Basic Fact Sheet 2

All proofs on the exam should follow the proper structure and use the precise definitions. You may use, with reference, any of the following definitions or theorems. You may also use, without reference, any axiom or proposition from algebra that we have used in the homework. **Everything** else must be clearly justified from definitions and appropriate logic.

Below, f is a function from A to B and g is a function from B to C.

- **well-defined**: $\forall x_1, x_2 \in A$, $x_1 = x_2 \Rightarrow f(x_1) = f(x_2)$.
- **injective (one-to-one)**: $\forall x_1, x_2 \in A$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
- **surjective (onto)**: $\forall b \in B$, $\exists a \in A$ such that $f(a) = b$.
- **composition**: The function $h = g \circ f : A \to C$ is called the composition and is given by $h(x) = g(f(x))$ for all $x \in A$.
- **increasing**: $\forall x_1, x_2 \in A$, $x_1 < x_2 \Rightarrow f(x_1) < f(x_2)$.
- **decreasing**: $\forall x_1, x_2 \in A$, $x_1 < x_2 \Rightarrow f(x_1) > f(x_2)$.
- **nondecreasing**: $\forall x_1, x_2 \in A$, $x_1 < x_2 \Rightarrow f(x_1) \leq f(x_2)$.
- **nonincreasing**: $\forall x_1, x_2 \in A$, $x_1 < x_2 \Rightarrow f(x_1) \geq f(x_2)$.

- **divisibility**: For $a, b \in \mathbb{Z}$ with $b \neq 0$, if there exists $k \in \mathbb{Z}$ such that $a = kb$, then we say b divides a (or a is divisible by b). We write $b|a$.
- **prime**: If $n \in \mathbb{N}$ with $n \neq 1$ and the only divisors of n are 1 and n, then we say n is a prime number.
- **greatest common divisor**: If $a, b \in \mathbb{Z}$ with not both zero, then gcd(a, b)=‘the largest positive integer that divides both a and b’.
- **relatively prime**: If $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$, then we say that a and b are relatively prime.

- **The Binomial Theorem**: For all $\forall x, y \in \mathbb{R}$ and $\forall n \in \mathbb{N}$, $(x+y)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.
- **Pascal's Identity**: $\forall k, n \in \mathbb{N}$ with $1 \leq k < n$, $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.
- **Division Algorithm**: If $a, b \in \mathbb{N}$ with $a \geq b > 0$, then there exists $q, r \in \mathbb{N}$ such that $a = qb + r$ with $0 \leq r < b$.
- **Euclidean Algorithm**: Let $a, b \in \mathbb{N}$ with $a \geq b > 0$ and define $r_0 = a$, $r_1 = b$ and
  $r_i = q_{i+1} r_{i+1} + r_{i+2}$, where $0 \leq r_{i+2} < r_{i+1}$.
  If $r_n \neq 0$ and $r_{n+1} = 0$ for some n, then $\gcd(a, b) = r_n$.