MAT 3530: Algebra **Name:** *SOLUTIONS*

Midterm Exam: take-home portion.

1. Since there are many ways to do this, I have not provided a solution, but I would be glad to discuss any of your solutions individually. For full credit, I expected your solution to clearly show it was constructed in a way that ensured it would map the points to their respective images.

2. Let l, m, and n be integers such that l divides mn and the greatest common divisor of l and m is k. Prove that l divides kn.

   Proof. We proved that $k = al+bm$ for suitable integers a and b. Thus, $kn = (al+bm)n = aln + bmn$ (by the distributive law). Since $l \mid mn$, $mn = lc$ for some integer c; hence, $kn = aln + bmn = aln + blc = l(an + bc)$. Thus, l divides kn by definition. □

   Remark: It should be clear that this result holds in any Euclidean domain.

3. We proved that if p is a prime integer, m and n are integers, and p divides mn, then either p divides m or p divides n. In applications, we actually needed a more general result:

   Lemma. *If p is a prime integer, $m_1, m_2, m_3, \ldots, m_k$ are integers, and p divides $m_1m_2m_3\cdots m_k$, then p divides m_i for some i.*

   Prove it!

   Proof. We proceed by simple induction on k, the number of factors.

   Initial case. $k = 1$. Then $p \mid m_1$ by hypothesis, so the result is obvious.

   Inductive claim. If $p \mid m_1m_2m_3\cdots m_k \Rightarrow p \mid m_i$ for some i, then $p \mid m_1m_2m_3\cdots m_{k+1} \Rightarrow p \mid m_i$ for some i.

   Assume (as inductive hypothesis) that $p \mid m_1m_2m_3\cdots m_k \Rightarrow p \mid m_i$ for some i. By hypothesis, $p \mid m_1m_2m_3\cdots m_{k+1}$, which implies that $p \mid (m_1m_2m_3\cdots m_k)m_{k+1}$ by associativity. By the result for two factors (proven previously and referenced above), $p \mid (m_1m_2m_3\cdots m_k)$ or $p \mid m_{k+1}$; thus, the proof naturally divides into two cases:

   Case 1. $p \mid (m_1m_2m_3\cdots m_k)$. Then $p \mid m_i$ for some i by inductive hypothesis.

   Case 2. $p \mid m_{k+1}$. Obviously in this case the conclusion holds. □

4. Prove that for any natural number n, 3 divides $n^3 - n$.

   There are at least two ways to go about this: induction, or factoring with division into cases.

   Proof by induction.

   Initial Case. n=1. $1^3 - 1 = 0$, and clearly $3 \mid 0$, since $3 \cdot 0 = 0$.

   Inductive Claim. If $3 \mid n^3 - n$, then $3 \mid (n+1)^3 - (n+1)$. Assume by inductive hypothesis that $3 \mid n^3 - n$. Using the distributive property (and the elementary and easily proven fact that the additive inverse of a sum is the sum of the inverses), we see

that $(n+1)^3-(n+1) = n^3+3n^2+3n+1-n-1 = (n^3-n)+3(n^2+n)$. Clearly, $3 \mid 3(n^2+n)$, and by inductive hypothesis $3 \mid n^3-n$; hence it follows easily (and was proven in the homework and on the in-class midterm) that $3 \mid (n^3-n)+3(n^2+n)$. □

Proof by factoring with division into cases. It is easy to see that $n^3-n = n(n-1)(n+1)$. We claim that 3 divides one of the factors $n, n-1$, or $n+1$, and hence divides the product n^3-n. To see this we must divide into cases. To divide into cases one always asks a question and considers all the possible answers. Here is our question: when 3 is divided into n,, what is the remainder? (We could just as well have considered dividing 3 into one of the other factors, but using n is simplest.) We know $n = 3q+r$ for some integer q, where $r = 0$, 1, or 2.

Case 1. $r = 0$. Then $n = 3q$, so $3 \mid n$.

Case 2. $r = 1$. Then $n = 3q+1$, so $n-1 = 3q$; thus, $3 \mid n-1$.

Case 3. $r = 2$. Then $n = 3q+2$, so $n+1 = 3q+3 = 3(q+1)$; thus, $3 \mid n+1$.

□

5. (a) Prove that, with the operations of addition and multiplication of functions defined above, the set of continuous functions from $\mathbb{R}$ to $\mathbb{R}$ constitutes a commutative ring. This ring is denoted $C^0(\mathbb{R})$.

