Name:__________________________________

Math 3560 **Fall 2011**

Solutions to the First Prelim

September 27, 2011

Problem 1: Answer T or F (true or false, of course) for each of the following (do not give reasons). You may use the back of this sheet for scratch paper.

(a) Every surjective map from a finite set to itself is bijective. **T**

(b) Every rotation of $\mathbb{R}^3$ has an axis. **T**

(c) If $(xy)^{-1} = x^{-1}y^{-1}$ for all elements x, y of a group G, then G is abelian.**T**

(d) If n is a positive, even integer, then every cycle of length n is even.**F**

Problem 2: Complete the following partial sentences so as to produce correct definitions:

(a): A function $f : X \to Y$ is injective if *for all* $x, y \in X, f(x) = f(y) \Rightarrow x = y$ *[or* $x \neq y \Rightarrow f(x) \neq f(y)$*].*

(b): A function $f : \mathbb{R}^3 \to \mathbb{R}^3$ is an isometry if ... *it preserves distances [or, for all* $x, y \in \mathbb{R}^3, ||f(x) - f(y)|| = ||x - y||$*].*

(c): An element g in a group G has order 24 provided that ...
textit$g^{24} = e$ and $g^n \neq e$, for all n satisfying $0 < n < 24$. (Note: Both conditions are important. Many students omitted the second condition.)

(d): A permutation σ in S_n is a cycle of length k provided that ... .
There are a number of possible answers for this one. Here's one: *There is an integer* $j \in \{1, 2, \ldots, n\}$ *such that (1)* $\sigma^k(j) = j$ *and (2)* $\sigma^i(j) \neq j$*, for all integers* i *satisfying* $0 < i < k$. Here's another: *There exist* k *distinct integers* $a_1, a_2, \ldots, a_k$ *such that* $\sigma(a_i) = a_{i+1}$*, for* $0 < i < k - 1$*, and* $\sigma(a_k) = a_1$.

Problem 3: Prove that the subgroup $H \leq S_4$ generated by $\{(12), (34)\}$ is abelian and has four elements. List the elements and give their orders. Justify your assertions.

Solution: By direct computation, the transpositions (12) and (34) have order 2. They commute because they are disjoint. Therefore $((12)(34))^2 = (12)^2(34)^2 = id \cdot id = id$. So the product $(12)(34)$ has order one or two. But only the identity has order one, and clearly $(12)(34)$ is not the identity. So it has order two.

Using the commutativity of (12) and (34), the terms in any product of (12's and (34)'s (in any order) can be rearranged so that all the (12)'s come first and then the (34)'s. So, it is of the form $(12)^m(34)^n$, for some integers m and n. But because (12) and (34) both have order two, the factors $(12)^m$ and $(34)^n$ depend only on the parity of m and n. The first is equal to the identity when m is even and equal to (12) when m is odd. Analogously for the second. Therefore, we get $(12)^m(34)^n = id$ when both m and n are even;$=(12)$ when m is odd and n is even;$=(34)$ when m is even and n is odd; $=(12(34)$ when both m and n are odd. This shows that $H = \{id, (12), (34), (12)(34)\}$ and completes the proof.

Problem 4: Suppose that G is a group of order 3. Say its elements are e, g, h, with e the identity element.

(a) Prove that $gh \neq g$ and $gh \neq h$. It follows that gh must equal e, that is, $h = g^{-1}$.

The first two assertions are proved by assuming the contrary of each and then performing a computation that leads to a contradiction. So: $gh = g$ implies that $g^{-1}gh = g^{-1}g = e$, hence $h = e$, contradicting what has been given. Similarly, $gh = h$ implies that $g = e$, again a contradiction. Thus by the principle of proof by contradiciton, we must have $gh \neq g$ and $gh \neq h$. (Of course, the only remaining possibility then is that $gh = e$, as stated. This was not necessary to prove.)

(b) Prove that the equation $g^2 = e$ contradicts the conclusion of **(a)**. Conclude that $g^2 = h$ and, therefore, that $g^3 = e$. (Justify these conclusions.)

The conclusion of (a) is that $gh = e$. It is slightly more convenient to state it as: $e = gh$. We now assume that $g^2 = e$ and derive a contradiction. Multiply these two last equations, obtaining: $e \cdot g^2 = e \cdot gh$, or $g^2 = gh$. Cancelling g from both sides (i.e., multiplying both sides by g^{-1}) yields $g = h$, contradicting what was given.

