Math 721 - Final Exam Version 1 - December 13, 2011

Name: _____

Question Number	Possible Points	Score
1	19	
2	19	
3	19	
4	19	
5	19	
6	19	
7	19	
8	19	
9	19	
10	19	
11	10	
Total	200	

Instructions:

- You MAY NOT use the book, notes, other people's work, or other people's brains in the course of taking this exam.
- You MAY quote the result of any homework problem that has been assigned in this course.
- You MAY have fun.
- You MAY have an excellent winter break.
- 42.

1. (19 points).

(a) (6 points). State the definition of a group.

A group G is a set together with a binary operation on G so that if $a, b \in G$, then $a * b \in G$. Also, we must have $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$. There must be an element $e \in G$ so that $a * e = e * a = a$ for all $a \in G$. Finally for each $a \in G$, there must be an element $a^{-1} \in G$ so that $a * a^{-1} = a^{-1} * a = e$.

(b) (4 points). What does it mean for a group to be abelian?

A group G is abelian if $a * b = b * a$ for all $a, b \in G$.

(c) (4 points). What does it mean for a group to be cyclic?

A group G is cyclic if there is an element $x \in G$ so that $G = \{x^k : kin\mathbb{Z}\}$.

(d) (5 points). True or false: In an abelian group G with order 2^n that contains an element x of order 2^k, then for any element y of order 2^{k-1}, there is an element $z \in G$ so that $z^2 = y$.

This is false. Let $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $x = (1, 0)$, which has order 4, and $y = (2, 1)$ which has order 2. There is no element $z \in G$ so that $z^2 = y$, because if $z = (a, b)$ then $z^2 = (2a, 2b)$ and so the second coordinate of y would have to be even.

2. (19 points).

(a) (5 points). If g_1 and g_2 are elements of a group G, what does it mean to say that g_1 and g_2 are conjugate? Prove that conjugacy is an equivalence relation.

The elements g_1 and g_2 are conjugate and write $g_1 \sim g_2$ if $g_2 = gg_1g^{-1}$ for some $g \in G$. To prove that conjugacy is an equivalence relation we must show that it is reflextive, symmetric, and transitive. Clearly, $g_1 \sim g_1$ (take g to be the identity). Also, if $g_2 = gg_1g^{-1}$, then $g^{-1}g_2g = g_1$ and so $g_1 \sim g_2$ implies that $g_2 \sim g_1$. Finally, if $g_1 \sim g_2$ and $g_2 \sim g_3$, then we have $g_2 = gg_1g^{-1}$ and $g_3 = hg_2h^{-1}$ and so $g_3 = hgg_1g^{-1}h^{-1} = (hg)g_1(hg)^{-1}$.

(b) (6 points). Prove that if g_1 and g_2 are conjugate, then g_1 and g_2 have the same order.

If g_1 and g_2 are conjugate, then we have

$$\begin{aligned} g_2^m &= \overbrace{(gg_1g^{-1})(gg_1g^{-1})\cdots(gg_1g^{-1})}^{n \text{ factors}} \\ &= gg_1^mg^{-1}. \end{aligned}$$

Hence, if $g_2^m = 1$, then $gg_1^mg^{-1} = 1$ so $g_1^m = g^{-1}g = 1$. Conversely, if $g_1^m = 1$, then $g_2^m = gg^{-1} = 1$. Hence if $S_1 = \{m \geq 1 : g_1^m = 1\}$ and $S_2 = \{m \geq 1 : g_2^m = 1\}$, then $S_1 = S_2$, and so they have the same smallest element (which is the order of g_1 and also the order of g_2). In the case that either has infinite order, then the other has infinite order as well, since $S_1 = S_2$ would both be empty.

(c) (8 points). Suppose that G is a finite group and $g \in G$ has exactly m conjugates. Prove that m divides $|G|$. Prove that G has a subgroup of index m.

The number of conjugates of $g \in G$ is equal to the size of the orbit acting of G acting on itself by conjugation. The Fundamental Counting Principle says that this equals the index of the stabilizer, and the stabilizer is $\{h \in G : hgh^{-1} = g\} = Z(g)$ is the centralizer of G. Thus, $|G : Z(g)| = m$ and so m divides $|G|$ and $Z(g)$ has index m.

3. (19 points).

