational number $x' \in \xi$ with $x' > x \geq 1$. Hence there exists a natural number m such that $x' > 1 + \frac{1}{m}$. Define $y_k = 1 + \frac{n^{k-1}}{m}$ for any natural number k. Observe that $y_1 = x' \in \xi$. Moreover, for any natural number k, if we have $y_k \in \xi$, then $\xi^n = \xi$ implies $(y_k)^n \in \xi$. On the other hand $y_{k+1} = 1 + \frac{n^k}{m} < (1 + \frac{n^{k-1}}{m})^n = (y_k)^n \in \xi$ implies $y_{k+1} \in \xi$. As a result, we have $y_k \in \xi$ for any natural number k. Since the sequence $\{y_k\}$ goes to infinity, we would have ξ contains all rational numbers, which is a contradiction.

Secondly, let $x < 1$ be a rational number. We need to show that $x \in \xi$. Assume the contrary. Suppose $x \notin \xi$. If $x^n \in \xi$, then we would have $x^n \in \xi^n$ and x^n can be written as a product of n terms lying outside of ξ (actually each term is just x), which is a contradiction. Therefore, we have $x^n \notin \xi$. Similarly, we can obtain $x^{n^k} \notin \xi$ for all natural numbers k. However, the sequence $\{x^{n^k}\}$ goes to zero, this implies there is no rational number in ξ, which is a contradiction.

Problem 3 Let ξ and ν be cuts. If $\xi^n = \nu^n$ for some natural number n, then prove that $\xi = \nu$.

If $\xi > \nu$, then we have $\xi^2 = \xi \cdot \xi > \xi \cdot \nu > \nu \cdot \nu = \nu^2$. Similarly we can obtain $\xi^n > \nu^n$ for all natural numbers n, which leads a contradiction. Due to the symmetry, we can say $\xi < \nu$ is not the case, too. As a result, $\xi^n = \nu^n$ implies $\xi = \nu$.

Problem 4 Let ξ be a cut. Prove that there exists a unique cut μ such that the cut $\xi \cdot \mu$ consists of all rational numbers smaller than 1.

Firstly, the uniqueness is trivial, we will just prove the existence. Let t be the smallest element satisfying $t \notin \xi$ (if such an element exists.) Define $\mu = \{\frac{1}{x} : x \notin \xi \text{ and } x \neq t\}$. We will prove that μ is a cut and $\xi \cdot \mu$ consists of all rational numbers smaller than 1. It can be easily seen that μ is a nonempty proper subset of rational numbers. Moreover, if $Z \in \mu$ and $U < Z$, then there exists $X \notin \xi$ with $Z \cdot X = 1$. Since $\frac{1}{U} > \frac{1}{Z} = X$, we have $\frac{1}{U} \notin \xi$ and it is trivially not the smallest. Hence $U \in \mu$. Also, since X is not the smallest, there exists $Y \notin \xi$ with $Y < X$ such that Y is not the smallest. Then we have an element $\frac{1}{Y} \in \mu$ with $Z < \frac{1}{Y}$. Therefore, μ is a cut.

On the other hand, for any rational $X < 1$, we can write $X = 1 - U$ for some rational U. As similar to the problem 1, choose $Z \in \mu$ and take the smallest natural number n satisfying $N = Z(1 + (n-1)U) \in \xi$ and $M = Z(1 + nU) \notin \xi$. Observe $M - N = ZU$ and $(M - N) + XM = ZU + XM < MU + XM = M = (M - N) + N$, and so $XM < N$. Then $\frac{N}{X} > M \notin \xi$ implies $\frac{1}{\frac{N}{X}} \in \mu$. As a result, $X = N \cdot \frac{X}{N}$ with $N \in \xi$ and $\frac{X}{N} \in \mu$, which implies $X \in \xi \cdot \mu$. Finally, if $X \in \xi \cdot \mu$, $X = A \cdot B$ where $A \in \xi$ and $B = \frac{1}{C}$ for some $C \notin \xi$. Since $A < C$, we have $X < 1$. Hence, $\xi \cdot \mu$ consists of all rational numbers smaller than 1.

PS 10

December 5, Wednesday

Recall that we say the sets A and B have the same cardinality if there is a bijection between them, and write $A \approx B$. Let denote the cardinality of the set by $\#S$.

Let define $N_0 = \emptyset$ and $N_n = \{x \in \mathbb{N} : 1 \leq x \leq n\}$ for each $n \in \mathbb{N}$. We say a set S is finite if $S \approx N_n$ for some nonnegative integer n (in this case write $\#S = n$), and S is infinite if it is not finite.

For any two sets A and B,

- If there is an injection from A to B, then $\#A \leq \#B$.
- If there is an injection from A to B, but there is no bijection between them, then $\#A < \#B$.
- If there is a surjection from A to B, then $\#A \geq \#B$.
- If there is a surjection from A to B, but there is no bijection between them, then $\#A > \#B$.
- (*Schröder–Bernstein Theorem*) If $\#A \leq \#B$ and $\#B \leq \#A$, then we have $\#A = \#B$.

A set S is said to be countably infinite if $S \approx \mathbb{N}$, and said to be countable if S is finite or countably infinite. Also, a set that is not countable is called uncountable.

Problem 1 Let A be the set of natural numbers that are divisible by 3 and let B be the set of natural numbers that are divisible by 9. Compare $\#A$ and $\#B$.

Let $f : A \to \mathbb{N}$ be a function given by $f(n) = 3n$. Clearly, $n \in A$ implies $f(n) \in B$ and so $Imf \subseteq B$. Moreover, for any $m \in B$, there exists a natural number n satisfying $m = 9n$ and then $f(3n) = m$ with $3n \in A$. Therefore, $Imf = B$. On the other hand, if $f(a) = f(b)$ for some $a, b \in A$, then $3a = 3b$ implies $a = b$. As a result, f is a bijection between A and B, hence $\#A = \#B$

Problem 2 Show that if $\#A \leq \#B$ then $\#\mathcal{P}(A) \leq \#\mathcal{P}(B)$.

If $\#A \leq \#B$, there exists an injective function $f : A \to B$. Define the function F from $\mathcal{P}(A)$ to $\mathcal{P}(B)$ as $F(S) = \{f(a) : a \in S\}$ for any $S \in \mathcal{P}(A)$. We will prove that $F : \mathcal{P}(A) \to \mathcal{P}(B)$ and it is injective.

For any $S \in \mathcal{P}(A)$, $a \in S$ implies $f(a) \in B$ since $f : A \to B$. Therefore, $F(S) \subseteq B$ and so $F(S) \in \mathcal{P}(B)$. As a result, $F : \mathcal{P}(A) \to \mathcal{P}(B)$.

Suppose $F(S_1) = F(S_2)$ for some $S_1, S_2 \in \mathcal{P}(A)$. If we prove that $S_1 \subseteq S_2$, then due to the symmetry we can say $S_2 \subseteq S_1$ and we get $S_1 = S_2$. Let $a \in S_1$. From the definition we have $f(a) \in F(S_1)$. Since $F(S_1) = F(S_2)$, this implies $f(a) \in F(S_2)$. Again from the definition we have $f(a) = f(b)$ for some $b \in S_2$. However, f was injective, then we get $a = b$ and so $a \in S_2$. Since a was arbitrary, we get $a \in S_1$ implies $a \in S_2$, in other words $S_1 \subseteq S_2$. As a result, F is injective.

Problem 3 Prove that $[a, b] \approx (a, b)$ for all real numbers $a < b$

(a) by using Schröder–Bernstein Theorem.

Let $f_1 : (a, b) \to [a, b]$ and $f_2 : [a, b] \to (a, b)$ be functions given by $f_1(x) = x$ and $f_2(x) = \frac{x+a}{2} + \frac{b-a}{4}$, respectively. It can be easily seen that f_1 is an injection from (a, b) to $[a, b]$ whereas f_2 is an injection from $[a, b]$ to (a, b). Then by using Schröder-Bernstein theorem, we can say $[a, b] \approx (a, b)$.

(b) without using Schröder–Bernstein Theorem.

We need to construct a bijection between $[a, b]$ and (a, b). Firstly, we have two bijections $h : [a, b] \to [0, 1]$ and $g : (0, 1) \to (a, b)$ given by $h(x) = \frac{x-a}{b-a}$ and $g(x) = (b-a)x + a$, respectively. Moreover, define the function $f : [0, 1] \to (0, 1)$ as follows:

$$f(x) = \begin{cases} \frac{1}{2}, & \text{if } x = 0 \\ \frac{x}{2x+1}, & \text{if } \frac{1}{x} \in \mathbb{N} \\ x, & \text{otherwise} \end{cases}$$

Firstly, f is well-defined since $f(x) \in (0, 1)$ for all $x \in [0, 1]$. On the other hand, if $f(x) = f(y)$ for some $x, y \in [0, 1]$ with $x \neq y$, then from the definition we must have $\frac{x}{2x+1} = y$ with $\frac{1}{x} \in \mathbb{N}$ and $\frac{1}{y} \notin \mathbb{N}$, or vice versa. Without loss of generality, assume $\frac{x}{2x+1} = y$, this leads $\frac{2x+1}{x} = \frac{1}{y}$ and so $2 + \frac{1}{x} = \frac{1}{y}$. However this is a contradiction since the left hand side is a natural number while the right hand side is not. Therefore, f is injective. Moreover, $f(0) = \frac{1}{2}$, and for any $\frac{p}{q} \in (0, 1)$ with $\frac{p}{q} \neq \frac{1}{2}$, we have either $q > p+1 = 2$ or $q > p > 1$. While we have $f(\frac{p}{q-2}) = \frac{p}{q}$ in the former case, we can write $f(\frac{p}{q}) = \frac{p}{q}$ in the latter case. As a result, f is surjective. Hence the composition $g \circ f \circ h : [a, b] \to (a, b)$ is a bijection.

Problem 4 Let S be a set. Prove that S is infinite if and only if there exists a proper subset $T \subset S$ satisfying $S \approx T$.

($\Leftarrow$) If S finite and there exists a proper subset $T \subset S$ satisfying $T \approx S$, then we would have two bijections $f : T \to \mathbb{N}_n$ and $g : S \to \mathbb{N}_m$ for some $n < m$, which leads a contradiction since $f \circ g^{-1}$ would be a bijection between $\mathbb{N}_m$ and $\mathbb{N}_n$.

($\Rightarrow$) Assume S is infinite, we need to construct a proper subset T with a bijection $f : S \to T$. Since S is infinite, there exists a countable subset $C \subseteq S$. Hence, by writing $C = \{c_1, c_2, c_3, ...\}$, we can define a function $f : S \to S$ as:

$$f(x) = \begin{cases} c_{2i}, & \text{if } x = c_i \text{ for some } i \in \mathbb{N} \\ x & \text{otherwise} \end{cases}$$

Clearly, f is a bijection between S and T where $T = S \backslash \{c_1, c_3, c_5, ...\}$ and so $T \subset S$.

Problem 5 Construct a bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$.

Remember the question 11 in homework 3, there was a function $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ given by $f(1,1) = 1$ and if $f(k) = (a,b)$ then $f(k+1) = \begin{cases} (a-1, b+1) & \text{if } a > 1 \\ (b+1, 1) & \text{if } a = 1 \end{cases}$. This function was surjective and it can be seen that it is also injective. Then we can say f^{-1} is a bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$. Here, we will construct another function.

Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be a function defined as $f(m,n) = 2^{m-1} \cdot (2n-1)$. We will prove that f is bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$.

Assume $f(m_1, n_1) = f(m_2, n_2)$ for some $(m_1, n_1), (m_2, n_2) \in \mathbb{N} \times \mathbb{N}$. From the definition, we have $2^{m_1-1} \cdot (2n_1 - 1) = 2^{m_2-1} \cdot (2n_2 - 1)$. If $m_1 \neq m_2$, without loss of generality assume $m_1 > m_2$. Then we get $2^{m_1-m_2} \cdot (2n_1 - 1) = 2n_2 - 1$, which is a contradiction since left hand side is even whereas the right hand side is odd. Hence we have $m_1 = m_2$, and this clearly implies $n_1 = n_2$. As a result, f is injective.

Let $k \in \mathbb{N}$. Define the set $X = \{\frac{k}{2^{m-1}} : k \text{ is divisible by } 2^{m-1}\}$. From the definition, X is a subset of natural numbers and it is nonempty since $k \in X$. Then by well-ordering principle, X has a minimum element, say r. Now we have $k = 2^{m-1} \cdot r$. On the other hand, if r is even, say $r = 2s$. Then, $n = 2^m \cdot s$ implies $s \in X$, which contradicts with the minimality of r. Hence r is odd, and so $r = 2n - 1$ for some natural number n. As a result, we can write $k = 2^{m-1} \cdot (2n-1) = f(m,n)$ for some $(m,n) \in \mathbb{N} \times \mathbb{N}$ and so f is surjective.

Since f is injective and surjective, we are done.

Problem 6 Let S be a set and $\mathcal{P}(S)$ be its power set. Prove that $\#S < \#\mathcal{P}(S)$.

Firstly, there is an injection f from S to $\mathcal{P}(S)$, defined as $f(x) = \{x\}$ for all $x \in S$. Now, we must show that there is no bijection between them. Assume the contrary, say $g : S \to \mathcal{P}(S)$ is a bijection. Notice that for any $x \in S$, we have $g(x) \subseteq S$. Define the set $E = \{x \in S : x \notin g(x)\}$. From the definition $E \subseteq S$ and so $E \in \mathcal{P}(S)$. Since g is surjective, there exists $z \in S$ such that $g(z) = E$. Hence

$z \in g(z) \Leftrightarrow z \in E \Leftrightarrow z \notin g(z)$ which is a contradiction. As a result, $\#S < \#\mathcal{P}(S)$.