It follows that $g^2 \neq e$. Of course, we cannot have $g^2 = g$, for then g would have to equal e. So, the only remaining possibility is $g^2 = h$. This shows, using the result of (a), that $g^2 = g^{-1}$ (since (a) tells us that $h = g^{-1}$). Therefore, multiplying both sides by g, we get $g^3 = e$. Therefore, the order of g is less than or equal to 3. It can't equal 1, because $g \neq e$, and it can't equal 2, by what we proved in the preceding paragraph. So, the order of g must be 3.

To summarize: $G = \{e, g, g^2\}$, with $o(g) = 3$.

Problem 5: (a) List all of the generators of $\mathbb{Z}_{12}$.

By a homework exercise, the generators of $\mathbb{Z}_{12}$ consist of the integers between 1 and 11 that are relatively prime to 12 (i.e., have no factors in common with 12 bigger than 1). These numbers are precisely $1, 5, 7, 11$.

Incidentally, a number of students used the multiplicative convention for $\mathbb{Z}_{12}$ rather than the more commonly used additive convention. This sometimes led to some confusion. It is better to stick to the additive convention for standard abelian groups like $\mathbb{Z}_{12}$.

(b) You are given an arbitrary generator x of $\mathbb{Z}_{12}$ as well as an isomorphism $f : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$. Prove that $f(x)$ is a generator of $\mathbb{Z}_{12}$.

Proof 1: An element of $\mathbb{Z}_{12}$ is of order 12 if and only if it is a generator of $\mathbb{Z}_{12}$. Therefore, the given generator x has order 12. Furthermore, we proved in class that an isomorphism preserves the order of an element. Therefore $f(x)$ also has order 12, implying that it is a generator of $\mathbb{Z}_{12}$.

Proof 2: Since x is a generator, the powers x^n give all 12 elements of $\mathbb{Z}_{12}$ as n goes from 0 to 11. Since f is a bijection, the elements $f(x^n)$ also comprise 12 distinct elements of $\mathbb{Z}_{12}$, i.e all the elements. But, we also know that $f(x^n) = (f(x))^n$, for every integer n, because f is an isomorphism. (In fact, this is true even if f is merely a homomorphism.) Therefore, the powers $(f(x))^n$ give all of $\mathbb{Z}_{12}$. So, $f(x)$ is a generator of $\mathbb{Z}_{12}$.

(c) Suppose that y is another generator of $\mathbb{Z}_{12}$. Show that there is a isomorphism $h : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ such that $h(x) = y$. (This means that you have to define an explicit function h and then prove that it is an isomorphism.)

Proof: We are given generators x and y of $\mathbb{Z}_{12}$. This means that the powers x^n give all of $\mathbb{Z}_{12}$ exactly once as n ranges from 0 to 11; the same holds for the powers y^n. Therefore, we may unambiguously define a function $h : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ by the formula $h(x^n) = y^n$, for each $n = 0, 1, \ldots, 11$. By the definition, the function is clearly surjective (since every y^n is a function value) and clearly injective as well (since, for the range of n's considered, $x^m \neq x^n$ implies $m \neq n$, which implies that $y^m \neq y^n$, hence $h(x^m) \neq h(x^n)$). So h is a bijection. To see that it is an isomorphism, simply compute $h(x^m x^n) = h(x^{m+n})$ (reducing mod 12 as necessary). Then $h(x^{m+n}) = y^{m+n} = y^m y^n = h(x^m)h(x^n)$, so, in summary: $h(x^m x^n) = h(x^m)h(x^n)$. This completes the proof that h is an isomorphism.

(d) Suppose that $h : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ is an isomorphism and that it satisfies $h(x) = f(x)$, with f as above. Prove that $f = h$.

Proof: By the property of homomorphisms and isomorphisms already used above, we have

$$h(x^n) = (h(x))^n = (f(x))^n = f(x^n),$$

for every integer n. But x^n ranges over all of the elements of $\mathbb{Z}_{12}$. So, h and f assume the same values for every element of $\mathbb{Z}_{12}$, which means they are equal. This completes the proof.

Items (b), (c) and (d) show that there is a bijection between the set of all generators of $\mathbb{Z}_{12}$ and the set of all isomorphisms $\mathbb{Z}_{12} \to \mathbb{Z}_{12}$