

## MATH 3200 THIRD MIDTERM EXAM

Directions: **Do any four of the five problems.** If there is any doubt as to which four problems you want me to grade, I will grade the first four problems, whether that is to your benefit or not. Always justify your reasoning completely. No calculators are permitted.

- 1) Let  $R \subseteq X \times Y$  be a relation.  
a) Define the inverse relation  $R^{-1}$ .

Solution:  $R^{-1}$  is the set  $\{(y, x) \in Y \times X \mid (x, y) \in R\}$ .

- b) Prove or disprove: if  $R \subseteq X \times Y$  is a relation whose inverse relation  $R^{-1}$  is a function from  $Y$  to  $X$ , then  $R$  is itself a function from  $X$  to  $Y$ .

Solution: This is false. For instance suppose  $X = \{1, 2\}$ ,  $Y = \{a, b\}$  and  $R = \{(1, a), (1, b)\}$ . Then  $R^{-1} = \{(a, 1), (b, 1)\}$ , which is a function from  $Y$  to  $X$ , but  $R$  itself is not a function, because the single element  $1 \in X$  is related to two distinct elements  $a$  and  $b \in Y$ .

Remark: We saw in class that if, instead of an arbitrary relation on  $X \times Y$ , we have a function  $f : X \rightarrow Y$ , then if the inverse relation  $f^{-1}$  is a function, it follows that  $f$  is invertible and  $f^{-1}$  is its inverse. But for this it is crucial that  $f$  itself be a function, as the above example shows.

- 2) Let  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$  be functions.  
a) Suppose that  $f$  and  $g$  are both injective. Show that  $g \circ f$  is injective.

Solution: Let  $x_1, x_2 \in X$  be such that  $(g \circ f)(x_1) = (g \circ f)(x_2)$ , or in other words  $g(f(x_1)) = g(f(x_2))$ . Since  $g$  is injective, this implies  $f(x_1) = f(x_2)$ . Since  $f$  is injective, this implies  $x_1 = x_2$ . Thus  $g \circ f$  is injective.

- b) Prove or disprove: it is possible for  $f$  to be injective,  $g$  to be surjective, and  $g \circ f$  to be neither injective nor surjective.

Solution: This is true. Take, for instance  $X = \{a, b\}$ ,  $Y = \{1, 2, 3\}$ ,  $f : a \mapsto 1, b \mapsto 2$ ,  $g : 1 \mapsto a, 2 \mapsto a, 3 \mapsto b$ . Evidently  $f$  is injective and  $g$  is surjective. Then  $(g \circ f) : a \mapsto a, b \mapsto a$ , which is neither injective nor surjective.

Remark: The above solution is most efficient one in the following sense: If  $X = Y = \emptyset$  everything holds vacuously. If  $X$  is empty and  $Y$  is nonempty, then no function  $g : Y \rightarrow X$  exists; similarly, if  $X$  is nonempty and  $Y$  is empty then no function  $f : X \rightarrow Y$  exists. If  $X$  has a single element, then there is only one function from  $X$  to itself, the identity function, which is both injective and surjective. So  $\#X \geq 2$ . If  $\#X = 2$  and  $\#Y = 1$  then there is no injection from  $X$  to  $Y$ . If  $X$  and  $Y$  are

both finite sets of the same cardinality, then a function between them is an injection iff it is a surjection iff it is a bijection, so the hypotheses would imply that  $g \circ f$  is a composition of bijections and therefore a bijection. So if  $\#X = 2$  we need  $\#Y \geq 3$ .

3) Show that for all  $n \in \mathbb{Z}$ ,  $e^n > n$ .

Solution: For any real number  $x$ ,  $e^x > 0$ , so if  $n < 0$  we have  $e^n > 0 > n$ . Therefore we may assume  $n \in \mathbb{N}$  and go by induction on  $n$ . However, things will go more smoothly if we start at  $n = 1$ , so we separately verify the claim for  $n = 0$ :  $e^0 = 1 > 0$ .