Remark: From the definition of countability, there is no injection from a countable set to an uncountable set. On the other hand, the set of real numbers is uncountable. Moreover, the set of irrational numbers, the set of positive numbers and the set of negative numbers are uncountable. Finally, it is unknown that whether there exists a set whose cardinality is strictly greater than natural numbers and strictly smaller than real numbers.

Problem 7 Prove that in the $xy-$plane there is a circle centered at the origin that passes through no points whose coordinates are both rational numbers.

Assume the contrary. Then for any $r > 0$, the circle of radius r centered at the origin contains a point whose both components are rational. Then we can choose a corresponding point (x_r, y_r) on the circle of radius r with $x_r, y_r \in \mathbb{Q}$. Define the function $g(r) = (x_r, y_r)$. Observe that g is injective since chosen points lie on different circles, which is impossible since g is a function from positive real numbers to a countable set $\mathbb{Q} \times \mathbb{Q}$. As a result, there is a circle centered at the origin through no points whose coordinates are both rational.

Alternatively, consider the circle of radius $\sqrt[4]{2}$. For any point (x, y) on this circle, we have $x^2 + y^2 = \sqrt{2}$. Hence at least one of x and y is irrational since $\sqrt{2}$ is irrational. Therefore, this circle cannot contain a point whose both components are rational.

Problem 8 Let $\mathcal{F}$ be a collection of pairwise disjoint open intervals on the real line. Prove that $\mathcal{F}$ is countable.

For any interval $u = (a, b) \in \mathcal{F}$, we can choose a rational point r_u in u since any open interval contains a rational number (to be proved in question 2 of PS 11). On the other hand, since any two elements of $\mathcal{F}$ are disjoint, all chosen points are different. This means there is an injection from $\mathcal{F}$ to the set of rational numbers, namely $g(u) = r_u$ for any $u \in \mathcal{F}$. Hence $\mathcal{F}$ is countable.

PS 11

December 12, Wednesday

Problem 1 Prove that $\#\mathbb{R} = \#\mathcal{P}(\mathbb{N})$.

Firstly, the cardinality of real numbers is the same as the cardinality of the open interval $(0, 1)$ since we can construct a bijection $f : (0, 1) \to \mathbb{R}$ that is given by $f(x) = \tan(\frac{x-1}{2}\pi)$. Moreover, in the last problem session, we have seen that $\#(0, 1) = \#[0, 1]$. Therefore, it suffices to show that $\#[0, 1] = \#\mathcal{P}(\mathbb{N})$.
For any real number in the interval $[0, 1]$, we can express it in base 2. In other words, each real number has a binary expansion. However, this representation is not unique. For example, we can write the binary expansion of $\frac{1}{4}$ as

0.01 or 0.00111111......

Nevertheless, we can make this expansion unique by adding this rule:
The binary expansion cannot end with infinitely many consecutive one's

Then, the bijection between $[0, 1]$ and $\mathcal{P}(\mathbb{N})$ will be clear. Define the function $f : [0, 1] \to \mathcal{P}(\mathbb{N})$ as follows:
Firstly write $f(0) = \emptyset$ and $f(1) = \mathbb{N}$. Then for any $x \in (0, 1)$, x has a unique binary expansion $0.a_1a_2a_3.....$ where $a_i \in \{0, 1\}$ with the rule that there is no natural number k satisfying $\forall m(m > k \Rightarrow a_m = 1)$. Hence write $f(x) = \{n \in \mathbb{N} : a_n = 1\}$. For example, if $x = 0.010111$ then $f(x) = \{2, 4, 5, 6\}$. This function is clearly bijective and we are done.

Problem 2 Let $a < b$. Prove that the open interval (a, b) contains infinitely many rational numbers and infinitely many irrational numbers.

Firstly, without loss of generality we can assume a and b are positive. Then there exists a natural number n such that $\frac{1}{n} < b - a$. Let $m = \lfloor 2na \rfloor$, where $\lfloor x \rfloor$ denotes the largest integer not exceeding x. From the definition, we have $m \le 2na < m + 1$ and so $\frac{m}{2n} \le a < \frac{m+1}{2n}$. On the other hand, $\frac{m+2}{2n} = \frac{m}{2n} + \frac{1}{n} < a + (b - a) = b$.
As a result, we have $\frac{m+1}{n}, \frac{m+2}{n} \in (a, b)$. Moreover, observe $\frac{m+1}{n} < \frac{m+\sqrt{2}}{n} < \frac{m+2}{n}$ and so $\frac{m+\sqrt{2}}{n} \in (a, b)$. Since m and n are natural numbers, we have $\frac{m+1}{n}$ is a rational number and $\frac{m+\sqrt{2}}{n}$ is an irrational number, and they lie on (a, b). Therefore, every open interval contains at least one rational and at least one irrational number which is greater than rational one.
Now, choose $x_1, y_1 \in (a, b)$ such that x_1 is rational and y_1 is irrational with $x_1 < y_1$. If we have an open interval (a, x_k), we can choose rational x_{k+1} and irrational y_{k+1} on (a, x_k) with $x_{k+1} < y_{k+1}$. At the end, we have two infinite sequences $\{x_n\}_{n\ge1} \in \mathbb{Q}$ and $\{y_n\}_{n\ge1} \in \mathbb{R}\backslash\mathbb{Q}$ such that $x_k > x_{k+1}$ and $y_k > y_{k+1}$ for any k.

Problem 3 For each part, prove that X is a group under the operation $*$.

(a) $X = \mathbb{Q}\backslash\{1\}$, $a * b = ab - a - b + 2$ for any $a, b \in X$.

(b) $X = \mathbb{Z}$, $a * b = a + b + 2$ for any $a, b \in X$.

(c) $X = \mathcal{P}(\mathbb{N})$, $A * B = (A\backslash B) \cup (B\backslash A)$ for any $A, B \in X$.

- Firstly we need to check that $*$ is a binary operation. Clearly $a * b$ is a rational number and observe that $a * b = 1 \Leftrightarrow (a-1)(b-1) = 0 \Leftrightarrow a = 1 \vee b = 1$, which is impossible. On the other hand, if e is the identity element, then $a = a * e = ae - a - e + 2$ implies $a(e-2) = e-2$ for all $a \in \mathbb{Q}\backslash\{1\}$. Hence the only candidate for identity element is 2. Let us prove that 2 is identity. For any $a \in \mathbb{Q}\backslash\{1\}$, $2 * a = a * 2 = 2a - a - 2 + 2 = a$. On the other hand, $a * x = 2 \Leftrightarrow x = \frac{a}{a-1}$, so every element $a \in X$ has a unique inverse $\frac{a}{a-1}$. Finally we need to prove associativity. Clearly, $(a * b) * c = a * (b * c) = abc - ac - bc - ab + a + b + c$.

- Clearly $*$ is an associative binary operation. Also observe that -2 is the identity and for each $a \in \mathbb{Z}$, $-4 - a$ is the unique inverse of a.

- Firstly, $*$ is a binary operation since the symmetric difference is always a subset of $\mathbb{N}$. Moreover, $\emptyset$ is the identity element since $(A\backslash\emptyset) \cup (\emptyset\backslash A) = A$ for any A, and the inverse of a set A is just itself. For the associativity, it can be seen that

  $$(A*B)*C = (A\backslash(B\cup C))\cup(B\backslash(A\cup C))\cup(C\backslash(A\cup B))\cup(A\cap B\cap C) = A*(B*C)$$

Problem 4 Let $M = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : a^2 - 5b^2 = 4\}$. Define the operation $\circ$ on M as $(a_1, b_1) \circ (a_2, b_2) = (\frac{a_1a_2 + 5b_1b_2}{2}, \frac{a_1b_2 + b_1a_2}{2})$. Determine whether $(M, \circ)$ is a group or not.

Suppose $(a_1, b_1), (a_2, b_2) \in M$. Then,

$$\begin{aligned}
\left(\frac{a_1a_2 + 5b_1b_2}{2}\right)^2 - 5\left(\frac{a_1b_2 + b_1a_2}{2}\right)^2 &= \frac{(a_1a_2)^2 - 5(a_1b_2)^2 - 5(a_2b_1)^2 + 25(b_1b_2)^2}{4} \\
&= \frac{a_1^2(a_2^2 - 5b_2^2) - 5b_1^2(a_2^2 - 5b_2^2)}{4} \\
&= \frac{4a_1^2 - 20b_1^2}{4} \\
&= 4 \qquad \text{and so } (a_1, b_1) \circ (a_2, b_2) \in M.
\end{aligned}$$

Suppose (e, f) is the identity. Firstly, we must have $\frac{ae+5bf}{2} = a$ and $\frac{af+be}{2} = b$ for all $(a,b) \in M$. Then we must have $a(2-e) = 5bf$ and $b(2-e) = af$ for all $(a,b) \in M$. Hence $5b^2f = a^2f$ implies $f = 0$ since $a^2 - 5b^2 = 4 \neq 0$. Moreover, $a(2-e) = b(2-e) = 0$ implies $e = 2$ since $a = b = 0$ is not the case. As a result, $(2,0) \in M$ is the only candidate for the identity. Clearly, it can be seen that $(a,b) \circ (2,0) = (a,b) = (2,0) \circ (a,b)$. Moreover, for any $(a,b) \in M$, $(a,b) \circ (-a,-b) = (2,0) = (-a,-b) \circ (a,b)$. Hence (a,b) has a unique inverse $(-a,-b) \in M$. Associativity is left as an exercise.

Problem 5 For two real numbers a and b, define the function $f_{a,b} : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ given by $f_{a,b}(x, y) = (x + a, y + b)$ for all $x, y \in \mathbb{R}$. Let X be the set of all such functions. Prove that X is a group under the function composition.

Firstly, observe that $f_{a,b} \circ f_{c,d} = f_{a+c,b+d}$ and so $\circ$ is a binary operation on X. Moreover, clearly it is associative. Finally, $f_{0,0}$ is the identity element and for any $f_{a,b}$, the function $f_{-a,-b}$ is the unique inverse.

Problem 6 The discussions about rotational symmetries in the lecture define a non-commutative group with $2n$ elements. Formally, dihedral group of order $2n$ is given by

$$D_n = \{r^a s^b : 0 \leq a \leq n-1, 0 \leq b \leq 1, a, b \in \mathbb{Z}\} \text{ where } r^n = s^2 = id \text{ and } sr = r^{-1}s$$

Suppose $n \geq 3$. How many elements x are there in D_n satisfying $x^2 = id$?

There are two cases:

- If $x = r^a$ for some $0 \leq a \leq n-1$, then $id = x^2 = r^{2a}$ implies $2a = 0$ or $2a = n$. Hence, if n is odd then there is only one option, and if n is even there are two options.

- If $x = r^a s$ for some $0 \leq a \leq n-1$, then $x^2 = r^a s r^a s = r^a r^{-1} s r^{a-1} s = ... = r^a r^{-a} s s = id$.

As a result, if n is odd then there are $n+1$ elements, and if n is even then there are $n+2$ elements.

PS 12

December 19, Wednesday

Definition 1: Let G be a group. If G is finite then the ***order*** of G is the number of elements in it. Also if G is infinite, we say G has ***infinite order***.

Definition 2: Let G be a group and $x \in G$. If $x^n \neq id$ for all positive integer n, we say x has ***infinite order***, and if $x^n = id$ for some positive integer n, we say x has a ***finite order***. Moreover, in the latter case, the smallest positive integer m satisfying $x^m = id$ is called the ***order of x***.

Definition 3: Let $(G, *)$ be a group and H be a subset of G. We say H is a ***subgroup*** of G if H itself forms a group under the operation $*$, and denote by $H < G$.

Definition 4: Let G be a group and $x \in G$. The subgroup $\prec x \succ = \{x^m : m \in \mathbb{Z}\}$ of G is called as ***subgroup generated by x***. If $G = \prec x \succ$ for some $x \in G$, we say G is a ***cyclic group***.

Problem 1 Let $G = \{x \in \mathbb{Q} : 0 \leq x < 1\}$. Define the operation on G as

$$a * b = \begin{cases} a + b & \text{if } a + b < 1 \\ a + b - 1 & \text{if } a + b \geq 1 \end{cases}$$

Prove that $(G, *)$ is a group with infinite order. Also show that for any $x \in G$, x has a finite order.

Observe that $a_1 * a_2 * ... * a_n = \lfloor a_1 + a_2 + ... + a_n \rfloor$ for any $a_1, a_2, ..., a_n \in G$. Since the usual addition is associative, the operation $*$ is associative on G. On the other hand, clearly 0 is the identity element. Moreover, for any $x \neq 0$, $1 - x$ is the unique inverse of x. Therefore, $(G, *)$ is a group with infinite order. Finally, for any $x \in G$, since x is a rational number we can write $x = \frac{p}{q}$ for some natural numbers p and q. From the definition of $*$, we have $x^q = \lfloor q \cdot \frac{p}{q} \rfloor = \lfloor p \rfloor = 0$. Hence x has a finite order (namely q).

Problem 2 *(Subgroup Criteria)* Let G be a group and H be a nonempty subset of G. Prove that H is a subgroup of G if and only if $xy^{-1} \in H$ for all $x, y \in H$.

($\Rightarrow$) Suppose H is a subgroup of G. Then for any $x, y \in H$, we have $y^{-1} \in H$ since H is closed under taking inverse and then $xy^{-1} \in H$ since the operation of G is binary.
($\Leftarrow$) Suppose $xy^{-1} \in H$ for all $x, y \in H$.

