Math 109: materials that are not covered in the midterms.

Prepared by Alireza Salehi Golsefidy

1 Injection, surjection, bijection.

1. Let $f : X \to Y$ and $g : Y \to Z$ be two functions. Prove the following

   (a) If $g \circ f$ is injective, then f is injective.

   (b) If $g \circ f$ is surjective, then g is surjective.

   (c) If $g \circ f$ is a bijection, then the restriction $g|_{\mathrm{Im(f)}} : \mathrm{Im(f)} \to \mathrm{X}$ of g to the image of f is a bijection.

   (d) If f and g are injective, then $g \circ f$ is injective.

   (e) If f and g are surjective, then $g \circ f$ is surjective.

   (f) If f and g are bijections, then $g \circ f$ is a bijection.

2. Let $f : X \to Y$ be a function. Prove the following

   (a) There is a function $g : Y \to X$ such that $g \circ f = I_X$ if and only if f in injective.

   (b) There is a function $g : Y \to X$ such that $f \circ g = I_Y$ if and only if f is surjective.

   (c) f is invertible if and only if f is a bijection.

   (d) If f is invertible, then there is a unique function $g : Y \to X$ such that $g \circ f = I_X$ and $f \circ g = I_Y$.

   (e) If f is invertible, then its inverse f^{-1} is a bijection.

3. Determine if the following functions are injective, surjective, or bijective.

   (a) $f : \mathbb{Z} \to \mathbb{Z}, f(x) = x - 1$ if x is odd, and $f(x) = x + 1$ if x is even. (This is from Professor Popescu's exam.)

   (b) Let X be a non-empty set, and

   $$f : P(X) \to \{g| \;\; g : X \to \{0, 1\}\}, \quad f(A) := \mathbb{1}_A$$

   where $\mathbb{1}_A : X \to \{0, 1\}$ is the characteristic function of A, i.e. $\mathbb{1}_A(x) = 1$ if $a \in A$, and $\mathbb{1}_A(x) = 0$ if $x \notin A$.

   (c) Let $Y \subsetneq X$, and $f : P(X) \to P(Y), f(A) = A \cap Y$.

   (d) Let $Y \subseteq X$, and $f : P(X) \to P(X), f(A) = A \triangle Y$.

   (e) Let $\varnothing \neq Y \subseteq X$, and $f : P(X) \to \{A \in P(X)| \; Y \subseteq A\}, f(A) = A \cup Y$.

   (f) Let $\alpha \in (0, 1)$, and $f : \mathbb{Z} \to \mathbb{Z}, f(n) = \lfloor n\alpha \rfloor$.

   (g) Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, and $f : \mathbb{Z} \to [0, 1), f(n) = n\alpha - \lfloor n\alpha \rfloor$.

   (h) Let $a, b \in \mathbb{Z}^+$. Suppose $\gcd(a, b) = 1$. Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, f(x, y) = ax + by$.

4. Give a set X and two functions $f, g : X \to X$ such that $g \circ f = I_X$ and $g \circ f \neq I_X$.

2 Cardinality of a set, enumerable sets.

1. Suppose X is enumerable and Y is an infinite subset of X. Prove that Y is enumerable.
2. Assuming that any infinite subset of an enumerable set is enumerable, prove that the set $\mathbb{Q}$ of rational numbers is enumerable.
3. State and prove Cantor's theorem.
4. Suppose X is enumerable. Prove that $|P(X)| = |P(\mathbb{Z}^+)|$, i.e. there is a bijection $f : P(X) \to P(\mathbb{Z}^+)$.
5. Prove that $\{X \in P(\mathbb{Z}) |\ X \text{ is finite}\}$ is enumerable.
6. Assuming that any infinite subset of an enumerable set is enumerable, prove that union of two enumerable sets is enumerable.
7. Prove that $A_1 \times \cdots \times A_n$ is enumerable if $A_1, \ldots, A_n$ are enumerable.
8. Prove that $\{f |\ f : \{1, \ldots, n\} \to \mathbb{Z}^+\}$ is enumerable. (Hint: show that
$$g : \{f |\ f : \{1, \ldots, n\} \to \mathbb{Z}^+\} \to \mathbb{Z}^+ \times \cdots \times \mathbb{Z}^+, g(f) = (f(1), f(2), \ldots, f(n))$$
is a bijection.)
9. Suppose $A_1, A_2, \ldots$ be a sequence of enumerable subsets of X.
   (a) For any $j \in \mathbb{Z}^+$, let $g_j : A_j \to \mathbb{Z}^+$ be a bijection. Let $Y = \{(x, i) \in X \times \mathbb{Z}^+ |\ x \in A_i\}$, and $f : Y \to \mathbb{Z}^+ \times \mathbb{Z}^+, f((x, i)) = (g_i(x), i)$. Prove that f is a bijection. Deduce that Y is enumerable.
   (b) For any $x \in A_1 \cup A_2 \cup \ldots$, let $i(x)$ be the smallest positive integer i such that $x \in A_i$. Let $g : \bigcup_{j=1}^{\infty} A_j \to Y, g(x) = (x, i(x))$. Prove that g is injective.
   (c) Assuming that any infinite subset of an enumerable set is enumerable, prove that $\bigcup_{j=1}^{\infty} A_j$ is enumerable.
10. Prove that $\{g |\ g : \mathbb{Z}^+ \to \{0, 1\}\}$ is not enumerable.
11. Use the decimal representation of numbers to show that there is a bijection
$$f : (0, 1) \setminus \mathbb{Q} \to \{g |\ g : \mathbb{Z}^+ \to \{0, 1, \ldots, 9\}\}.$$
Deduce that $(0, 1) \setminus \mathbb{Q}$ is not enumerable.