Base case:  $n = 1$ :  $e^1 = e = 2.71828\dots > 1$

Inductive step: Assume that for some  $n \in \mathbb{Z}^+$ ,  $e^n > n$ . Then

$$e^{n+1} = ee^n > en = (e-1)n + n \geq (e-1) + n \geq 1 + n.$$

Alternate solution: We will show in fact that for all  $x \in \mathbb{R}$ ,  $e^x > x$ . As above, this is trivial for  $x < 0$  because  $e^x > 0$  and  $x < 0$ . We also have  $e^0 = 1 > 0$ . Now put  $f(x) = e^x$  and  $g(x) = x$ . Then  $(f-g)' = e^x - 1$ . This is non-negative for all  $x \geq 0$  and strictly positive for all  $x > 0$ , because  $e^x$ , having a positive derivative, is strictly increasing, and  $e^0 = 1$ . Therefore  $f-g = e^x - x$  is strictly increasing for all  $x \geq 0$ . Therefore, since it is positive at  $x = 0$ , it must also be positive for all positive  $x$ .

4) For each of the following functions  $f : \mathbb{R} \rightarrow \mathbb{R}$ , determine whether  $f$  is injective, surjective and/or bijective.

a)  $f(x) = x^3 + x + 1$ .

Solution: Any polynomial function of odd degree  $P(x) = a_n x^n + \dots + a_1 x + a_0 : \mathbb{R} \rightarrow \mathbb{R}$  is surjective. Indeed, if  $a_n > 0$ , then  $\lim_{x \rightarrow \infty} P(x) = \infty$ ,  $\lim_{x \rightarrow -\infty} P(x) = -\infty$ . On the other hand, if  $a_n < 0$ , then  $\lim_{x \rightarrow \infty} P(x) = -\infty$ ,  $\lim_{x \rightarrow -\infty} P(x) = \infty$ . Either way,  $P$  assumes arbitrarily large and arbitrarily small real values. Since  $P$  is continuous, by the intermediate value theorem all values are assumed. To see that  $f$  is injective, it suffices to show that it is strictly increasing. But  $f'(x) = 3x^2 + 1 > 0$  for all real  $x$ , so indeed  $f$  is strictly increasing. In summary,  $f$  is injective and surjective, hence bijective.

b)  $f(x) = x^3 - x + 1$ .

Solution: As above, since  $f$  is a polynomial of odd degree, it is surjective. However, this time  $f$  is not injective. The easiest way is to observe that  $f(0) = f(1) = 1$ . (How could you see this easily? One way: adding or subtracting a constant does not change the injectivity or surjectivity of a function, so we might as well be given  $f(x) = x^3 - x$ . Evidently, this factors as  $x(x^2 - 1)$  and thus as  $x(x-1)(x+1)$ . So it has three zeros so is not injective.)

A more sophisticated, but also more general, solution is to look at the derivative:  $f'(x) = 3x^2 - 1$  and observe that the first derivative test shows that it has a local minimum and local maximum, and is not injective in any neighborhood of either point. (Draw a picture!)

c)  $f(x) = \ln(x^2 + 1)$ .

Solution: Since  $f(-x) = f(x)$ ,  $f$  is *even*, and no even function is injective. As for surjectivity, the function  $\ln x$  is indeed surjective, but for any real  $x$ ,  $x^2 + 1 \geq 1$ , so the image is  $\ln([1, \infty)) = [0, \infty)$ . In plainer terms, we are only plugging in numbers which are at least one, so their natural logarithms must be at least zero. Thus  $f$  is neither injective nor surjective.

d)  $f(x) = e^{e^{x^3}}$ .

Solution:  $f$  is of the form  $g_3 \circ g_2 \circ g_1$ , with  $g_1(x) = x^3$  and  $g_2(x) = g_3(x) = e^x$ . As we know, the composition of two injective functions is surjective. Similarly one shows that the composition of three injective functions is injective. (In fact, it is an easy induction problem to show that for all  $n \geq 2$ , the composition of any  $n$  injective functions is injective. Make sure you know how to do it!) So  $f$  is injective. However, because the outside function  $e^x$  is not surjective – its range is  $(0, \infty)$ , certainly  $f$  is not surjective.