- Since H is nonempty, we can take an element $a \in H$. Then by choosing $x = y = a$, we get $aa^{-1} = id \in H$.
- For any $h \in H$, by choosing $x = id, y = h$, we get $id \cdot h^{-1} = h^{-1} \in H$.
- For any $h_1, h_2 \in H$, we know $h_2^{-1} \in H$, and then by choosing $x = h_1, y = h_2^{-1}$, we get $h_1 \cdot (h_2^{-1})^{-1} = h_1 h_2 \in H$.

Problem 3 Let G be a group, H and K be subgroups of G. Prove that $H \cap K$ is a subgroup of G.

Let $u, v \in H \cap K$. We must show that $uv^{-1} \in H \cap K$. Firstly, we have $u, v \in H$ and $u, v \in K$. Moreover, since H and K are subgroups of G, we have $u^{-1}, v^{-1} \in H$ and $u^{-1}, v^{-1} \in K$. This implies $uv^{-1} \in H$ and $uv^{-1} \in K$, hence the result follows.

Lagrange's Theorem: Let G be a finite group and $H < G$. Prove that order of G is divisible by order of H.

Problem 4 Let G be a group with n elements and $x \in G$. Prove that $x^n = id$.

Consider the subgroup generated by x. Since all elements of this subgroup are inside in G, we get $\prec x \succ$ is finite, too. Hence x has finite order, say k. Then we get $\prec x \succ = \{id, x, x^2, ..., x^{k-1}\}$. Hence, from Lagrange's theorem, we have n is divisible by k, say $n = km$ with $m \in \mathbb{N}$. Then, $x^n = x^{km} = id^m = id$.

Problem 5 Let G be group with p elements where p is a prime. Show that G is cyclic.

Since $p > 1$, there exists an element $x \in G$ with $x \neq id$. Let k be the number of elements in the subgroup generated by x. Since $x \neq id$, we have $k > 1$ and from Lagrange's theorem p is divisible by k. Since p is prime we get $p = k$, which implies $\prec x \succ = G$ and so G is cyclic.

2 Homeworks

Homework 1

October 23, Tuesday

Problem 1 Determine when the statement $(R \wedge S) \Rightarrow [P \Rightarrow (\sim Q \vee S)]$ is true by using the truth table.

P	Q	R	S	$R \wedge S$	$(\sim Q \vee S)$	$P \Rightarrow (\sim Q \vee S)$	$(R \wedge S) \Rightarrow [P \Rightarrow (\sim Q \vee S)]$
T	T	T	T	T	T	T	T
T	T	F	T	F	T	T	T
T	F	T	T	T	T	T	T
T	F	F	T	F	T	T	T
F	T	T	T	T	T	T	T
F	T	F	T	F	T	T	T
F	F	T	T	T	T	T	T
F	F	F	T	F	T	T	T
T	T	T	F	F	F	F	T
T	T	F	F	F	F	F	T
T	F	T	F	F	T	T	T
T	F	F	F	F	T	T	T
F	T	T	F	F	F	T	T
F	T	F	F	F	F	T	T
F	F	T	F	F	T	T	T
F	F	F	F	F	T	T	T

Hence the statement is always true.

Problem 2 Show that the followings are tautologies:

(a) $[(P \Rightarrow Q) \wedge \sim Q] \Rightarrow \sim P$

$$\begin{aligned}
[(P \Rightarrow Q) \wedge \sim Q] \Rightarrow \sim P &\equiv [(\sim P \vee Q) \wedge \sim Q] \Rightarrow \sim P \ \textit{(def. of cond. statement)} \\
&\equiv [(\sim P \wedge \sim Q) \vee (Q \wedge \sim Q)] \Rightarrow \sim P \ \textit{(distributive rule)} \\
&\equiv (\sim P \wedge \sim Q) \Rightarrow \sim P \ \textit{(since } Q \wedge \sim Q \textit{ is false)} \\
&\equiv \sim (\sim P \wedge \sim Q) \vee \sim P \ \textit{(def. of cond. statement)} \\
&\equiv (P \vee Q) \vee \sim P \ \textit{(negation rule)} \\
&\equiv P \vee Q \vee \sim P \ \textit{(associativity)} \\
&\equiv Q \vee (P \vee \sim P) \ \textit{(commutativity)} \\
&\equiv Q \vee \textit{(tautology)} \equiv \textit{(tautology)}
\end{aligned}$$

(b) $[\sim (P \Leftrightarrow Q)] \Leftrightarrow (\sim P \Leftrightarrow Q)$

$$\begin{aligned}
\sim (P \Leftrightarrow Q) &\equiv \sim [(P \Rightarrow Q) \wedge (Q \Rightarrow P)] \ \textit{(def. of biconditional)} \\
&\equiv \sim [(\sim P \vee Q) \wedge (\sim Q \vee P)] \ \textit{(def. of conditional)} \\
&\equiv [\sim (\sim P \vee Q)] \vee [\sim (\sim Q \vee P)] \ \textit{(negation rule)} \\
&\equiv (P \wedge \sim Q) \vee (Q \wedge \sim P) \ \textit{(negation rule)} \\
&\equiv [P \vee (Q \wedge \sim P)] \wedge [\sim Q \vee (Q \wedge \sim P)] \ \textit{(distributive law)} \\
&\equiv [(P \vee Q) \wedge (P \vee \sim P)] \wedge [(\sim Q \vee Q) \wedge (\sim Q \vee \sim P)] \ \textit{(dist. law)} \\
&\equiv [(P \vee Q) \wedge (\textit{tautology})] \wedge [(\textit{tautology}) \wedge (\sim Q \vee \sim P)] \\
&\equiv (P \vee Q) \wedge (\sim Q \vee \sim P) \\
&\equiv (\sim P \Rightarrow Q) \wedge (Q \Rightarrow \sim P) \ \textit{(def. of conditional)} \\
&\equiv (\sim P \Leftrightarrow Q) \ \textit{(def. of biconditional)}
\end{aligned}$$

As a result $\sim (P \Leftrightarrow Q) \equiv (\sim P \Leftrightarrow Q)$. Therefore $[\sim (P \Leftrightarrow Q)] \Leftrightarrow (\sim P \Leftrightarrow Q)$ is a tautology.

Problem 3 Let $A = \{1, 2, 3\}$. Determine the truth value of each of the following statements:

(a) $(\exists x \in A)(\forall y \in A)(x^2 < y + 1)$

TRUE Choose $x = 1$. Then for all $y \in A$ we have $1 < y + 1$.

(b) $(\forall x \in A)(\exists y \in A)(x^2 + y^2 < 12)$

TRUE For all $x \in A$, if we choose $y = 1$ then we have $x^2 + 1 < 12$.

(c) $(\forall x \in A)(\forall y \in A)(x^2 + y^2 < 12)$

FALSE If $x = 3$ and $y = 3$, then we have $x^2 + y^2 \geq 12$.

(d) $(\exists x \in A)(\forall y \in A)(\exists z \in A)(x^2 + y^2 < 2z^2)$

TRUE Choose $x = 1$. Then for any $y \in A$, we can choose $z = 3$ so that $1 + y^2 < 18$.

(e) $(\exists x \in A)(\exists y \in A)(\forall z \in A)(x^2 + y^2 < 2z^2)$

FALSE If the statement is true, then by choosing $z = 1$, we must find $x, y \in A$ such that $x^2 + y^2 < 2$, which is clearly false.

Problem 4 Write the negation of $(\forall x)[x \neq 0 \Rightarrow (x^2 > 0)]$.

$$\exists x(x \neq 0 \wedge (x^2 \leq 0))$$

Problem 5 A function f is continuous at the point $a \in \mathbb{R}$ if the following condition holds: For every $\epsilon > 0$ there is a number $\delta > 0$ such that $|f(x) - f(a)| < \epsilon$ whenever $|x - a| < \delta$.

(a) Write the condition abbreviated form, using quantifiers.

$$\forall \epsilon > 0, \exists \delta > 0, \forall x(|x - a| < \delta \Rightarrow |f(x) - f(a)| < \epsilon)$$

(b) Write the negation of this condition in a quantified form, using no negation symbols.

$$\exists \epsilon > 0, \forall \delta > 0, \exists x(|x - a| < \delta \wedge |f(x) - f(a)| \geq \epsilon)$$

Problem 6 Let p be a prime number. Prove that $\sqrt{p}$ is irrational.

Assume the contrary, say $\sqrt{p}$ is rational for some prime number p. Then we can find two natural numbers a and b satisfying $\sqrt{p} = \frac{a}{b}$. Moreover, without loss of generality, we can assume that a and b are relatively prime.

If $\sqrt{p} = \frac{a}{b}$, then we have $a^2 = p \cdot b^2$. Since $p|a^2$ and p is prime, we can conclude that $p|a$. Hence there exists a natural number k such that $a = p \cdot k$. Now, $a^2 = p \cdot b^2$ leads $p^2 \cdot k^2 = p \cdot b^2$, which implies $p \cdot k^2 = b^2$. From the last equality we have $p|b^2$ and by using p being prime we can say that $p|b$.

As a result, we found that p divides both of a and b, which contradicts with the assumption a and b are relatively prime. Therefore, $\sqrt{p}$ is irrational for any prime p.

Problem 7 Prove that there is a digit that appears infinitely often in the decimal expansion of $\sqrt{7}$.

Assume the contrary. Then all digits must appear finitely often in the decimal expansion of $\sqrt{7}$. Observe that the sum of finitely many finite numbers will be finite. Hence $\sqrt{7}$ contains finitely many digits in its decimal expansion since there are only finitely many (ten) digits.

However, if there are finitely many numbers (say m times) in the decimal expansion of a number r, then r can be represented as $\frac{s}{10^r}$ for some integer s. Therefore we can conclude that $\sqrt{7}$ is rational, which contradicts with the statement proved in the previous question.

Problem 8 Prove that for every integer $n \geq 1$, we have $1^3 + 2^3 + ... + n^3 = (1 + 2 + ... + n)^2$.

We will prove the statement by induction on n.

Base Case: For $n = 1$, we need $1^3 = 1^2$, which is clearly true.

Induction Hypothesis: Assume the claim holds for $n = k$, in other words assume $1^3 + 2^3 + ... + k^3 = (1 + 2 + ... + k)^2$ for some natural number $k \geq 1$.

Induction Step: We must show $1^3 + 2^3 + ... + k^3 + (k+1)^3 = (1+2+...+k+(k+1))^2$. From induction hypothesis we have $1^3+2^3+...+k^3+(k+1)^3 = (1+2+...+k)^2+(k+1)^3$. On the other hand, we know $1+2+...+s = \frac{s(s+1)}{2}$ for any natural number s (from the class). Hence $1^3+2^3+...+k^3+(k+1)^3 = 1+2+...+k)^2+(k+1)^3 = (\frac{k(k+1)}{2})^2+(k+1)^3$. Now, $(\frac{k(k+1)}{2})^2+(k+1)^3 = (k+1)^2 \cdot (\frac{k^2}{4}+k+1) = (k+1)^2 \cdot (\frac{k^2+4k+4}{4}) = (k+1)^2 \cdot \frac{(k+2)^2}{4} = (\frac{(k+1)(k+2)}{2})^2 = (1 + 2 + ... + k + (k + 1))^2$ and we are done.

Problem 9 Let a, b, c, d be positive real numbers. Prove that $(a^2 + b^2)(c^2 + d^2) \geq (ac + bd)^2$.

$$\begin{aligned}
(a^2 + b^2)(c^2 + d^2) \geq (ac + bd)^2 \quad &\Leftrightarrow \quad a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \geq a^2c^2 + b^2d^2 + 2abcd \\
&\Leftrightarrow \quad a^2d^2 + b^2c^2 \geq 2abcd \\
&\Leftrightarrow \quad a^2d^2 + b^2c^2 - 2abcd \geq 0 \\
&\Leftrightarrow \quad (ad - bc)^2 \geq 0 \ \textit{(which is clearly true)}
\end{aligned}$$

Problem 10 Prove that for every integer $n \geq 0$, $4^{2n+1} + 3^{n+2}$ is a multiple of 13.

We will prove the statement by induction on n.

Base Case: For $n = 0$, we need $4^1 + 3^2$ is a multiple of 13, which is clearly true.

Induction Hypothesis: Assume the claim holds for $n = k$, in other words assume $4^{2k+1} + 3^{k+2}$ is a multiple of 13 for some natural number $k \geq 0$.

Induction Step: We must show $4^{2(k+1)+1} + 3^{(k+1)+2}$ is a multiple of 13. Observe that $4^{2(k+1)+1} + 3^{(k+1)+2} = 4^{2k+3} + 3^{k+3} = 16 \cdot 4^{2k+1} + 3 \cdot 3^{k+2} = 16 \cdot (4^{2k+1} + 3^{k+2}) - 13 \cdot 3^{k+2}$. From induction hypothesis, we know $4^{2k+1} + 3^{k+2}$ is divisible by 13 and trivially $13 \cdot 3^{k+2}$ is a multiple of 13. Clearly, if two integers are divisible by 13, then their difference will be divisible by 13, too. Hence $4^{2(k+1)+1} + 3^{(k+1)+2}$ is a multiple of 13 and we are done.