   First we must prove that the set of continuous functions is closed under the operations of addition and multiplication as defined. This follows immediately from the fact that the sum or product of continuous functions is continuous, proved (or at least stated) in Calculus 1. Thus, we have a set with two operations defined on it.

   Next, recall the defining properties (or axioms, if you prefer) of a commutative ring, which these operations must satisfy:

   - Both + and $\cdot$ are associative.
   - Both + and $\cdot$ are commutative. (Commutativity of $\cdot$ is what makes the ring commutative; + is always commutative in any ring or any other algebraic structure, such as a vector space, in which it is used.)
   - There is an additive identity and there is a multiplicative identity.
   - Every element of the ring has an additive inverse.
   - The distributive property holds (multiplication distributes over addition).

   Remark. The existence of and additive identity and additive inverses makes any ring into an additive group.

   We must prove all of these properties.

   Proof.

   - Associativity. By definition, for any $x \in \mathbb{R}$ and any continuous real-valued functions f, g, and h, $[(f+g)+h](x) = [f+g](x)+h(x) = (f(x)+g(x))+h(x)$. By the associativity of addition in the real number system, $(f(x)+g(x))+h(x) = f(x)+(g(x)+h(x))$, and by definition, $f(x)+(g(x)+h(x)) = f(x)+[g+h](x) = [f+(g+h)](x)$. Thus, $[(f+g)+h](x) = [f+(g+h)](x)$ for all real numbers x. Since the outputs of the functions $(f+g)+h$ and $f+(g+h)$ agree for every input, they are the same function: $(f+g)+h = f+(g+h)$. Similarly, using

the associativity of multiplication in the real number system, $(fg)h = f(gh)$. I leave the details to you.

- Commutativity. For any $x \in \mathbb{R}$, $[f+g](x) = f(x) + g(x)$. By commutativity of addition in the real number system, $f(x)+g(x) = g(x)+f(x)$, and by definition, $g(x) + f(x) = [g + f](x)$. Thus, $[f + g](x) = [g + f](x)$ for all real numbers x. Since their outputs agree for every input, $f + g = g + f$. Similarly, using commutativity of multiplication in the real number system, $fg = gf$. Again I leave the details to you for practice.
- Identities. The additive identity is the constant function 0. For any real number x and any continuous real-valued function f, $[f+0](x) = f(x)+0 = f(x) = 0+f(x) = [0+f](x)$, by the identity property of 0 in the real number system (and, of course, the definition of addition of functions). Since this is true for every real number x, $f + 0 = f = 0 + f$ as functions. Similarly, the constant function 1 is the multiplicative identity: $[f \cdot 1](x) = f(x) \cdot 1 = f(x) = 1 \cdot f(x) = [1 \cdot f](x)$.
- Additive inverses. The additive inverse of a function f is the function $-f$ defined by $[-f](x) = -f(x)$. since $-f = (-1)f$, constant functions such as -1 are certainly continuous, and the product of two continuous functions is continuous, $-f$ is a continuous function. It is clear that $[f + (-f)](x) = f(x) + (-f(x)) = 0 = -f(x) + f(x) = [-f + f](x)$ for every real number x.
- The distributive law. As you might well expect, this is a consequence of the distributive law in the real number system: $[f(g + h)](x) = f(x)[g + h](x) = f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x) = [fg + fh](x)$; hence, $f(g + h) = fg + fh$.

□

(b) Prove or disprove by giving a counter-example: $C^0(\mathbb{R})$ is an integral domain.
Consider the non-zero continuous functions f and g defined by:

$$f(x) = \begin{cases} 0 & \text{, if } x < 0 \\ x & \text{, if } x \geq 0 \end{cases}$$

$$g(x) = \begin{cases} x & \text{, if } x < 0 \\ 0 & \text{, if } x \geq 0 \end{cases}$$

Clearly $fg = 0$. Thus $C^0(\mathbb{R})$ has zero-divisors and is not a domain.

(c) Describe the group of units of $C^0(\mathbb{R})$.
The multiplicative inverse of a function f is an element of $C^0(\mathbb{R})$ if and only if $\frac{1}{f(x)}$ is defined for all real numbers x. By a theorem from Calculus 1, the function $\frac{1}{f}$ (defined in the obvious way by $\frac{1}{f}(x) = \frac{1}{f(x)}$) is continuous at all points where it is defined, but it is not defined for any values of x such that $f(x) = 0$. Thus the units of $C^0(\mathbb{R})$ are exactly those functions whose outputs are never 0: $U = \{f : (\forall x \in \mathbb{R}) f(x) \neq 0\}$.