5) Let  $X$  be the set of all functions  $f : \mathbb{R} \rightarrow \mathbb{R}$ . For each of the following relations  $R$  on  $X$ , determine whether  $R$  is an equivalence relation, a partial ordering and/or a total ordering.

a)  $f R g$  iff  $f(2009) = g(2009)$ .

Solution: It is straightforward to verify that this relation is reflexive, symmetric and transitive, so is an equivalence relation.

b)  $f R g$  iff  $f(2009) < g(2009)$ .

Solution: This relation is very far from being reflexive: for *no* function  $f : \mathbb{R} \rightarrow \mathbb{R}$  do we have  $f(2009) < f(2009)$ . So it cannot be an equivalence relation or a partial ordering. Since a total ordering is a special kind of partial ordering, it cannot be a total ordering either.

c)  $f R g$  iff  $f(2009) \leq g(2009)$ .

Solution: This relation is reflexive. It is rather clearly not symmetric: suppose  $f(2009) < g(2009)$ , then we do not have  $g(2009) \leq f(2009)$ . It is also not anti-symmetric:  $fRg$  and  $gRf$  means that  $f(2009) \leq g(2009)$  and  $g(2009) \leq f(2009)$ , i.e.,  $f(2009) = g(2009)$ . But certainly this does not imply  $f = g$ : e.g. take  $f(x) = x$  and  $g(x) = 2009$ . So it is not an equivalence relation or a partial ordering.

d)  $f R g$  iff  $f(x) \leq g(x)$  for all  $x \in \mathbb{R}$ .

Solution:  $f$  is indeed reflexive: for all  $f$ ,  $f(x) \leq f(x)$  for all  $x \in \mathbb{R}$ . It is not symmetric, as above. It is anti-symmetric: if  $f(x) \leq g(x)$  for all  $x$  and  $g(x) \leq f(x)$  for all  $x$ , then  $f(x) = g(x)$  for all  $x$ , which means that  $f = g$ . It is also transitive: if  $f(x) \leq g(x)$  for all  $x$  and  $g(x) \leq h(x)$  for all  $x$ , then  $f(x) \leq h(x)$  for all  $x$ . Therefore  $R$  is not an equivalence relation but is a partial ordering. It is not a total

ordering: to say that it is is to say that given any two functions, the graph of one of them lies entirely above or equal to the graph of the other, which is certainly not true: e.g.  $f(x) = \sin x$ ,  $g(x) = 0$ .

Extra credit: One version of Fermat's Little Theorem states that for any prime number  $p$  and for any natural number  $a$ ,  $a^p \equiv a \pmod{p}$ . Prove this as follows:

Step 1: Show that for  $0 < i < p$ , the binomial coefficient  $\binom{p}{i}$  is  $0 \pmod{p}$ .

Solution: We have  $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ . But  $i!$  and  $(p-i)!$  are both products of positive integers which are strictly less than  $p$ , so (by Euclid's Lemma) neither is divisible by  $p$ . So the numerator is divisible by  $p$  and the denominator isn't, so  $\binom{p}{i}$  is divisible by  $p$ .

Step 2: Use Step 1 to show that for all  $a \in \mathbb{Z}$ ,  $(a+1)^p \equiv a^p + 1 \pmod{p}$ .

Solution: We have

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \dots + \binom{p}{p-1}a + 1.$$

Since all the binomial coefficients  $\binom{p}{i}$  are divisible by  $p$ , modulo  $p$  they are congruent to 0:

$$(a+1)^p \equiv a^p + 0a^{p-1} + \dots + 0a + 1 \equiv a^p + 1 \pmod{p}.$$

Step 3: Now apply induction.

Solution: The case case is  $a = 0$ :  $0^p = 0 \equiv 0 \pmod{p}$ . Assume that the result holds for any natural number  $a$ :  $a^p \equiv a \pmod{p}$ . Then by Step 2 we have

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}.$$