Homework 2

October 31, Wednesday

Problem 1 Let A be a set and let $\{B_i\}_{i\in I}$ be an indexed family of sets. Prove or disprove:

(a) $A - \bigcap_{i\in I} B_i = \bigcup_{i\in I}(A - B_i)$

TRUE

$$\begin{aligned} x \in A - \bigcap_{i\in I} B_i &\Leftrightarrow x \in A \wedge \sim (\forall i \in I(x \in B_i)) \\ &\Leftrightarrow x \in A \wedge (\exists i \in I(x \notin B_i)) \\ &\Leftrightarrow \exists i \in I(x \in A \wedge x \notin B_i) \\ &\Leftrightarrow x \in \bigcup_{i\in I}(A - B_i) \end{aligned}$$

(b) $A - \bigcup_{i\in I} B_i = \bigcap_{i\in I}(A - B_i)$

TRUE

$$\begin{aligned} x \in A - \bigcup_{i\in I} B_i &\Leftrightarrow x \in A \wedge \sim (\exists i \in I(x \in B_i)) \\ &\Leftrightarrow x \in A \wedge (\forall i \in I(x \notin B_i)) \\ &\Leftrightarrow \forall i \in I(x \in A \wedge x \notin B_i) \\ &\Leftrightarrow x \in \bigcap_{i\in I}(A - B_i) \end{aligned}$$

Problem 2 Express the following relations and their negations for the sets A, B and C in terms of quantifiers and logical connectives.

(a) $A \cap B \neq \emptyset$

Statement: $\exists x(x \in A \wedge x \in B)$
Negation: $\forall x(x \notin A \vee x \notin B)$

(b) $A \cup B = C$

Statement: $\forall x((x \in A \vee x \in B) \Leftrightarrow x \in C)$
Negation: $\exists x[((x \in A \vee x \in B) \wedge x \notin C) \vee ((x \notin A \wedge x \notin B) \wedge x \in C)]$

Problem 3 Let X, Y and Z be sets. If $X \cap Y = X \cap Z$ and $X \cup Y = X \cup Z$, then show that $Y = Z$.

We will show that $Y \subseteq Z$ and $Z \subseteq Y$.

- ($Y \subseteq Z$) Take an arbitrary element y from Y. There are two cases:

  1. If $y \in X$, then we have $y \in X \cap Y$. Then from the first equality we get $y \in X \cap Z$, which implies $y \in Z$.
  2. If $y \notin X$, then from the second equality $y \in X \cup Y$ gives us $y \in X \cup Z$. Since $y \notin X$ and $y \in X \cup Z$, we can get $y \in Z$.

  In both cases we have $y \in Z$, which implies $Y \subseteq Z$.

- ($Z \subseteq Y$) Take an arbitrary element z from Z. There are two cases:

  1. If $z \in X$, then we have $z \in X \cap Z$. Then from the first equality we get $Z \in X \cap Y$, which implies $z \in Y$.
  2. If $z \notin X$, then from the second equality $z \in X \cup Z$ gives us $z \in X \cup Y$. Since $z \notin X$ and $z \in X \cup Y$, we can get $z \in Y$.

  In both cases we have $z \in Y$, which implies $Z \subseteq Y$.

Problem 4 Let $\{A_i\}_{i \in I}$ and $\{B_i\}_{i \in I}$ be indexed family of sets. Prove or disprove:

$$(\bigcup_{i \in I} A_i) \bigcap (\bigcup_{i \in I} B_i) \subseteq \bigcup_{i \in I} (A_i \cap B_i)$$

FALSE Let $A_1 = B_2 = \{a, b\}$ and $A_2 = B_1 = \{c, d\}$ where $I = \{1, 2\}$. Hence $(\bigcup_{i \in I} A_i) \bigcap (\bigcup_{i \in I} B_i) = \{a, b, c, d\} \bigcap \{a, b, c, d\} = \{a, b, c, d\}$. On the other hand, $\bigcup_{i \in I}(A_i \cap B_i) = (\{a, b\} \cap \{c, d\}) \bigcup (\{a, b\} \cap \{c, d\}) = \emptyset \cup \emptyset = \emptyset$. Hence if the statement is true, then we would have $\{a, b, c, d\} \subseteq \emptyset$ and so the result follows.

Problem 5 Show the equality $A = (A \backslash B) \cup (A \backslash C) \cup (A \cap B \cap C)$.

Observe $(A \backslash B) \subseteq A$, $(A \backslash C) \subseteq A$ and $(A \cap B \cap C) \subseteq A$. Since all three sets are subsets of A, their union must be a subset of A. Hence $(A \backslash B) \cup (A \backslash C) \cup (A \cap B \cap C) \subseteq A$. Now we must show that $A \subseteq (A \backslash B) \cup (A \backslash C) \cup (A \cap B \cap C)$.

Take an arbitrary element a from A and assume the contrary. In other words, assume $a \notin (A \backslash B) \cup (A \backslash C) \cup (A \cap B \cap C)$. Then we have $a \notin A \backslash B$, $a \notin A \backslash C$ and $a \notin A \cap B \cap C$. Since $a \notin A \backslash B$, we get $\sim (a \in A \wedge a \notin B) \equiv a \notin A \vee a \in B$. However, we know $a \in A$, so we get $a \in B$. Similarly, $a \notin A \backslash C$ gives us $a \in C$. As a result, we have $a \in A$, $a \in B$ and $a \in C$, which contradicts with $a \notin A \cap B \cap C$. Therefore, $A \subseteq (A \backslash B) \cup (A \backslash C) \cup (A \cap B \cap C)$ and the result follows.

Problem 6 Find nonempty sets A, B, C and D satisfying

$$(A \cup B) \cap (C \cup D) \neq (A \cap C) \cup (B \cap D)$$

Let $A = D = \{a, b\}$ and $B = C = \{c, d\}$. Observe that $A \cup B = C \cup D = \{a, b, c, d\}$ and $A \cap C = B \cap D = \emptyset$. Then, $(A \cup B) \cap (C \cup D) = \{a, b, c, d\} \neq \emptyset = (A \cap C) \cup (B \cap D)$.

Problem 7 If the union of power sets of A and B are equal to the power set of $A \cup B$, then prove that either $A \subseteq B$ or $B \subseteq A$.

Let $\rho(X)$ be the power set of X for any set X. Suppose $\rho(A) \cup \rho(B) = \rho(A \cup B)$. Since $A \cup B \subseteq A \cup B$, we have $A \cup B \in \rho(A \cup B)$. Then we get $A \cup B \in \rho(A) \cup \rho(B)$ from the equality $\rho(A) \cup \rho(B) = \rho(A \cup B)$. Hence either $A \cup B \in \rho(A)$ or $A \cup B \in \rho(A)$. On the other hand, we know $A \subseteq A \cup B$ and $B \subseteq A \cup B$. There are two cases:

- If $A \cup B \in \rho(A)$, then $A \cup B \subseteq A$ and this gives $B \subseteq A \cup B \subseteq A$.
- If $A \cup B \in \rho(B)$, then $A \cup B \subseteq B$ and this gives $A \subseteq A \cup B \subseteq B$.

As a result, either $A \subseteq B$ or $B \subseteq A$.

Homework 3

November 12, Monday

Problem 1 Let $A = \{a, b, c, d\}$. Find the number of equivalence relations on A having

(a) exactly 4 ordered pairs.

(b) exactly 5 ordered pairs.

(b) exactly 6 ordered pairs.

Let R be an equivalence relation on A. Since R is reflexive, we have $\{(a, a), (b, b), (c, c), (d, d)\} \subseteq R$.

(a) If R contains exactly four pairs, R must be equal to $\{(a, a), (b, b), (c, c), (d, d)\}$. Hence there is only **one** equivalence relation containing exactly 4 ordered pairs.

(b) If R contains exactly four pairs, then there must be a pair (x, y) with $x \neq y$. On the other hand, since R is symmetric we must have $(y, x) \in R$, which is a contradiction. As a result, there are **no** equivalence relation containing exactly 5 ordered pairs.

(c) By a similar reasoning with part (b), we have only two pairs (x, y) and (y, x) other than $\{(a, a), (b, b), (c, c), (d, d)\}$. Hence we must choose two element from $\{a, b, c, d\}$. Therefore, there are **six** equivalence relations containing exactly 6 ordered pairs.

Problem 2 Suppose A, B, C, and D are sets. Prove or disprove:

(a) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$

TRUE Observe that elements of $(A \times B) \cup (C \times D)$ are ordered pairs. Take an element from left hand side, say $(x, y) \in (A \times B) \cup (C \times D)$. Then we have either $(x, y) \in A \times B$ or $(x, y) \in C \times D$, and we must show that $(x, y) \in (A \cup C) \times (B \cup D)$.

If $(x, y) \in A \times B$, then we have $x \in A$ and $y \in B$. Since $A \subseteq A \cup C$ and $B \subseteq B \cup D$, we can say $x \in A \cup C$ and $y \in B \cup D$ and so $(x, y) \in (A \cup C) \times (B \cup D)$.

Similarly, if $(x, y) \in C \times D$ then we have $x \in C$ and $y \in D$. Again we have $C \subseteq A \cup C$ and $D \subseteq B \cup D$, then we can say $x \in A \cup C$ and $y \in B \cup D$. As a result $(x, y) \in (A \cup C) \times (B \cup D)$.

(b) $(A \cup C) \times (B \cup D) \subseteq (A \times B) \cup (C \times D)$

FALSE Take an element $(x, y) \in (A \cup C) \times (B \cup D)$. Hence we have $x \in A \cup C$ and $y \in B \cup D$, and we must show either $(x, y) \in A \times B$ or $(x, y) \in C \cup D$. Therefore we need either $(x \in A \wedge y \in B)$ or $(x \in C \wedge y \in D)$. However, we can have $(x \in A \wedge y \in D)$ since this does not contradict with $x \in A \cup C$ and $y \in B \cup D$. Then, let us try to build a counter example.

Let $A = \{1, 2\}$, $B = \{a\}$, $C = \{1\}$ and $D = \{a, b\}$. We will find an element in the left hand side which is not contained in the right hand side. Observe that $(2, b) \in (A \cup C) \times (B \cup D)$ since $2 \in A \cup C$ and $b \in B \cup D$, but $(2, b) \notin (A \times B) \cup (C \times D)$ because $(2, b) \notin A \times B$ since $b \notin B$ and $(2, b) \notin C \times D$ since $2 \notin C$.

(c) $A \times (B - C) = (A \times B) - (A \times C)$

TRUE The equality holds since for any pair (x, y), we have

$$\begin{aligned}
(x, y) \in \text{ R.H.S} &\Leftrightarrow [(x, y) \in A \times B] \wedge [(x, y) \notin A \times C] \\
&\Leftrightarrow (x \in A \wedge y \in B) \wedge (\sim (x \in A \wedge y \in C)) \\
&\Leftrightarrow (x \in A \wedge y \in B) \wedge (x \notin A \vee y \notin C) \\
&\Leftrightarrow [(x \in A \wedge y \in B) \wedge x \notin A] \vee [(x \in A \wedge y \in B) \wedge y \notin C] \\
&\Leftrightarrow [x \in A \wedge x \notin A \wedge y \in B] \vee [x \in A \wedge y \in B \wedge y \notin C] \\
&\Leftrightarrow [\mathit{contradiction}] \vee [x \in A \wedge y \in B \wedge y \notin C] \\
&\Leftrightarrow x \in A \wedge y \in B \wedge y \notin C \\
&\Leftrightarrow (x \in A) \wedge (y \in B \wedge y \notin C) \\
&\Leftrightarrow x \in A \wedge y \in (B - C) \\
&\Leftrightarrow (x, y) \in A \times (B - C) \\
&\Leftrightarrow (x, y) \in \text{ L.H.S.}
\end{aligned}$$

(d) $(A \times B) - (C \times D) = [A \times (B - D)] \cup [(A - C) \times B]$

TRUE The equality holds since for any pair (x, y), we have

$$\begin{aligned}
(x, y) \in \text{ L.H.S.} &\Leftrightarrow ((x, y) \in A \times B) \wedge ((x, y) \notin C \times D) \\
&\Leftrightarrow (x \in A \wedge y \in B) \wedge (\sim (x \in C \wedge y \in D)) \\
&\Leftrightarrow (x \in A \wedge y \in B) \wedge (x \notin C \vee y \notin D) \\
&\Leftrightarrow [(x \in A \wedge y \in B) \wedge (y \notin D)] \vee [(x \in A \wedge y \in B) \wedge (x \notin C)] \\
&\Leftrightarrow [x \in A \wedge y \in B \wedge y \notin D] \vee [x \in A \wedge y \in B \wedge x \notin C] \\
&\Leftrightarrow [(x \in A) \wedge (y \in B \wedge y \notin D)] \vee [(x \in A \wedge x \notin C) \wedge y \in B] \\
&\Leftrightarrow [(x, y) \in A \times (B - D)] \vee [(x, y) \in (A - C) \times B] \\
&\Leftrightarrow (x, y) \in \text{ R.H.S.}
\end{aligned}$$

(e) If $A \times B \subseteq C \times D$ then $A \subseteq C$ and $B \subseteq D$

> **FALSE** Suppose $A \times B \subseteq C \times D$. Take an element $a \in A$. We must show that $a \in C$. If we have an element $b \in B$ then we would have $(a, b) \in A \times B \subseteq C \times D$ and so $(a, b) \in C \times D$, which implies $a \in C$. Therefore we need an element in B to prove that $A \subseteq C$. However, the set B may be empty.
>
> Remember that $X \times \emptyset = \emptyset \times X = \emptyset$ for any set X. Therefore if we choose $B = \emptyset$, then $A \times B = \emptyset$ and so $A \times B \subseteq C \times D$ holds. However, we can choose $A = \{1, 2\}$ and $C = \{a, b\}$ so that $A \not\subseteq C$.

Problem 3 Let $X = \{\text{apple,cat,dog,banana,yellow,red,math,green,eleven,seven}\}$. Define $R = \{(x, y) \in X \times X : \text{there is at least one letter that occurs in both of the words } x \text{ and } y\}$. Determine whether R is reflexive, symmetric, and transitive.