(a) (6 points). State the definition of a ring homomorphism. State the definition of an ideal (you may state whichever version of the definition you like).

A ring homomorphism is a function $\phi : R \to S$ where R and S are rings so that $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$, and $\phi(1) = 1$. An ideal of a ring R is a set $I \subseteq R$ so that if $x, y \in I$, then $x + y \in I$ and if $x \in I$ and $r \in R$, then $xr \in I$.

(b) (7 points). Explain why the kernel of a ring homomorphism is an ideal. Is every ideal the kernel of some ring homomorphism?

If $I = \ker \phi$, where ϕ is a ring homomorphism, then if $a, b \in I$ we have $\phi(a+b) = \phi(a)+\phi(b) = 0$ and so $a + b \in I$. If $x \in I$ and $r \in R$, then $\phi(xr) = \phi(x) \cdot \phi(r) = 0 \cdot \phi(r) = 0$ and so $xr \in I$.

Yes, every ideal is the kernel of some ring homomorphism. In particular, if I is an ideal of R and $\phi : R \to R/I$ is the map given by $\phi(x) = x + I$, then $\ker \phi = I$.

(c) (6 points). State the correspondence theorem for rings.

If R is a ring and $\phi : R \to \mathcal{R}$ is a *surjective* ring homomorphism with kernel I, then there is a bijection between ideals J of R that contain I and ideals of $\mathcal{R}$. This bijection is given by $\phi(I) \mapsto \mathcal{I}$ and $\mathcal{I} \mapsto \phi^{-1}(\mathcal{I}) = \{x \in R : \phi(x) \in \mathcal{I}\}$. Moreover, if I and $\mathcal{I}$ correspond, then $R/I \approx \mathcal{R}/\mathcal{I}$.

4. (19 points). Is there a finite group G containing two elements x and y so that

- x and y both have order 2
- xy has order 4?

Give an example of such a group G and elements x and y, or prove that no such objects exist.

Let $G = S_4$, $x = (1, 3)$ and $y = (1, 2)(3, 4)$. Then x and y have order 2, and

$$xy = (1, 2, 3, 4)$$

has order 4.

5. (19 points).

(a) (4 points). State Lagrange's theorem.

If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

(b) (15 points). Prove Lagrange's theorem. [Prove any properties of cosets you use.]

Claim: We have that

- If aH is any left coset of H, then $|aH| = |H|$.
- Any two left cosets of H are equal or disjoint.
- We have $G = \bigcup_{g \in G} gH$.

Since G is a union of cosets, and any two cosets are equal or disjoint, the order of G is equal to the sum of the sizes of the cosets. Since each coset has size equal to $|H|$, $|G| = |H| \cdot (\text{ the number of left cosets of } H)$. Thus, $|H|$ divides $|G|$.

Proof of claim: The map $\phi(x) = ax$ is a map from H to aH. It is a bijection because $\phi_2(x) = a^{-1}x$ is its inverse. Thus, $|H| = |aH|$.

If $a_1H \cap a_2H \neq \emptyset$, then there is some $a_3 \in a_1H \cap a_2H$. We get that $a_3 = a_1h_1 = a_2h_2$ for $h_1, h_2 \in H$. Thus, for any element $h \in H$, $a_2h = a_1h_1h_2^{-1}h \in a_1H$ and so $a_2H \subseteq a_1H$. Since $|a_2H| = |a_1H|$ it follows that $a_2H = a_1H$.

Finally, it is easy to see that if $g \in G$, then g is contained in some left coset (namely gH). This proves the claim.

6. (19 points). Suppose that G acts transitively on a set S and s_1 and s_2 are two elements of S. Let K_1 be the stabilizer of s_1 and K_2 be the stabilizer of s_2. Prove that K_1 and K_2 are conjugate subgroups of G. [You may assume that K_1 and K_2 are in fact subgroups.]

