KFUPM/ Department of Mathematics/T222/MATH 210/ Final Exam/Solution

Name: **ID #:** **Serial #:**

---

1. [12pts] (a) For each of the following sets, indicate if it is finite, denumerable, or uncountable and justify your answers: $\mathcal{P}(\mathbb{Z}_{10})$, $\mathbb{Q} \times \mathbb{Z}$, $\mathbb{C}$.

(b) Let X and Y be sets such that $X \subseteq Y$. Prove that if X is uncountable, then Y is uncountable.

(c) State Schröder-Bernstein Theorem and prove that $[-2,2) \approx [0,1]$.

Solution. (a) $\mathcal{P}(\mathbb{Z}_{10})$ is finite because $\mathbb{Z}_{10}$ is finite ($|\mathcal{P}(\mathbb{Z}_{10})| = 2^{10}$).
$\mathbb{Q} \times \mathbb{Z}$ is denumerable because $\mathbb{Q}$ and $\mathbb{Z}$ are denumerable (using a result that if A and B are denumerable sets, then $A \times B$ is denumerable).
$\mathbb{C}$ is uncountable because it contains $\mathbb{R}$ which is uncountable (see Part (b)).

(b) By contrapositive: If Y is countable, then it is either finite and then X is finite, or it is denumerable and then X is denumerable. In both cases X is countable. $\blacksquare$

(c) SBT: If A and B are sets such that $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.
Proof that $[-2,2) \approx [0,1]$: There is a one-to-one function (inclusion map) from $[0,1]$ to $[-2,2)$, so $|[0,1]| \leq |[-2,2)|$.
Also, each of the inclusion maps $f : [-2,2) \longrightarrow \mathbb{R}$ and $h : (0,1) \longrightarrow [0,1]$ is one-to-one and we have a bijection $g : \mathbb{R} \longrightarrow (0,1)$. Hence the composition $h \circ g \circ f : [-2,2) \longrightarrow [0,1]$ is one-to-one and therefore $|[-2,2)| \leq |[0,1]|$. By SBT, $[-2,2) \approx [0,1]$. $\blacksquare$

Note that instead of the composition above, we can directly construct a one-to-one function from $[-2,2)$ to $[0,1]$, for example the function k given by $k(x) = \dfrac{1}{2} + \dfrac{x}{4}$.

---

2. [12pts] (a) Use the Euclidean algorithm to find $\gcd(390, 186)$ and integers x, y such that $\gcd(390, 186) = 390x + 186y$.

(b) State the Fundamental Theorem of Arithmetic and prove that if n is an integer greater than 1, then there is a prime p such that p^3 divides n^3.

(c) Two integers m and n are such that $m \geq 2$, $n^3 \equiv 5 \pmod{m}$, and $n^2 \equiv 2 \pmod{m}$. Find m.

Solution. (a) $390 = 2 \times 186 + 18$, $186 = 10 \times 18 + 6$, $18 = 3 \times 6$. Hence $\gcd(390, 186) = 6$.
We have $6 = 186 - 10 \times 18 = 186 - 10 \times (390 - 2 \times 186) = (-10) \times 390 + 21 \times 186$. We can therefore take $x = -10$, $y = 21$.
(b) FTA: Every integer greater than 1 is a product of primes, and this decomposition is unique up to the order of the prime factors.

Let n be an integer greater than 1. By FTA, n is a product of prime factors. Let p be one of these prime factors, then $p|n$ and hence $p^3|n^3$.

(c) We have $0 \equiv (n^3)^2 - (n^2)^3 \equiv 5^2 - 2^3 \pmod{m}$, hence $17 \equiv 0 \pmod{m}$. Since $m > 1$, we get $m = 17$.

---

3. [12pts] (a) Let G and G' be groups with respective identity elements e and e' and let $f : G \longrightarrow G'$ be an isomorphism. Prove that $f(e) = e'$.