> R ***is reflexive:*** Since every word has a common letter with itself, clearly R is reflexive.
>
> R ***is symmetric:*** If the words x and y have a common letter, then we can trivially say y and x has a common letter. Hence R is symmetric.
>
> R ***is not transitive:*** Observe that we have $(\text{cat}, \text{apple}) \in R$ and $(\text{apple}, \text{yellow}) \in R$. If R is transitive, then we would have $(\text{cat}, \text{yellow}) \in R$, which is false. Hence R is not transitive.

Problem 4 Suppose R_1 and R_2 are relations on a nonempty set A.

(a) If R_1 and R_2 are reflexive, must $R_1 \cup R_2$ be reflexive?

> **TRUE** For any $x \in A$, we have $(x, x) \in R_1 \subseteq R_1 \cup R_2$ since R_1 is reflexive. Hence $(x, x) \in R_1 \cup R_2$.

(b) If R_1 and R_2 are reflexive, must $R_1 \cap R_2$ be reflexive?

> **TRUE** For any $x \in A$, we have $(x, x) \in R_1$ and $(x, x) \in R_2$ since R_1 and R_2 are reflexive. Hence $(x, x) \in R_1 \cap R_2$.

(c) If R_1 and R_2 are reflexive, must $R_1 \backslash R_2$ be reflexive?

> **FALSE** For any $x \in A$, $(x, x) \in R_1 \backslash R_2$ implies $(x, x) \in R_1$ and $(x, x) \notin R_2$, which is clearly false since R_2 is reflexive. Hence, $R_1 \backslash R_2$ is not reflexive if R_1 and R_2 are reflexive.

(d) If R_1 and R_2 are symmetric, must $R_1 \cup R_2$ be symmetric?

> **TRUE** Suppose $(x, y) \in R_1 \cup R_2$ for some $x, y \in A$. Then either $(x, y) \in R_1$ or $(x, y) \in R_2$, and without loss of generality say $(x, y) \in R_1$. Since R_1 is symmetric we have $(y, x) \in R_1 \subseteq R_1 \cup R_2$. Hence $(y, x) \in R_1 \cup R_2$.

(e) If R_1 and R_2 are symmetric, must $R_1 \cap R_2$ be symmetric?

> **TRUE** Suppose $(x, y) \in R_1 \cap R_2$ for some $x, y \in A$. Then we have $(x, y) \in R_1$ and $(x, y) \in R_2$. Since R_1 and R_2 are symmetric, we have $(x, y) \in R_1 \Rightarrow (y, x) \in R_1$ and $(x, y) \in R_2 \Rightarrow (y, x) \in R_2$. Hence we have $(y, x) \in R_1 \cap R_2$.

(f) If R_1 and R_2 are symmetric, must $R_1 \backslash R_2$ be symmetric?

> **TRUE** Suppose $(x, y) \in R_1 \backslash R_2$ for some $x, y \in A$. Hence we have $(x, y) \in R_1$ and $(x, y) \notin R_2$. Since R_1 is symmetric we have $(y, x) \in R_1$. Moreover, if $(y, x) \in R_2$ then we would have $(y, x) \in R_2$ since R_2 is symmetric, which is false. Therefore, we have $(y, x) \notin R_2$ and $(y, x) \in R_1$, which implies $(y, x) \in R_1 \backslash R_2$.

(g) If R_1 and R_2 are transitive, must $R_1 \cup R_2$ be transitive?

> **FALSE** Let $A = \{1, 2, 3\}$, $R_1 = \{(1, 2)\}$ and $R_2 = \{(2, 3)\}$. Since each of R_1 and R_2 contains exactly one pair, they are transitive. On the other hand, $(1, 2), (2, 3) \in R_1 \cup R_2$, but $(1, 3) \notin R_1 \cup R_2$. As a result, $R_1 \cup R_2$ might not be transitive even if R_1 and R_2 are transitive.

(h) If R_1 and R_2 are transitive, must $R_1 \cap R_2$ be transitive?

> **TRUE** Suppose $(x, y) \in R_1 \cap R_2$, $(y, z) \in R_1 \cap R_2$. Then, $(x, y) \in R_1$, $(y, z) \in R_1$ give us $(x, z) \in R_1$ since R_1 is transitive, and $(x, y) \in R_2$, $(y, z) \in R_2$ give us $(x, z) \in R_2$ since R_2 is transitive. As a result, $(x, z) \in R_1 \cap R_2$.

(i) If R_1 and R_2 are transitive, must $R_1 \backslash R_2$ be transitive?

> **FALSE** Let $A = \{1, 2, 3\}$, $R_1 = \{(1, 2), (2, 3), (1, 3)\}$ and $R_2 = \{(1, 3)\}$. It can be easily seen that R_1 and R_2 are transitive, and $R_1 \backslash R_2 = \{(1, 2), (2, 3)\}$. However we have $(1, 2), (2, 3) \in R_1 \backslash R_2 \not\Rightarrow (1, 3) \in R_1 \backslash R_2$. Therefore $R_1 \backslash R_2$ might be not transitive even if R_1 and R_2 are transitive.

Problem 5 Suppose A is a nonempty set. Let $\mathcal{P}(A)$ be the power set of A and $\mathcal{F} \subseteq \mathcal{P}(A)$. Define $R = \{(a,b) \in A \times A : \forall X \subseteq A \backslash \{a,b\}(X \cup \{a\} \in \mathcal{F} \Rightarrow X \cup \{b\} \in \mathcal{F})\}$. Show that R is transitive.

Let $(a,b) \in R$ and $(b,c) \in R$ for some $a,b,c \in A$. We must show that $(a,c) \in R$. Take a set $X \subseteq A \backslash \{a,c\}$. We need $X \cup \{a\} \in \mathcal{F} \Rightarrow X \cup \{c\} \in \mathcal{F}$. Then assume $X \cup \{a\} \in \mathcal{F}$ and we must conclude that $X \cup \{c\} \in \mathcal{F}$. Notice that $a \notin X$ and $c \notin X$.

If $b \in X$, then consider $Y = \{c\} \cup (X \backslash \{b\})$ and $Z = \{a\} \cup (X \backslash \{b\})$.
Since $Z \subseteq A \backslash \{b,c\}$ and we know $(b,c) \in R$, we have $Z \cup \{b\} \in \mathcal{F} \Rightarrow Z \cup \{c\} \in \mathcal{F}$.
Also observe that $Z \cup \{b\} = X \cup \{a\}$ and we know $X \cup \{a\} \in \mathcal{F}$, hence $Z \cup \{c\} \in \mathcal{F}$.
Since $Y \subseteq A \backslash \{a,b\}$ and we know $(a,b) \in R$, we have $Y \cup \{a\} \in \mathcal{F} \Rightarrow Y \cup \{b\} \in \mathcal{F}$.
Moreover, we have $Z \cup \{c\} = Y \cup \{a\}$ and $Z \cup \{c\} \in \mathcal{F}$. Then we have $Y \cup \{b\} \in \mathcal{F}$.
On the other hand, since $Y \cup \{b\} = X \cup \{c\}$, we have $X \cup \{c\} \in \mathcal{F}$.

If $b \notin X$, then $X \subseteq A \backslash \{a,b\}$ and $(a,b) \in R$ give us $X \cup \{a\} \in \mathcal{F} \Rightarrow X \cup \{b\} \in \mathcal{F}$. Since $X \cup \{a\} \in \mathcal{F}$ is true, we have $X \cup \{b\} \in \mathcal{F}$. Similarly, $X \subseteq A \backslash \{b,c\}$ and $(b,c) \in R$ give us $X \cup \{b\} \in \mathcal{F} \Rightarrow X \cup \{c\} \in \mathcal{F}$ and we know $X \cup \{b\} \in \mathcal{F}$. As a result, $X \cup \{c\} \in \mathcal{F}$.

Problem 6 Let A and B be nonempty sets with $B \subseteq A$, and let $\mathcal{P}(A)$ be the power set of A. Define $R = \{(X,Y) \in \mathcal{P}(A) \times \mathcal{P}(A) : (X \backslash Y) \cup (Y \backslash X) \subseteq B\}$. Prove that R is an equivalence relation on $\mathcal{P}(A)$.

R is reflexive: For any $X \in \mathcal{P}(A)$, we have $(X \backslash X) \cup (X \backslash X) = \emptyset \cup \emptyset = \emptyset \subseteq B$. Hence $(X,X) \in R$ and so R is reflexive.

R is symmetric: If $(X,Y) \in R$ for some $X,Y \in \mathcal{P}(A)$, then $(X \backslash Y) \cup (Y \backslash X) \subseteq B$ and hence clearly $(Y \backslash X) \cup (X \backslash Y) = (X \backslash Y) \cup (Y \backslash X) \subseteq B$. Therefore, R is symmetric.

R is transitive: Suppose $(X \backslash Y) \cup (Y \backslash X) \subseteq B$ and $(Y \backslash Z) \cup (Z \backslash Y) \subseteq B$ for some $X,Y,Z \in \mathcal{P}(A)$. We must show $(X \backslash Z) \cup (Z \backslash X) \subseteq B$. Take an element $a \in (X \backslash Z) \cup (Z \backslash X)$ and we will prove that $a \in B$. Then either $a \in X \backslash Z$ or $a \in Z \backslash X$. In other words, we have either $(a \in X \wedge a \notin Z)$ or $(a \in Z \wedge a \notin X)$.

Suppose $(a \in X \wedge a \notin Z)$. If $a \in Y$, then $a \in Y \wedge a \notin Z$ implies $a \in Y \backslash Z$, and we know $Y \backslash Z \subseteq B$. Hence $a \in B$. If $a \notin Y$, then $a \in X \wedge a \notin Y$ implies $a \in X \backslash Y$, and we know $X \backslash Y \subseteq B$. Again, we have $a \in B$.

Suppose $(a \in Z \wedge a \notin X)$. If $a \in Y$, then $a \in Y \wedge a \notin X$ implies $a \in Y \backslash X$, and we know $Y \backslash X \subseteq B$. Hence $a \in B$. If $a \notin Y$, then $a \in Z \wedge a \notin Y$ implies $a \in Z \backslash Y$, and we know $Z \backslash Y \subseteq B$. Again, we have $a \in B$.

As a result, R is an equivalence relation.

Problem 7 Let A and B be nonempty sets. Suppose $\mathcal{F}$ is a partition of A and $\mathcal{G}$ is a partition of B. Define $\mathcal{H} = \{Z \subseteq A \times B : \exists X \in \mathcal{F}, \exists Y \in \mathcal{G}(Z = X \times Y)\}$. Prove that $\mathcal{H}$ is a partition of $A \times B$.

Let $\mathcal{H} = \{Z_i : i \in I\}$ for some index set I. We know that $\mathcal{H}$ is a partition of $A \times B$ if $\cup_{i \in I} Z_i = A \times B$ and $Z_i \cap Z_j \neq \emptyset \Rightarrow Z_i = Z_j$ for all $i, j \in I$..

- Take two sets Z_i and Z_j in $\mathcal{H}$ for some $i, j \in I$, and assume $Z_i \cap Z_j \neq \emptyset$. Then there exists $(a, b) \in Z_i \cap Z_j$. On the other hand, from the definition of $\mathcal{H}$, we have $Z_i = X \times Y$ for some $X \in \mathcal{F}$, $Y \in \mathcal{G}$, and $Z_j = U \times V$ for some $U \in \mathcal{F}$, $V \in \mathcal{G}$. Hence we have $(a, b) \in X \times Y$ and $(a, b) \in U \times V$, which implies $a \in X \cap U$ and $b \in V \cap Y$. Moreover, we know $\mathcal{F}$ is a partition for A and $X, U \in \mathcal{F}$. Since $a \in X \cap U$ and so $X \cap U \neq \emptyset$, we must have $X = U$. Similarly we can obtain $Y = V$, which implies $Z_i = X \times Y = U \times V = Z_j$.

- Let $(a, b) \in A \times B$. We must show that $(a, b) \in \mathcal{H}$, in other words we need $(a, b) \in Z_i$ for some $i \in I$. Observe that $\mathcal{F}$ is a partition for A and $a \in A$, so we can find $X \in \mathcal{F}$ satisfying $a \in X$. Similarly, $\mathcal{G}$ is a partition for B and $b \in B$, so we can find $Y \in \mathcal{G}$ satisfying $b \in Y$. Then from the definition of $\mathcal{H}$, we have $X \times Y \in \mathcal{F}$ and so $X \times Y = Z_i$ for some $i \in I$. As a result, $(a, b) \in \mathcal{H}$ and so $\mathcal{H}$ is a partition.

Problem 8 Let A, B, C, and D be subsets of the set X. Express $\chi_{(A \cup B) \cap (C \setminus D)}$ in terms of χ_A, χ_B, χ_C, and χ_D where χ_S denotes the characteristic function of the set S.

We know that $\chi_U(x) + \chi_{X \setminus U}(x) = 1$, $\chi_{U \cap V}(x) = \chi_U(x) \cdot \chi_V(x)$ and $\chi_{U \cup V}(x) = \chi_U(x) + \chi_V(x) - \chi_U(x) \cdot \chi_V(x)$ for any $U, V \subseteq X$ and $x \in X$. Hence
$\chi_{(A \cup B) \cap (C \setminus D)} = \chi_{A \cup B}(x) \cdot \chi_{C \setminus D}(x) = \chi_{A \cup B}(x) \cdot \chi_{C \cap (X \setminus D)}(x) = \chi_{A \cup B}(x) \cdot [\chi_C(x) \cdot \chi_{X \setminus D}(x)]$
$= \chi_{A \cup B}(x) \cdot \chi_C(x) \cdot \chi_{X \setminus D}(x) = [\chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x)] \cdot \chi_C(x) \cdot [1 - \chi_D(x)]$

Problem 9 Find nonempty sets A, B, C and functions $f : A \to B$ and $g : B \to C$ such that

(a) g is not injective but $g \circ f$ is injective.