Since G acts transitively on S, there is an element $g \in G$ so that $g * s_1 = s_2$. Now, if $x \in K_1$, then

$$\begin{aligned} gxg^{-1} * s_2 &= gxg^{-1} * (g * s_1) \\ &= gx * (g^{-1}g * s_1) = gx * s_1 \\ &= g * (x * s_1) = g * s_1 = s_2. \end{aligned}$$

Hence, the function $\phi(x) = gxg^{-1}$ sends K_1 to K_2. A similar argument shows that if $x \in K_2$, then

$$\begin{aligned} g^{-1}xg * s_1 &= g^{-1}x * (g * s_1) \\ &= g^{-1}x * s_2 \\ &= g^{-1} * (x * s_2) = g^{-1} * s_2 = g^{-1} * (g * s_1) \\ &= g^{-1}g * s_1 = 1 * s_1 = s_1. \end{aligned}$$

Hence, $\psi(x) = g^{-1}xg$ sends K_2 to K_1. Finally,

$$\begin{aligned} \phi \circ \psi(x) = \phi(\psi(x)) = \phi(g^{-1}xg) = g(g^{-1}xg)g^{-1} = x \\ \psi \circ \phi(x) = \psi(\phi(x)) = \psi(gxg^{-1}) = g^{-1}(gxg^{-1})g = x \end{aligned}$$

and so ϕ is a bijection. Thus, $K_2 = gK_1g^{-1}$, as desired.

7. (19 points). Prove the second Sylow theorem. This states that if G is a finite group and p divides $|G|$, then all the Sylow p-subgroups of G are conjugate, and every subgroup of G whose order is a power of p is contained in some Sylow p-subgroup. [You may use the first Sylow theorem in your proof.]

Let K be a subgroup of G whose order is a power of p and let H be a Sylow p-subgroup of G. We will show that K is contained in some conjugate of H. All conjugates of H are Sylow p-subgroups and so this proves that K is contained in a Sylow p-subgroup. Moreover, if we take K to be a Sylow p-subgroup itself, we have that $K \subseteq gHg^{-1}$ and since $|K| = |gHg^{-1}|$, this proves that $K = gHg^{-1}$ and so all Sylow p-subgroups of G are conjugate.

Let K act on the left cosets of H. Since $|G : H|$ is not a multiple of p, there must be some orbit whose size is not a multiple of p. However, the size of an orbit must divide the order of K which is a power of p. Hence, an orbit whose size is not a multiple of p must have size one. Therefore, there is some $g \in G$ so that $kgH = gH$ for all $k \in K$. This means that $g^{-1}kgH = H$ for all $k \in K$ and so $g^{-1}kg \in H$ for all $k \in K$. This means that $k \in gHg^{-1}$ for all $k \in K$ and so $K \subseteq gHg^{-1}$, as desired.

8. (19 points). Prove that every group of order 721 is cyclic. [Hint: The number 103 is prime.]

If $|G| = 721 = 7 \cdot 103$, then $n_{103}(G)|7$ and $n_{103}(G) \equiv 1 \pmod 7$. This proves that $n_{103}(G) = 1$ and so if P is a Sylow 103-subgroup, then $P \trianglelefteq G$. Also, $n_7(G)|103$ and $n_7(G) \equiv 1 \pmod 7$. Since $103 = 98 + 5 = 5 + 7 \cdot 14$, we have that $103 \equiv 5 \pmod 7$ and so $n_7(G) = 1$. Thus, if Q is a Sylow 7-subgroup of G, then $Q \trianglelefteq G$. We have $|P \cap Q|$ divides both 7 and 103 and so $P \cap Q = 1$. Also, PQ is a subgroup of G (since at least one of P and Q is normal). By Lagrange's theorem, $|P|$ divides $|PQ|$ and $|Q|$ divides $|PQ|$ and hence $|PQ|$ is a multiple of both 7 and 103. Thus, $|PQ| = 721$ and so $G = PQ$.

Hence, $G = P \times Q \approx \mathbb{Z}/103\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. If $x = (1, 1) \in G$, then $7x = (7, 7) = (7, 0)$. Also, $103x = (103, 103) = (0, 5)$. Hence, the order of x cannot be 7 or 103, and so the order of x is 721 and so G is cyclic.

9. (19 points). Let R be the set of continuous functions $f : [0, 1] \to \mathbb{R}$, and define addition and multiplication on R by setting

$$(f + g)(x) = f(x) + g(x), (f \cdot g)(x) = f(x) \cdot g(x).$$

(a) (8 points). List the properties that would need to be checked to prove that R is a ring.

We'd need to check closure under addition, associativity of addition, the existence of an additive identity, additive inverses, and commutativity of addition. We'd need to check commutativity and associativity of multiplication, the existence of a multiplicative identity, and the distributive law.