3 Integer part.

1. Prove that for any $x \in \mathbb{R}$ there is a unique $m \in bbz$ such that $m \le x < m + 1$.
2. Prove that for any $x \in \mathbb{R}$ there is a unique $m \in \mathbb{Z}$ such that $m < x \le m + 1$. This is called the ceiling of x and it is denoted by $\lceil x \rceil$.
3. Prove that for any $x \in \mathbb{R} \setminus \mathbb{Z}$ we have $\lfloor -x \rfloor = -\lceil x \rceil$.
4. Prove that $\forall x \in \mathbb{R}, \forall n \in \mathbb{Z}^+, \lfloor nx \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{n} \rfloor + \cdots + \lfloor x + \frac{n-1}{n} \rfloor$.
5. Prove that for any $n, m \in \mathbb{Z}^+$ we have $|\{k \in \{1, 2, \ldots, n\} |\ m|k\}| = \lfloor \frac{n}{m} \rfloor$.
6. For $x \in \mathbb{R}$ let $\langle x \rangle = \min\{|x - k| |\ k \in \mathbb{Z}\}$. Prove that $\langle x \rangle = \min\{x - \lfloor x \rfloor, \lceil x \rceil - x\}$.
7. Suppose $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.
   (a) Prove that for any $n \in \mathbb{Z}^+$ there is $m \in \{1, 2, \ldots, n\}$ such that $\langle m\alpha \rangle < 1/n$.
   (b) Suppose $\langle x \rangle < 1/n$ for some $n \in \mathbb{Z}^+$. Prove that for any $y \in [0, 1]$ there are $s, t \in \mathbb{Z}$ such that $|y - sx - t| < 1/n$.
   (c) Prove that for any $y \in [0, 1]$ and any $\varepsilon > 0$ there are integers m, k such that $|y - m\alpha - k| < \varepsilon$.

4 Basic arithmetic.

1. Write down the Division theorem and prove it.
2. Prove that no integer of the form $7k + 3$ (where $k \in \mathbb{Z}$) is a perfect square.
3. Prove that $\sum_{i=0}^{m} a_i 10^i \equiv \sum_{i=0}^{m} a_i \pmod 9$.
4. Let $a, b, n \in \mathbb{Z}^+$. Prove that $ax \equiv b \pmod n$ has a solution if and only if $\gcd(a, n)|b$.
5. Find an integer solution of $2015x + 273y = \gcd(2015, 273)$. (This is from Professor Sorense's exam.)
6. Let $f : \{0, 1, \ldots, 7\} \times \{0, 1, \ldots, 7\} \to \{0, 1, \ldots, 7\}, f(x, y) \equiv xy \pmod 8$. Write an 8×8 table where the i, j entry is $f(i - 1, j - 1)$. In which rows is there a 1?
7. Find the remainder of 9^{16} divided by 13.
8. Suppose $a \equiv b \pmod n$. Prove that $\gcd(a, n) = \gcd(b, n)$.
9. Suppose p is prime. Prove that $p|ab$ if and only if either $p|a$ or $p|b$.
10. Suppose $\gcd(a, b) = 1$. Prove that $a|bc$ if and only if $a|c$.

Look at the last problem set for more related problems.