Let $A = \{1\}$, $B = C = \{1, 2\}$, $f(1) = 1$, $g(1) = g(2) = 1$. Since the domain of $g \circ f$ contains exactly one element, trivially it is injective while g is not injective.

(b) f is not surjective but $g \circ f$ is surjective.

Let $A = B = \{1, 2\}$, $C = \{1\}$, $f(1) = f(2) = 1$, $g(1) = g(2) = 1$. Since the C is singleton, $g \circ f$ is surjective but $f(x) \neq 2$ for any $x \in A$.

Problem 10 Let $F = \{a, b, c, d, e\}$ and $G = \{1, 2, 3\}$. How many surjective functions are there from F to G?

Firstly observe that there are $3^5 = 243$ functions from F to G. Let $f : F \to G$ be function which is not surjective and $Im(f)$ denotes the values taken under the function f.

If f is a constant function, or $Im(f)$ contains exactly one element, then there are three possibilities. Suppose $Im(f)$ contains at least two elements. Also since f is not surjective, we know f cannot take three different values and hence the size of $Im(f)$ must be equal to 2. There are three cases, which are completely symmetric:

- $Im(f) = \{1, 2\}$
- $Im(f) = \{1, 3\}$
- $Im(f) = \{2, 3\}$

If $Im(f) = \{1, 2\}$, we have $2^5 - 2 = 30$ such functions since f can take two values, but we can exclude the cases that $f \equiv 1$ and $f \equiv 2$. Similarly, if $Im(f) = \{1, 3\}$ or $Im(f) = \{2, 3\}$ then we have 30 such functions.

As a result, there are $243 - 3 - 3 \cdot 30 = 150$ surjective functions.

Problem 11 Let $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be a function defined recursively as follows:
$f(1) = (1, 1)$ and if $f(k) = (a, b)$ then $f(k+1) = \begin{cases} (a-1, b+1) & \text{if } a > 1 \\ (b+1, 1) & \text{if } a = 1 \end{cases}$
Prove that f is surjective.

Suppose the function f is not surjective. Hence the following set is nonempty.

$$A = \{n \geq 2 : n = a + b \text{ for some } a, b \in \mathbb{N} \text{ such that } f(k) \neq (a, b) \text{ for all } k \in \mathbb{N}\}$$

Since A is a nonempty subset of natural numbers, it has a minimum element from well-ordering principle, say m. Observe that $f(1) = (1, 1)$, which implies $2 \notin A$ and so $m \geq 3$. Since $m - 1 \notin A$ due to the minimality, we can say there exist natural numbers a, b satisfying $f(k) = (a, b)$ for some $k \in \mathbb{N}$ with $a + b = m - 1$.

If $a > 1$ then we would get $f(k + 1) = (a - 1, b + 1)$ and observe that $(a - 1) + (b + 1) = m - 1$ again. Hence we can reduce a by one without changing the sum of the components, so we can assume that $a = 1$ (and then $b = m - 2$) without loss of generality.

Now if $f(k) = (1, m - 2)$ then we have $f(k + 1) = (m - 1, 1)$, which implies $m \notin A$ and therefore we have a contradiction. As a result, A is empty and so f is surjective.

Problem 12 Let $f(x) = x^2 + x + 1$ be a function on positive real numbers. Find the largest subset S of positive real numbers and a function g such that $(g \circ f)(x) = (f \circ g)(x) = x$ for all $x \in S$.

Observe that we must find the inverse of the function f with an appropriate domain. Since $f(x) = \frac{(2x+1)^2+3}{4}$, we can write $g(x) = \frac{\sqrt{4x-3}-1}{2}$.

Since the domain of f is set of positive real numbers, $2x + 1$ is always positive and hence there is no problem while taking square root. Then the only thing is to guarantee that $\frac{\sqrt{4x-3}-1}{2} > 0$, which simplified as $x > 1$ and clearly it is equivalent to say that the range of f is the interval $(1, \infty)$. As a result, $g(x) = \frac{\sqrt{4x-3}-1}{2}$ and $S = (1, \infty)$.

Problem 13 Define a relation $\sim$ on the set of integers as $x \sim y \Leftrightarrow x^2 - y^2$ is divisible by 6. Prove that $\sim$ is an equivalence relation and find the equivalence classes.

It can be easily seen that $(6|x^2 - x^2)$ for any $x \in \mathbb{Z}$, $(6|x^2 - y^2 \Leftrightarrow 6|y^2 - x^2)$ for all $x, y \in \mathbb{Z}$, and $(6|x^2 - y^2 \wedge 6|y^2 - z^2 \Rightarrow 6|x^2 - z^2)$ for all $x, y, z \in \mathbb{Z}$. Therefore R is an equivalence relation. On the other hand, we can write

$$6|x^2 - y^2 \Leftrightarrow 6|(x-y)(x+y) \Leftrightarrow 2|(x-y)(x+y) \wedge 3|(x-y)(x+y)$$

Moreover, $2|(x-y)(x+y)$ means that x and y have the same parity. As a result, $x \sim y$ if and only if they have the same parity and either $x - y$ or $x + y$ is divisible by 3. Hence there are four equivalence classes:

- $[1] = \{n \in \mathbb{Z} : n = 6k + 1$ or $n = 6k - 1$ for some integer k$\}$
- $[2] = \{n \in \mathbb{Z} : n = 6k + 2$ or $n = 6k - 2$ for some integer k$\}$
- $[3] = \{n \in \mathbb{Z} : n = 6k + 3$ for some integer k$\}$
- $[6] = \{n \in \mathbb{Z} : n = 6k$ for some integer k$\}$

Problem 14 Construct equivalence relations $\sim_1$ and $\sim_2$ on the set of natural numbers such that $1 \sim_1 2$, $2 \sim_1 7$, $1 \not\sim_2 7$ and $2 \not\sim_2 7$.

We know that any partition defines an equivalence relation. Then take $\Pi_1 = \{A, B\}$ and $\Pi_2 = \{B, C, D\}$ where $A = \{1, 2, 7\}$, $B = \mathbb{N} \backslash \{1, 2, 7\}$, $C = \{1, 2\}$, $D = \{7\}$. By using these partitions we can define natural equivalence relations:

$x \sim_1 y \Leftrightarrow$ they are in the same set with respect to Π_1 and
$x \sim_2 y \Leftrightarrow$ they are in the same set with respect to Π_2.

Then clearly we have $1 \sim_1 2$, $2 \sim_1 7$, $1 \not\sim_2 7$ and $2 \not\sim_2 7$.

Problem 15 Determine which of the following functions are injective, surjective or bijective.

(a) $a : [-\pi, \pi] \to \mathbb{R}$, $a(x) = \cos(x^3)$

a **is not injective:** Observe $a(-1) = a(1)$ since cos is an even function.

a **is not surjective:** Observe $\cos(x^3) \neq 2$ for any x.

Hence a **is not bijective** since it is not injective.

(b) $b : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $b(x, y) = 2^x 3^y$

b **is injective:** If $b(x_1, y_1) = b(x_2, y_2)$, in other words if $2^{x_1}3^{y_1} = 2^{x_2}3^{y_2}$ for some natural numbers x_1, x_2, y_1, y_2, then we have $2^{x_1-x_2} = 3^{y_2-y_1}$. Since the powers of 2 and 3 can be equal only if the powers are zero, we can say $x_1 = x_2$ and $y_1 = y_2$.

b **is not surjective:** Observe $b(x, y) \neq 5$ for all $x, y \in \mathbb{N}$.

Hence b **is not bijective** since it is not surjective.

(c) $c : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $c(x, y) = 2x + 3y$

c **is not injective:** Observe $c(0, 2) = c(3, 0)$.

c **is surjective:** Take $m \in \mathbb{Z}$. If m is odd then $c(\frac{m-3}{2}, 1) = m$, and if m is even then $c(\frac{m}{2}, 0) = m$.

Hence c **is not bijective** since it is not injective.

(d) $d : \mathbb{Q}\backslash\{2\} \to \mathbb{Q}\backslash\{3\}$, $d(x) = \frac{3x+1}{x-2}$

d **is injective:** Suppose $d(x) = d(y)$ for some $x, y \in \mathbb{Q}\backslash\{2\}$. Then $\frac{3x+1}{x-2} = \frac{3y+1}{y-2}$ implies $3xy + y - 6x - 2 = 3xy - 6y + x - 2$ and so $x = y$.

d **is surjective:** Take $x \in \mathbb{Q}\backslash\{3\}$. Then we need $u \in \mathbb{Q}\backslash\{2\}$ satisfying $\frac{3u+1}{u-2} = x$, which implies $3u + 1 = ux - 2x$. Then we have $u = \frac{2x+1}{x-3}$ and $x \neq 3$ implies there is a such rational number u.

Hence d **is bijective** since it is both injective and surjective.

Homework 4

December 21, Friday

Problem 1 Let $2 = 1'$, $3 = 2'$, $4 = 3'$, and $5 = 4'$. By using the definitions of addition and multiplication on natural numbers from Landau, prove the followings:

(a) $4 = 2 \cdot 2$

(b) $4 = 2 + 2$

(c) $(4 \cdot 2)' = 3 \cdot 3$

(d) $5' = 2 \cdot 3$

(e) $(3 \cdot 3)' = 2 \cdot 5$

Equalities trivially come from the definitions.

Problem 2 By using the definitions of addition and multiplication on rational numbers from Landau, prove that $P \cdot P + P + 1 = Q \cdot Q$ has no solution on rational numbers.

Let $a = N(P)$, $b = D(P)$, $c = N(Q)$, $d = D(Q)$. From the definition of multiplication, $(a^2, b^2) = (N(P \cdot P), D(P \cdot P))$ and $(c^2, d^2) = (N(Q \cdot Q), D(Q \cdot Q))$. On the other hand, $(a^2b + b^2a + b^3, b^3) \in P \cdot P + P + 1$ and we need to prove that $(a^2b + b^2a + b^3, b^3) \not\sim (c^2, d^2)$. Assume the contrary. Then we have the equality $(a^2b + b^2a + b^3) \cdot d^2 = b^3 \cdot c^2$. Hence $b(a^2d^2 + abd^2 + b^2d^2) = b(b^2c^2)$ implies $a^2d^2 + abd^2 + b^2d^2 = b^2c^2$. This clearly implies $(a^2 + ab + b^2, b^2) \sim (c^2, d^2)$. Since $N(Q \cdot Q) = c^2$ and $D(Q \cdot Q) = d^2$, we have $a^2 + ab + b^2 = kc^2$ and $b^2 = kd^2$ for some natural number $k \in \mathbb{N}$. Moreover, we can say $k > 1$ since otherwise we get $b = d$, which is impossible since $Q > 1$ clearly. Let R be the class of the pair (b, d). Then $N(R)d = D(R)b$ implies $(k, 1) \sim (N(R)^2, D(R)^2)$. Since $D(R \cdot R) = D(R)^2$ and $D(R)^2 \geq 1$, we get $1 = D(R \cdot R)$ and $k = N(R \cdot R) = N(R)^2$. Let $l = N(R)$. Hence we can write $b^2 = l^2d^2$ and so $b^2 = (dl)^2$, which implies $b = dl$. Then, $a^2 + adl + d^2l^2 = l^2c^2$ and then we get $l(ad + ld^2) < l(lc^2)$, in other words $ad + ld^2 < lc^2$. Then, there exists a natural number w with $lc^2 = ad + ld^2 + w$, which implies $wl = a^2$. Hence, $a^2d^2l = wld^2l = wd^2l^2 = wb^2$, this gives us $(a^2, b^2) \sim (w, d^2l)$. However, $a^2 = N(P \cdot P)$ and $b^2 = D(P \cdot P)$ imply $w = a^2y$ for some $y \in \mathbb{N}$. Finally this gives $a^2yl = a^2$ and so $y = l = 1$, hence $k = l^2 = 1$, which is a contradiction.

Problem 3 Remember that cuts correspond to the positive real numbers. State the cut corresponding to $\sqrt{3} + \sqrt{2} + 1$.

Observe that $\xi_1 = \{x \in \mathbb{Q} : x^2 < 3\}$, $\xi_2 = \{x \in \mathbb{Q} : x^2 < 2\}$ and $\xi_3 = \{x \in \mathbb{Q} : x < 1\}$ are cuts. From the definition of addition on cuts, we know $\nu = \{x + y : x \in \xi_1, y \in \xi_2\}$ and $\mu = \{u + v : u \in \nu, v \in \xi_3\}$ are cuts, too. Clearly, μ corresponds to the real number $\sqrt{3} + \sqrt{2} + 1$.

Problem 4 Let ξ and ν be different cuts. Prove that either $\xi \subset \nu$ or $\nu \subset \xi$.

Since $\xi \neq \nu$, there exists an element x such that either $x \in \xi, x \notin \nu$ or $x \notin \xi, x \in \nu$. Without loss of generality, say $x \in \xi$ and $x \notin \nu$. Take any element $y \in \nu$. Since $x \notin \nu$ and $y \in \nu$, we have $y < x$. Hence, we get $x \in \xi$ because ξ is a cut with $x \in \xi$ and $y < x$. As a result, $y \in \nu$ implies $y \in \xi$ and then $\nu \subseteq \xi$. Finally, $x \notin \nu$ and $x \in \xi$ imply ν is a proper subset of ξ.