(b) Let G be the set of all real numbers of the form $n\sqrt{2}$ where n is an integer. Is G a subgroup of the (additive) group $\mathbb{R}$? Justify your answer.

(c) Let H be a subgroup of a group G such that $|H| = n$. If the number of distinct left cosets of H in G is $2n+1$ and $20 < |G| < 60$, find all possible values of n.

Solution. (a) We will use the multiplicative notation for both groups. We have $e'f(e) = f(e) = f(ee) = f(e)f(e)$, so, by right cancellation, $e' = f(e)$.

(b) Yes, G is a subgroup of $\mathbb{R}$: G is clearly nonempty (for example, it contains $0\sqrt{2}$). Also, if $a, b \in G$, then $a = a'\sqrt{2}$ and $b = b'\sqrt{2}$ for some $a', b' \in \mathbb{Z}$, so $a + b = (a' + b')\sqrt{2} \in G$ (because $a' + b' \in \mathbb{Z}$) and $-a = (-a')\sqrt{2} \in G$ (because $-a' \in \mathbb{Z}$).

(c) By Lagrange Theorem, $|G| = n(2n+1)$, so $20 < n(2n+1) < 60$. This implies that $3, 4, 5$ are the only possible values of n.

---

4. [12pts] (a) Let S be a relation on $\mathbb{R}$ defined by aSb if and only if $a^2 - b^2 \in \mathbb{Q}$. Is S reflexive? symmetric? antisymmetric? transitive? Justify your answers.

(b) Let T be a relation on $\mathbb{Q}$ defined by xTy if and only if $x - y$ is a nonnegative integer. Is $(\mathbb{Q}, T)$ a poset? Is it well-ordered? Justify your answers.

Solution. (a) $\forall a, b, c \in \mathbb{R}$:

- $a^2 - a^2 = 0 \in \mathbb{Q}$, so S is reflexive.
- If $a^2 - b^2 \in \mathbb{Q}$, then $b^2 - a^2 = -(a^2 - b^2) \in \mathbb{Q}$, so S is symmetric.
- If $a^2 - b^2 \in \mathbb{Q}$ and $b^2 - c^2 \in \mathbb{Q}$, then $a^2 - c^2 = a^2 - b^2 + b^2 - c^2 \in \mathbb{Q}$, so S is transitive.
- S is not antisymmetric because, for example, $1S0$ and $0S1$, but $1 \neq 0$.

(b) Denote by W the set of all nonnegative integers. Then, $\forall a, b \in \mathbb{Q}$:

- $a - a = 0 \in W$, so T is reflexive.
- If $a - b \in W$ and $b - a \in W$, then $a \geq b \geq a$, i.e. $a = b$. Hence T is antisymmetric.

- If $a-b \in W$ and $b-c \in W$, then $a-c=a-b+b-c \in W$, so T is transitive.

This proves that $(\mathbb{Q}, T)$ is a poset. However, $(\mathbb{Q}, T)$ is not well-ordered because $1/2$ and 0 are not comparable.

---

5. [12pts] Mark each of the following statements as True or False and justify your choices.

(a) If p is prime and $n \in \mathbb{Z}$ such that $\gcd(p, n) > 1$, then $p|n$. **True**: $\gcd(p, n)\,|p$, so $\gcd(p, n) = p$ (because p is prime and $\gcd(p, n) > 1$), and this implies $p|n$.

(b) If $f : Z_6 \longrightarrow Z_6$ is the function given by $f([a]) = [3a]$ for each $a \in \mathbb{Z}$, then f is a bijection. **False**: $f([0]) = f([2]) = [0]$, but $[0] \neq [2]$, so f is not one-to-one.

(c) $\{[1], [2], [4], [8]\}$ is a cyclic subgroup of the multiplicative group $\mathbb{Z}_{17}^*$. **False**: $[4][4] = [16] \notin \{[1], [2], [4], [8]\}$, so $\{[1], [2], [4], [8]\}$ is not even a subgroup of $\mathbb{Z}_{17}^*$.