# MATH 558 EXAM I SOLUTIONS

**Name:**

**Statements and Definitions.**

1. Let $X$ be a set and $\sim$ a relation on $X$.

(i) State what it means for $\sim$ to be an equivalence relation.

Solution.

(a) $x \sim x$, for all $x \in X$.
(b) For all $x_1, x_2 \in X$, if $x_1 \sim x_2$, then $x_2 \sim x_1$.
(c) For all $x_1, x_2, x_2 \in X$, if $x_1 \sim x_2$ and $x_2 \sim x_3$, then $x_1 \sim x_3$.

(ii) Assuming $\sim$ is an equivalence relation, for $x \in X$, define $[x]$, the equivalence class of $x$.

Solution.

$$[x] = \{x' \in X \mid x' \sim x\}$$

(iii) Assume $\sim$ is an equivalence relation. For $x_1, x_2 \in X$, what can you say about the relationship between $[x_1]$ and $[x_2]$?

Solution.

$$[x_1] = [x_2] \quad \text{or} \quad [x_1] \cap [x_2] = \emptyset$$

2. State the Well Ordering Principle.

Solution.

First version: Every non-empty set of positive integers has a least element.

Second Version: Every set of integers that is bounded below has a least element.

Either version is acceptable

3. Define the greatest common divisor of two integers $a, b$ **and** state one property you know about the greatest common divisor of $a$ and $b$.

Solution.

The greatest common divisor of $a$ and $b$ is the largest integer that divides both $a$ and $b$. Some properties are:

(a) The gcd of $a$ and $b$ is divisible by any common divisor of $a$ and $b$.
(b) The gcd of $a$ and $b$ is unique.
(c) The gcd of $a$ and $b$ can be written as an integer combination of $a$ and $b$.

4. State the Fundamental Theorem of Arithmetic for the integers.

Solution.

Every positive integer $n$ can be written as a product $n = p_1 \cdots p_r$, where each $p_j$ is a prime number and $p_1 \leq \cdots \leq p_r$. Moreover, if $n = q_1 \cdots q_s$, with $q_1 \leq \cdots \leq q_s$ and each $q_j$ is prime, then $r = s$ and $p_1 = q_1, \ldots, p_r = q_r$.

5. State the Fundamental Theorem of Arithmetic for monic polynomials with coefficients in $F$.

Solution.

Every polynomial monic $f(x)$ of degree greater than zero can be written as a product $f(x) = p_1(x) \cdots p_r(x)$, where each $p_j(x)$ is a monic irreducible polynomial with coefficients in $F$. Moreover, if $f(x) = q_1(x) \cdots q_s(x)$, with each $q_j(x)$ a monic irreducible polynomial with coefficients in $F$, then $r = s$ and after re-indexing, $p_1(x) = q_1(x), \ldots, p_r(x) = q_r(x)$.

**Short Answer.** 1. Use mathematical induction to prove that $n! > 2^n$, for all $n \geq 4$.

Solution.

Base case: $4! = 24 > 16 = 2^4$

Inductive step: Suppose $n! > 2^n$. Multiply both side by $n+1$ to get:

$$(n+1)! = (n+1) \cdot n! > (n+1) \cdot 2^n > 2 \cdot 2^n = 2^{n+1}.$$

Note to class: This was the original intended problem - without the typo appearing on exam day.

2. Use the Euclidean algorithm to find the greatest common divisor of 42 and 72 and then use what you have derived to write the greatest common divisor as an integer combination of 42 and 72.

Solution.

$$\begin{aligned} 72 &= 1 \cdot 42 + 30 \\ 42 &= 1 \cdot 30 + 12 \\ 30 &= 2 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0, \end{aligned}$$

Thus, 6 is the gcd of 72 and 42. Using backwards substitution, starting with the last equation, we get:

$$\begin{aligned} 6 &= 30 - 2 \cdot 12 \\ 6 &= 30 - 2 \cdot (42 - 30) \\ 6 &= 3 \cdot 30 - 2 \cdot 42 \\ 6 &= 3 \cdot (72 - 42) - 2 \cdot 42 \\ 6 &= 3 \cdot 72 - 5 \cdot 42), \end{aligned}$$

which gives what we want.

**Proof Presentation.** Give a rigorous proof of the following statement. Let $f(x)$ and $g(x)$ be non-zero polynomials in $F[x]$. Then there exist $q(x)$ and $r(x)$ in $F[x]$ such that $g(x) = f(x) \cdot q(x) + r(x)$ and the degree of $r(x)$ is strictly less than the degree of $f(x)$.

Solution.

Suppose $g(x)$ has degree less than the degree of $f(x)$. Then $g(x) = 0 \cdot f(z) + g(x)$.

If deg $g(x) \geq$ deg $f(x)$, write $g(x) = b_m x^m + \cdots + b_0$ and $f(x) = a_n x^n + \cdots + a_0$, and proceed by induction on deg $g(x)$.

Suppose $m = n$. Then $r(x) = g(x) - \frac{b_n}{a_n} \cdot f(x)$ has degree less than the degree of $f(x)$. Thus,

$$g(x) = \frac{b_n}{a_n} \cdot f(x) + r(x).$$

If $m > n$, then we note that $g_0(x) = g(x) - \frac{b_m}{a_n} x^{m-n} \cdot f(x)$ has degree less than the degree of $g(x)$. By induction, we can write $g_0(x) = q_0(x) \cdot f(x) + r(x)$, where the degree of $r(x)$ is less than the degree of $f(x)$. Thus, $g(x) = (\frac{b_m}{a_n} x^{m-1} + q_0(x)) \cdot f(x) + r(x)$, which gives what we want.