Problem 5 Let $\xi_n = \{x \in \mathbb{Q}^+ : x < \sum_{i=0}^{n} \frac{1}{n!}\}$ for a nonnegative integer n. Show that ξ_n is a cut for any n. Moreover, deduce that $e = \bigcup_{n \geq 0} \xi_n$ is a cut.

Let $r_n = \sum_{i=0}^{n} \frac{1}{n!}$ for any natural number n. Clearly, r_n is rational for all $n \in \mathbb{N}$. Moreover, ξ_n is nonempty since $1 \in \xi_n$, and it is a proper subset of rational numbers because all summands are less than or equal to 1 and so $n + 2 \notin \xi_n$. Moreover, if $x \in \xi_n$ and $u < x$, then $u \in \xi_n$ since $u < x$ and $x < r_n$ imply $u < x$. Also, for any $x \in \xi_n$, from $x < r_n$, we can find a rational number on the open interval (x, r_n), say q. Hence $q \in \xi_n$ implies there is no greatest element in ξ_n. As a result, ξ_n is a cut for any n.

Secondly, e is trivially nonempty. Also, it can be seen that $n! > 2^n$ for $n \geq 4$. Hence, $r_n < 1 + 1 + 2 + 6 + \sum_{i=4}^{\infty} \frac{1}{2^i} < 11$ implies $11 \notin e$. Therefore, e is a nonempty proper subset of rational numbers.

Let $x \in e$ and $u < x$. From the definition of the union, there exists a natural number n with $x \in \xi_n$. Then we have $u < x$ and $x \in \xi_n$, which clearly implies $u \in \xi_n$ and so $u \in e$. On the other hand, since x is not the greatest in xi_n, we have $y \in \xi_n$ with $x < y$. Again, from the definition, we have $y \in e$ and then x is not the greatest element in e. As a result, e is a cut.

Problem 6 Construct a bijection between $[2, 3]$ and $(7, 17)$.

Clearly $h \circ f \circ g$ is a bijection between $[2, 3]$ and $(7, 17)$ where:

- $g : [2, 3] \to [0, 1]$ given by $g(x) = x - 2$
- $f : [0, 1] \to (0, 1)$ given by $f(x) = \begin{cases} \frac{1}{2}, & \text{if } x = 0 \\ \frac{x}{2x+1}, & \text{if } \frac{1}{x} \in \mathbb{N} \\ x, & \text{otherwise} \end{cases}$
- $h : (0, 1) \to (7, 17)$ given by $h(x) = 10x + 7$

Problem 7 Let $A \subset B$ and B is a finite set. Prove that $\#A < \#B$.

Suppose A and B contain n and m elements, respectively. Since $A \subset B$, the identity function will be an injection from A to B and so $\#A \leq \#B$. Moreover, suppose f is a bijection from A to B. Since there are bijections $g : A \to \mathbb{N}_n$ and $h : B \to \mathbb{N}_m$, the function $h \circ f \circ g^{-1}$ would be a bijection between $\mathbb{N}_n$ and $\mathbb{N}_m$, which is a contradiction since $n \neq m$. As a result, there is no bijection between A and B and so $\#A < \#B$.

Problem 8 Let A be set containing 142857 elements. Let X and Y be the collections of subsets containing exactly 111111 and 31746 elements from A, respectively. By constructing a bijection, prove that $\#X = \#Y$.

Define the function $f : X \to \mathcal{P}(A)$ given by $f(S) = A \backslash S$ for any $S \in X$. Firstly, $A \backslash S \subseteq A$ and so f is well-defined. On the other hand, since A and S respectively contain 142857 and 111111 elements, we have $f(S)$ contains 31746 elements and then $f(S) \in Y$. Moreover, for any $T \in Y$, we have $A \backslash T$ contains 111111 elements and then $f(A \backslash T) = T$. Finally, if $f(S_1) = f(S_2)$, then we would have $A \backslash S_1 = A \backslash S_2$, which clearly implies $S_1 = S_2$. As a result, f is a bijection between X and Y, so we are done.

Problem 9 Let $A = \{(a, b) : a, b \in \mathbb{N} \text{ with } a + 1 = b\}$. Compare $\#A$ and $\#\mathbb{Q}^+$.

We know $\mathbb{Q}^+$ has the same cardinality with natural numbers. On the other hand, $f(a, b) = a$ is a bijection between A and $\mathbb{N}$. Hence $\#A = \#\mathbb{Q}^+$.

Problem 10 By using Schröder–Bernstein theorem, prove that A and B have the same cardinality where $A = [1, 2] \cup (5, 6]$ and $B = (1, 6)$.

The following two injections $f : A \to B$ and $g : B \to A$ complete the proof with Schröder–Bernstein theorem.

$$f(x) = \begin{cases} x + 1, & \text{if } x \in [1, 2] \\ x - 1, & \text{if } x \in (5, 6) \end{cases} \qquad g(x) = \frac{x + 12}{10}$$

3 Midterms

Q1	Q2	Q3	Q4	Q5	TOTAL
8 pts	12 pts	10 pts	10 pts	10 pts	50 pts

B U Department of Mathematics
Math 111

Date: October 23, 2018	Full Name : ANSWERS
Time: 17:00-18:30	Student ID No :

Fall 2018 First Midterm Exam

1. The exam consists of 5 questions some of which have multiple parts. **2.** Read each question carefully and put your answer neatly in the space provided. **3.** Show all your work. Explain your reasoning. Correct answers without supporting work will <u>not</u> get credit.

1. Find a formula involving only the connectives $\sim$ and $\wedge$ that has the following truth table:

P	Q	R	?
F	F	F	F
F	F	T	F
F	T	F	F
F	T	T	T
T	F	F	F
T	F	T	T
T	T	F	F
T	T	T	T

Observe that we must have a true statement only if

- P is false, Q is true, R is true OR
- P is true, Q is false, R is true OR
- P is true, Q is true, R is true.

Hence we have the formula $(\sim P \wedge Q \wedge R) \vee (P \wedge \sim Q \wedge R) \vee (P \wedge Q \wedge R)$.
Then by using De Morgan's laws,

$$\begin{aligned}
(\sim P \wedge Q \wedge R) \vee (P \wedge \sim Q \wedge R) \vee (P \wedge Q \wedge R) &\equiv [(\sim P \wedge Q) \vee (P \wedge \sim Q) \vee (P \wedge Q)] \wedge R \\
&\equiv [(\sim P \wedge Q) \vee (P \wedge (\sim Q \vee Q))] \wedge R \\
&\equiv [(\sim P \wedge Q) \vee (P \wedge (tautology))] \wedge R \\
&\equiv [(\sim P \wedge Q) \vee P] \wedge R \\
&\equiv [(\sim P \vee P) \wedge (Q \vee P)] \wedge R \\
&\equiv [(tautology) \wedge (Q \vee P)] \wedge R \\
&\equiv (Q \vee P) \wedge R \\
&\equiv \sim (\sim Q \wedge \sim P) \wedge R
\end{aligned}$$

Alternatively, even if it is not elegant, we can write

$$\sim [\sim (\sim P \wedge Q \wedge R) \wedge \sim (P \wedge \sim Q \wedge R) \wedge \sim (P \wedge Q \wedge R)]$$

2. Write the following statements using only quantifiers, logical connectors, numbers and basic arithmetic operations.

   (a) 5 is an odd integer.

   $\exists n \in \mathbb{Z}(5 = 2n + 1)$

   (b) There exists an even integer.

   $\exists n \in \mathbb{Z}, \exists m \in \mathbb{Z}(n = 2m)$

   (c) Any integer that is a multiple of 111, is also a multiple of 37.

   $\forall n \in \mathbb{Z}[\exists k \in \mathbb{Z}(n = 111k) \Rightarrow \exists k \in \mathbb{Z}(n = 37k)]$

   (d) Every natural number is either odd, or even, but not both.

   $\forall n \in \mathbb{N}[[\exists k \in \mathbb{Z}(n = 2k) \vee \exists k \in \mathbb{Z}(n = 2k+1)] \wedge \sim [\exists k \in \mathbb{Z}(n = 2k) \wedge \exists k \in \mathbb{Z}(n = 2k + 1)]]$

   (e) Every integer can be written as the sum of two integers, of which at least one is even and at most one is bigger than 3.

   $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, \exists z \in \mathbb{Z}(x = y + z \wedge (\exists k \in \mathbb{Z}(y = 2k) \vee \exists k \in \mathbb{Z}(z = 2k)) \wedge \sim (y > 3 \wedge z > 3))$

   (f) 1729 is the smallest natural number expressible as the sum of two cubes in two different ways.

   $[\exists a \in \mathbb{N}, \exists b \in \mathbb{N}, \exists c \in \mathbb{N}, \exists d \in \mathbb{N}(1729 = a^3 + b^3 \wedge 1729 = c^3 + d^3 \wedge \sim (a = c \wedge b = d) \wedge \sim (a = d \wedge b = c))] \wedge$

   $[\forall n \in \mathbb{N}(n < 1729 \Rightarrow ((\exists a \in \mathbb{N}, \exists b \in \mathbb{N}, \exists c \in \mathbb{N}, \exists d \in \mathbb{N}(n = a^3 + b^3 \wedge n = c^3 + d^3)) \Rightarrow ((a = c \wedge b = d) \vee (a = d \wedge b = c))))]$

3. Let m and n be integers. Prove that $m \cdot n$ is odd if and only if both m and n are odd.

($\Rightarrow$) Assume $m \cdot n$ is odd for some integers m and n. We must show that both m and n are odd. Assume the contrary. Then at least one of m and n would be even, and without loss of generality, say m is even. Then there exists an integer k satisfying $m = 2k$. Hence $m \cdot n = 2k \cdot n = 2 \cdot (kn)$ and so $m \cdot n$ is even, which is a contradiction. Therefore, if $m \cdot n$ is odd then both m and n are odd.

($\Leftarrow$) Assume both m and n are odd integers. We must show that $m \cdot n$ is odd. Since m is odd, we can find an integer k satisfying $m = 2k+1$. Similarly, since n is odd, we can find an integer r satisfying $n = 2r+1$. Then we can write $m \cdot n = (2k+1) \cdot (2r+1) = 4kr + 2k + 2r + 1 = 2 \cdot (2kr + k + r) + 1$, which is odd. Therefore, if both m and n are odd integers, then $m \cdot n$ is odd.

As a result, $m \cdot n$ is odd if and only if both m and n are odd integers.

4. (a) State the well-ordering principle.

   Every nonempty subset of natural numbers has a minimum element.

   (b) Using the well-ordering principle, prove that using only 5 kuruş and 3 kuruş coins you can pay every amount bigger than 7 kuruş.

   We must prove that for every natural number $n \geq 8$, we can find nonnegative integers a and b satisfying $n = 3a + 5b$.

   Suppose the claim is false. Then there exist some natural numbers $n \geq 8$ such that $n \neq 3a + 5b$ for all nonnegative integers a and b. Hence the following set A would be nonempty.

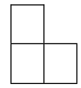
$$A = \{n \in \mathbb{N} : n \geq 8 \text{ and } n \neq 3a + 5b \text{ for all nonnegative integers } a \text{ and } b\}$$

   Since A is a nonempty subset of natural numbers, A has a minimum element by well-ordering principle, say k. Observe that $8 \notin A$ since $8 = 3 \cdot 1 + 5 \cdot 1$, $9 \notin A$ since $9 = 3 \cdot 3 + 5 \cdot 0$, and $10 \notin A$ since $10 = 3 \cdot 0 + 5 \cdot 2$. Hence $k \geq 11$.

   Due to the minimality of k, we can say $k - 3 \notin A$ and $k - 3 \geq 8$ implies there exist nonnegative integers a and b satisfying $k - 3 = 3a + 5b$. Then we can write $k = 3(a+1) + 5b$, which contradicts with $k \in A$.

   As a result, we can pay every amount bigger than 7 kuruş by using only 5 kuruş and 3 kuruş coins.

5. Show that for every natural number n, a figure that is obtained by removing one arbitrary square from a $2^n \times 2^n$ chessboard can be covered by L-shaped pieces:



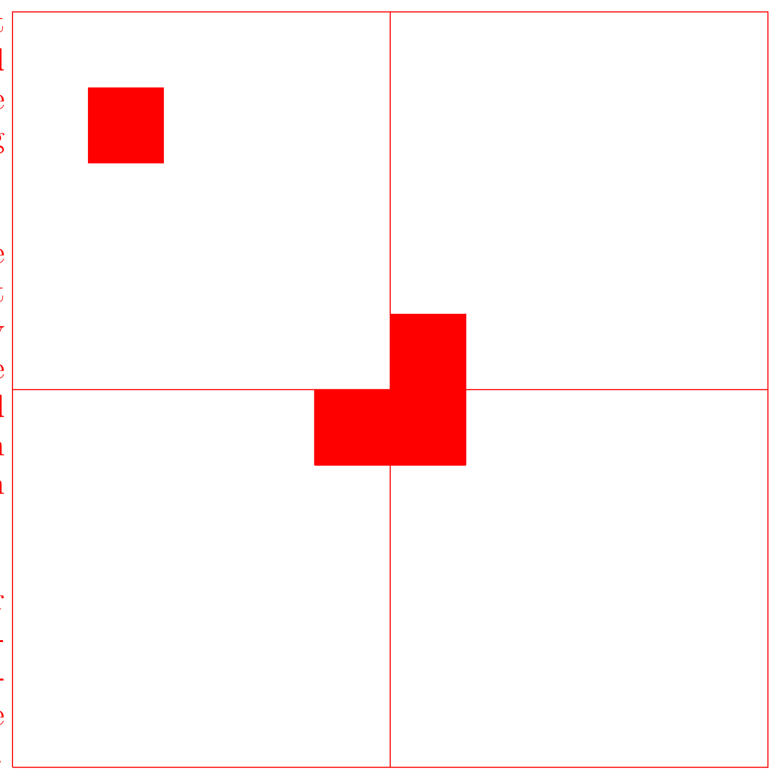
The L-shaped pieces should cover the whole chessboard except the removed square and should not overlap.