(b) (6 points). Let $\phi : R \to \mathbb{R}$ be given by $\phi(f) = f(1/2)$. Prove that ϕ is a homomorphism.

We have $\phi(f + g) = (f + g)(1/2) = f(1/2) + g(1/2) = \phi(f) + \phi(g)$, $\phi(f \cdot g) = (f \cdot g)(1/2 = f(1/2) \cdot g(1/2) = \phi(f) \cdot \phi(g)$. Finally, if $f(x) = 1$ is the identity of R, then $\phi(f) = f(1/2) = 1$ is the identity of $\mathbb{R}$.

(c) (5 points). Is $\ker \phi$ a principal ideal of R? [Hint: You may use that if $f(x) \in R$, then $f(x)^{1/3} \in R$.]

Let $I = \ker \phi$. I claim that I is not principal. Suppose to the contrary that $I = (f(x))$ is principal.

Claim: If $y \neq 1/2$, $f(y) \neq 0$.

Proof: Suppose to the contrary that $f(y) = 0$ for some $y \neq 1/2$. We have $g(x) = x - 1/2 \in I$. By assumption, $g(x) = h(x)f(x)$ and so $0 \neq y - 1/2 = h(y)f(y)$, but $f(y) = 0$. This is a contradiction. QED Claim

Now, we have $f(1/2)^{1/3} = 0$ and so $f(x)^{1/3} \in I$. Thus, $f(x)^{1/3} = f(x)h(x)$ for some $h(x) \in R$. This implies that $f(x)^{1/3} = (f(x)^{1/3})^3 h(x)$ and so

$$f(x)^{1/3} \left(1 - f(x)^{2/3} h(x)\right) = 0.$$

Since $f(x)$ is not equal to zero if $x \neq 1/2$, we have that $1 = f(x)^{2/3} h(x)$ for $x \neq 1/2$ and so

$$h(x) = \begin{cases} f(x)^{-2/3} & x \neq 1/2 \\ c & x = 1/2. \end{cases}$$

However, we have $\lim_{x \to 1/2} f(x) = 0$ and so $\lim_{x \to 1/2} h(x)$ does not exist. This contradicts that $h(x) \in R$.

10. (19 points). Suppose that R and S are rings and $\phi : R \to S$ is a surjective ring homomorphism with $\ker \phi = I$. Prove that if J is a *prime* ideal of R containing I, then $\phi(J)$ is a prime ideal of S.

Suppose that $a, b \in S$ and $ab \in \phi(J)$. To prove that $\phi(J)$ is prime, we must show that either $a \in \phi(J)$ or $b \in \phi(J)$.

Since ϕ is surjective, we have $a = \phi(\alpha)$ and $b = \phi(\beta)$ for some $\alpha, \beta \in R$. We have $ab \in \phi(J)$ and so $\alpha\beta = \phi^{-1}(ab) \in \phi^{-1}(\phi(J)) = J$. [The equality of $\phi^{-1}(\phi(J))$ and J comes from the correspondence theorem.]

It follows that either $\alpha \in J$ or $\beta \in J$ and so either $a = \phi(\alpha)$ or $b = \phi(\beta)$ are in $\phi(J)$.

[Another way to argue would be that R/J is isomorphic to $S/\phi(J)$, and since J is a prime ideal of R, R/J is an integral domain. Thus, $S/\phi(J)$ is an integral domain, and so $\phi(J)$ must be a prime ideal of S.]

11. (10 points). Please wait to answer this question until you have finished your work on all other problems on the exam. You may also work on this question once the three hours alloted for the final exam have finished.

Please comment on your understanding of each of the first ten problems on this exam. Did you finish the problem? If so, are you confident that your work is correct? [One point will be for each problem. If your work is correct and you are confident, then you'll earn 1 point for that problem. If either your work is correct and you're not confident, or you say you're confident and your work is not correct, you don't get the point. If you don't finish or you say you're not confident and your work is incorrect, you get the point.]

When I this exam in practice, I made a few mistakes. I somehow forgot to prove that conjugacy was an equivalence relation in part 2(a). I was not confident in my answer to 2(c). Finally, I completely blanked on the proof of the second Sylow theorem in problem 7. I invented a new proof that was significantly more complicated than the one in the book. [I'm confident that this new proof is correct, but the proof I've included in these solutions is the one from the book.]