CS60005 Foundations of Computing Science
Tutorial 3

Countability

1. Let A and B be uncountable sets with $A \subseteq B$. Prove or disprove: A and B are equinumerous.

2. Let A be an uncountable set and B a countably infinite subset of A. Prove or disprove: A is equinumerous with $A - B$.

3. Prove that the real interval $[0, 1)$ is equinumerous with the unit square $[0, 1) \times [0, 1)$.

4. Define a relation $\sim$ on $\mathbb{R}$ such that $a \sim b$ if and only if $a - b \in \mathbb{Q}$. Answer the following:
   (a) Prove that $\sim$ is an equivalence relation.
   (b) Is the set $\mathbb{R}/\sim$ of all equivalence classes of $\sim$ countable?

5. Let $\mathbb{Z}[x]$ denote the set of all univariate polynimials with integer coefficients. Answer the following:
   (a) Prove that $\mathbb{Z}[x]$ is countable.
   (b) A real or complex number a is called algrbraic if $f(a) = 0$ for some non-zero $f(x) \in \mathbb{Z}[x]$. Let $\mathbb{A}$ denote the set of all algebraic numbers. Prove that $\mathbb{A}$ is countable.

6. Let $\mathbb{Z}[x, y]$ be the set of all bivariate polynomials with integer coefficients. Answer the following:
   (a) Prove that $\mathbb{Z}[x, y]$ is countable.
   (b) Let $V = \{(a, b) \in \mathbb{C} \times \mathbb{C} \mid f(a, b) = 0 \text{ for some nonzero } f(x, y) \in \mathbb{Z}[x, y]\}$. Is V countable?

7. A set $S \subseteq \mathbb{R}$ is called bounded if S has both a lower bound and an upper bound. Answer whether the following sets are countable/uncountable?
   (a) The set of all bounded subsets of $\mathbb{Z}$.
   (b) The set of all bounded subsets of $\mathbb{Q}$.

Algebraic Structures

1. Let $R_1, R_2, \ldots, R_n$ be rings. Prove that, the Cartesian product $(R_1 \times R_2 \times \cdots \times R_n)$ is a ring under component-wise additionand multiplication. Show that, if each R_i is a ring with identity, then so also is the product.

2. Let $R = \mathbb{Z} \times \mathbb{Z}$, and r, s be constant integers. Define two operations, on R as follows:
   $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) * (c, d) = (ad + bc + rac, bd + sac)$.
   Prove that, R is a ring under these operations, $+$ and $*$.

3. Let R be a commutative ring with identity. Prove that, the set $R[x]$ of all univariate polynomials with coefficients from R is again a commutative ring with identity (under polynomial addition and multiplication).

4. Define an operation $\circ$ on $G = \mathbb{R}^* \times \mathbb{R}$ as $(a, b) \circ (c, d) = (ac, bc + d)$. Prove that, $(G, \circ)$ is a non-abelian group.

5. Let G be a (multiplicative) group, and H, K are subgroups of G. Prove that,
   (a) $H \cap K$ is a subgroup of G.
   (b) $H \cup G$ need not be a subgroup of G.
   (c) $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.
   (d) Define $HK = \{hk \mid h \in H, k \in K\}$. Define KH analogously.
   Prove that, HK is a subgroup of G if and only if $HK = KH$.

6. Let G be a non-abelian group, and $a, b \in G$. Prove that, $\texttt{ord}(ab) = \texttt{ord}(ba)$.

7. Let G be the set of all points on the hyperbola $xy = 1$ along with the point $(0, \infty)$ at infinity. Define $(a, \frac{1}{a}) + (b, \frac{1}{b}) = (a + b, \frac{1}{a+b})$. Prove that, G is an abelian group under this operation.