We will prove the claim by induction on n.

Base Case: If $n = 1$, then we have a 2×2 chessboard with one removed square. If we remove a square from 2×2 chessboard, we get exactly an L-shape. Trivially, we can cover this by using one L-shaped piece.

Induction Hypothesis: Suppose the claim holds for $n = k$. In other words, assume any $2^k \times 2^k$ chessboard with one arbitrary removed square can be covered by L-shaped pieces for some integer $k \geq 1$.

Induction Step: Take a $2^{k+1} \times 2^{k+1}$ chessboard with one arbitrary removed square. Then divide this $2^{k+1} \times 2^{k+1}$ chessboard into four $2^k \times 2^k$ chessboards as in the figure below where exactly one of those four chessboards has one removed square.



Without loss of generality, say the left upper $2^k \times 2^k$ chessboard has the removed one. From the induction hypothesis, we can cover this chessboard by using L-shaped pieces.

On the other hand, put an L-shaped piece as in the figure. Then, consider the right upper $2^k \times 2^k$ chessboard. Since exactly one square has already covered, the remaining figure is a $2^k \times 2^k$ chessboard with one removed square. Hence we can cover it by using L-shaped pieces from the induction hypothesis.

Similarly, the remaining parts of left lower and right lower chessboards can be covered. As a result, any $2^{k+1} \times 2^{k+1}$ chessboard with one arbitrary removed square can be covered by using L-shaped pieces.

Q1	Q2	Q3	Q4	Q5	Q6	Q7	TOTAL
6 pts	4 pts	4 pts	8 pts	9 pts	9 pts	10 pts	50 pts

B U Department of Mathematics
Math 111

Date: November 13, 2018	Full Name	: ANSWERS
Time: 17:00-18:30	Student ID No	:
	Math 111 No	:

Fall 2018 Second Midterm Exam

1. The exam consists of 5 questions some of which have multiple parts. **2.** Read each question carefully and put your answer neatly in the space provided. **3.** Show all your work. Explain your reasoning. Correct answers without supporting work will not get credit.

1. Give the definitions of the followings:

   (a) A partition of a set X.
   Let $\mathcal{H} \subseteq \mathcal{P}(X)$. Then $\mathcal{H}$ is a partition of the set X if
   - The union of the sets in $\mathcal{H}$ is equal to X.
   - For any different two sets in $\mathcal{H}$, their intersection is empty.

   (b) Transitivity of a relation R.
   Let A be set and $R \subseteq A \times A$. Then R is a transitive relation on A if
   - $(a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R$ for all $a,b,c \in A$.

   (c) The proper inclusion $A \subset B$ for sets A and B.
   Let A and B be sets. Then $A \subset B$ if
   - $\forall x(x \in A \Rightarrow x \in B) \wedge \exists y(y \in B \wedge y \notin A)$

2. For a set S denote by $\mathcal{P}(S)$ the power set of S. Determine each of the following sets:

   (a) $\mathcal{P}(\{2\})$
   $\mathcal{P}(\{2\}) = \{\emptyset, \{2\}\}$

   (b) $\mathcal{P}(\mathcal{P}(\{2\}))$
   $\mathcal{P}(\mathcal{P}(\{2\})) = \{\emptyset, \{\emptyset\}, \{\{2\}\}, \{\emptyset, \{2\}\}\}$

   (c) $\mathcal{P}(\mathcal{P}(\mathcal{P}(\{2\})))$
   $\mathcal{P}(\mathcal{P}(\mathcal{P}(\{2\}))) = A_0 \cup A_1 \cup A_2 \cup A_3 \cup A_4$ where
   - $A_0 = \{\emptyset\}$
   - $A_1 = \{\{\emptyset\}, \{\{\emptyset\}\}, \{\{\{2\}\}\}, \{\{\emptyset, \{2\}\}\}\}$
   - $A_2 = \{\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\{2\}\}\}, \{\emptyset, \{\emptyset, \{2\}\}\}, \{\{\emptyset\}, \{\{2\}\}\}, \{\{\emptyset\}, \{\emptyset, \{2\}\}\}, \{\{\{2\}\}, \{\emptyset, \{2\}\}\}\}$
   - $A_3 = \{\{\emptyset, \{\emptyset\}, \{\{2\}\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{2\}\}\}, \{\emptyset, \{\{2\}\}, \{\emptyset, \{2\}\}\}, \{\{\emptyset\}, \{\{2\}\}, \{\emptyset, \{2\}\}\}\}$
   - $A_4 = \{\{\emptyset, \{\emptyset\}, \{\{2\}\}, \{\emptyset, \{2\}\}\}\}$

3. Prove or disprove: $\{\{\{5\}\}\} = \{\{5\}\}$.

Suppose $\{\{\{5\}\}\} = \{\{5\}\}$. Observe that $\{5\}$ is an element in the right hand side and the left hand side contains exactly one element, namely $\{\{5\}\}$. Therefore we need to have $\{5\} = \{\{5\}\}$. Then 5 is the only element of the set $\{5\}$ while the set $\{\{5\}\}$ contains exactly one element, namely $\{5\}$. Hence we must have $5 = \{5\}$, which is false because the left hand side is an element whereas the right hand side is a set. Therefore, $\{\{\{5\}\}\} \neq \{\{5\}\}$.

4. For given sets A, B, C and functions $f : A \to B$, $g : B \to C$, prove or disprove:

   (a) If g is not injective then $g \circ f$ is not injective.

   FALSE

   We will give a counter example such that $g \circ f$ is injective even if g is not injective. Let

   - $A = \{1\}$, $B = C = \{1, 2\}$
   - $f(1) = 1$, $g(1) = g(2) = 1$

   Since the domain of $g \circ f$ contains exactly one element, trivially it is injective while g is not injective because $g(1) = g(2)$.

   (b) If f is not injective then $g \circ f$ is not injective.

   TRUE

   We will prove the claim by using contrapositive. By assuming $g \circ f$ is injective, we will show that f is injective.

   Assume $f(x) = f(y)$ for some $x, y \in A$. Then

   $$(g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y)$$

   Since $g \circ f$ is injective, $(g \circ f)(x) = (g \circ f)(y)$ implies $x = y$.

   Hence $f(x) = f(y)$ implies $x = y$ and so f is injective.

5. For each of the parts below, either give an example or prove that it does not exist:

   (a) Sets A and B satisfying $A \in B$ and $A \subseteq B$.
   We will give an example. Consider the following sets A and B:

   - $A = \{1, 2\}$
   - $B = \{1, 2, \{1, 2\}\}$

   Clearly, $A \in B$ and $A \subseteq B$.

   (b) An equivalence relation $\sim$ on the set $\{1, 2, 3\}$ consisting of exactly 4 ordered pairs.
   We will prove that there is no equivalence relation on the set $\{1, 2, 3\}$ consisting of exactly 4 ordered pairs.

   Suppose $\sim$ an equivalence relation on $\{1, 2, 3\}$. Since $\sim$ is reflexive, then we have $1 \sim 1$, $2 \sim 2$, $3 \sim 3$. Therefore if $\sim$ contains exactly four elements, there exists a unique element (a, b) satisfying $a \sim b$ and $a \neq b$. However, if $a \sim b$ then we have $b \sim a$ and $(b, a) \neq (a, b)$ since $\sim$ is symmetric and $a \neq b$. This implies either $\sim$ contains exactly three elements or it contains at least five elements.

   (c) A relation on the set of natural numbers that is reflexive, symmetric but not transitive.
   We will give an example. Consider the following relation R on natural numbers:

   $$(x, y) \in R \Leftrightarrow |x - y| \leq 1$$

   Observe that

   - R is reflexive since $|x - x| \leq 1$ for all natural numbers x.
   - R is symmetric since $|x - y| = |y - x|$ for all natural numbers x and y.
   - R is not transitive since $(1, 2) \in R$, $(2, 3) \in R$ but $(1, 3) \notin R$.

6. Using just the axioms describing the natural numbers given in class, prove that for every natural number x we have $x \neq x'$.

   Let T be the set of all natural numbers x for which the inequality $x \neq x'$ holds. By *Axiom 1* and *Axiom 3*, we have $1 \neq 1'$ and so $1 \in T$. On the other hand, suppose $x \in T$ for some natural number x. If $(x')' = x'$, then from *Axiom 4* we would have $x' = x$, which contradicts with $x \in T$. Hence $x \in T$ implies $x' \in T$. Finally, from *Axiom 5*, we can conclude T contains all natural numbers.

7. Let A and B be non-empty sets. Suppose $\mathcal{F}$ is a partition of A and $\mathcal{G}$ is a partition of B. Define

$$\mathcal{H} = \{Z \subseteq A \times B : \exists X \in \mathcal{F}, \exists Y \in \mathcal{G}\ (Z = X \times Y)\}$$

   (a) Prove that $\mathcal{H}$ is a partition of $A \times B$.
   Let $\mathcal{H} = \{Z_i : i \in I\}$ for some index set I. We know that $\mathcal{H}$ is a partition of $A \times B$ if $\cup_{i \in I} Z_i = A \times B$ and $Z_i \cap Z_j \neq \emptyset \Rightarrow Z_i = Z_j$ for all $i, j \in I$.

   - Take two sets Z_i and Z_j in $\mathcal{H}$ for some $i, j \in I$, and assume $Z_i \cap Z_j \neq \emptyset$. Then there exists $(a, b) \in Z_i \cap Z_j$. On the other hand, from the definition of $\mathcal{H}$, we have $Z_i = X \times Y$ for some $X \in \mathcal{F}$, $Y \in \mathcal{G}$, and $Z_j = U \times V$ for some $U \in \mathcal{F}$, $V \in \mathcal{G}$. Hence we have $(a, b) \in X \times Y$ and $(a, b) \in U \times V$, which implies $a \in X \cap U$ and $b \in V \cap Y$. Moreover, we know $\mathcal{F}$ is a partition for A and $X, U \in \mathcal{F}$. Since $a \in X \cap U$ and so $X \cap U \neq \emptyset$, we must have $X = U$. Similarly we can obtain $Y = V$, which implies $Z_i = X \times Y = U \times V = Z_j$.
   - Observe that $Z_i \subseteq A \times B$ for any $i \in I$ from the definition. Then clearly $\cup_{i \in I} Z_i \subseteq A \times B$. Therefore we need to show that $A \times B \subseteq \cup_{i \in I} Z_i$. Let $(a, b) \in A \times B$, we must show that $(a, b) \in Z_i$ for some $i \in I$. Observe that $\mathcal{F}$ is a partition for A and $a \in A$, so we can find $X \in \mathcal{F}$ satisfying $a \in X$. Similarly, $\mathcal{G}$ is a partition for B and $b \in B$, so we can find $Y \in \mathcal{G}$ satisfying $b \in Y$. Then from the definition of $\mathcal{H}$, we have $X \times Y \in \mathcal{H}$ and so $X \times Y = Z_i$ for some $i \in I$. Therefore, $(a, b) \in \mathcal{H}$.

   As a result, $\mathcal{H}$ is a partition for $A \times B$.

   (b) If the partition $\mathcal{F}$ corresponds to the equivalence relation $\sim_1$ on A and $\mathcal{G}$ corresponds to the equivalence relation $\sim_2$ on B, what equivalence relation does $\mathcal{H}$ correspond to?
   Let $\sim$ be the equivalence relation corresponding to the partition $\mathcal{H}$ on $A \times B$. We must understand when $(a_1, b_1) \sim (a_2, b_2)$ for $(a_1, b_1), (a_2, b_2) \in A \times B$.

   We know that corresponding equivalence to the partition $\mathcal{H}$ means $(a_1, b_1) \sim (a_2, b_2)$ whenever (a_1, b_1) and (a_2, b_2) are in the same set with respect to $\mathcal{H}$. On the other hand, $(a_1, b_1), (a_2, b_2) \in Z_i$ for some $i \in I$ means that there exists $X \in \mathcal{F}$ and $Y \in \mathcal{G}$ such that $(a_1, b_1), (a_2, b_2) \in X \times Y$. Then we have $a_1, a_2 \in X$ and $b_1, b_2 \in Y$, which implies $a_1 \sim_1 a_2$ and $b_1 \sim_2 b_2$. As a result, if $(a_1, b_1) \sim (a_2, b_2)$ then we have $a_1 \sim_1 a_2$ and $b_1 \sim_2 b_2$.

   Conversely, if $a_1 \sim_1 a_2$ and $b_1 \sim_2 b_2$, then the class of a_1 and a_2 with respect to $\sim_1$ is a set in $\mathcal{F}$, say X, whereas the class of b_1 and b_2 with respect to $\sim_2$ is a set in $\mathcal{G}$, say Y. Hence $X \times Y$ is a set in $\mathcal{H}$ and so it defines an equivalence class. Moreover, $(a_1, a_2), (b_1, b_2) \in X \times Y$. Hence $a_1 \sim_1 a_2$ and $b_1 \sim_2 b_2$ imply $(a_1, b_1) \sim (a_2, b_2)$.

   Finally, $(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow (a_1 \sim_1 a_2) \wedge (b_1 \sim_2 b_2)$.