Math 721 - Final Exam Version 2 - 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) (5 points). If G is a group, and H is a subset of G, describe the process you would use to prove that H is a subgroup of G.

It would be necessary to show that if $a, b \in H$, then $ab \in H$, that $1 \in H$, and that if $a \in H$, then $a^{-1} \in H$.

(b) (5 points). What does it mean for a subgroup N of G to be a normal subgroup? What is the relation between normal subgroups and kernels of homomorphisms?

A subgroup N of G is normal if for all $g \in G$ and all $n \in N$, $gng^{-1} \in N$. The kernel K of a homomorphism is a normal subgroup, and for any normal subgroup N of G, the homomorphism $\phi : G \to G/N$ given by $\phi(g) = gN$ has kernel N.

(c) (5 points). Show that if G is an abelian group, then every subgroup of G is normal.

If G is abelian and H is a subgroup of G, then if $g \in G$ and $h \in H$ then $ghg^{-1} = gg^{-1}h = 1h = h \in H$. Hence, H is normal in G.

(d) (4 points). Is it true that if G is a group with the property that every subgroup of G is a normal subgroup, then G is abelian?

No, it is not. If G is the group of quaternions $\{\pm 1, \pm i, \pm j, \pm k\}$, then $|G| = 8$. By Lagrange's theorem, if H is a subgroup of G, $|H| = 1$, 2, 4, or 8. If $|G : H| = 2$, then H is normal (by a previous homework problem). Since $\pm i$, $\pm j$ and $\pm k$ all have order 4, the only subgroup of order 2 is $\{\pm 1\}$ which is $Z(G)$ and so it is normal. Thus, every subgroup of G is normal, but G is not abelian since $ij = k$ and $ji = -k$.

2. (19 points).

(a) (4 points). What does it mean for G to act (or operate) on a set S?

This means that for each element $g \in G$ and $s \in S$, there is an element $g * s \in S$. We also need the properties that $g_1 * (g_2 * s) = g_1 g_2 * s$ for all $g_1, g_2 \in G$ and $s \in S$, and also that $1 * s = s$ for all $s \in S$.

(b) (7 points). What does it mean for an action to be transitive? What does it mean for an action to be faithful?

An action is transitive if for every pair $s_1, s_2 \in S$, there is an element $g \in G$ so that $g * s_1 = s_2$. An action is faithful if when $g * s = s$ for all $s \in S$, then $g = 1$.

(c) (8 points). How does a group action give rise to a homomorphism?

If $g \in G$, let $m_g : S \to S$ be given by $m_g(s) = g * s$. This is a permutation of S. Moreover, the map $\phi : G \to \mathrm{Perm}(S)$ given by $\phi(g) = m_g$ is a homomorphism. This is how a group action gives rise to a homomorphism.

3. (19 points).

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

A ring is a set R together with two binary operations ($+$ and $\cdot$) on it so that R is an abelian group with respect to the operation $+$, R is closed under $\cdot$, and $\cdot$ is commutative and associative, and we have that $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$.

(b) (7 points). What is a unit in a ring? Prove that the set S of units in a ring R is an abelian group (under multiplication).

A unit in a ring R is an element r so that $rs = 1$ for some $s \in R$. If $r_1, r_2 \in S$, then there are $s_1, s_2 \in S$ so that $r_1 s_1 = r_2 s_2 = 1$. Then, $(r_1 r_2)(s_2 s_1) = 1$ and so $r_1 r_2 \in S$. The associativity of multiplication is one of the ring axioms, and so this follows. We have that $1 \cdot 1 = 1$ and so $1 \in S$. Also, 1 is the multiplicative identity of R and so it is the identity in S. Finally, for any $r \in S$, we have $rs = 1$ and so $s = r^{-1}$. Note that $rs = 1$ implies that $sr = 1$ since multiplication is commutative.

(c) (6 points). Is there a ring that is not a field? Is there a field that is not a ring? [If the answer to either question is yes, give an example. If the answer to either question is no, explain why.]

There is a ring that is not a field, namely $\mathbb{Z}$. The element $2 \in \mathbb{Z}$ is nonzero, but it is not a unit since $1/2 \notin \mathbb{Z}$. In a field, every nonzero element must be a unit.

Every field is a ring, since a field is a ring in which every nonzero element is a unit.

4. (19 points). Suppose that G is a group with the property that for every subgroup H of G, $Z(H) \subseteq Z(G)$. Prove that G is abelian.

If $x \in G$, then let $H = \langle x \rangle$. Then, H is cyclic and so H is abelian. It follows that $x \in Z(H) \subseteq Z(G)$ and so $x \in Z(G)$. Thus, for any element $x \in G$, $x \in Z(G)$ and so $G = Z(G)$ and so G is abelian.

[There was some confusion on this problem, since the book sometimes uses the notation $Z(g)$ to denote the centralizer of an element $g \in G$. I didn't take points of if students assumed that $Z(H)$ means the centralizer of H in G - the result is still true in this case, but the proof is different. One can prove that $Z(H) = Z(G)$ for all subgroups H of G. Then taking $H = \{1\}$ we see that $G = Z(H) = Z(G)$ and so G is abelian.]

5. (19 points). Is it true that if G is a finite group and N is a normal subgroup of G, then

$$G \approx N \times G/N?$$

Either prove the statement is always true, or give an example of G and N where the statement is false.

This statement is false. Let $G = \mathbb{Z}/4\mathbb{Z}$, $N = \{0, 2\}$. Then, $|N| = 2$, $|G/N| = |G|/|N| = 2$ and so N and G/N are both cyclic. It follows that the right hand side is $N \times G/N \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This group contains the identity and three elements of order 2, $(1, 0)$, $(0, 1)$ and $(1, 1)$. However, G itself contains elements of order 4 and so G and $N \times G/N$ are not isomorphic.

6. (19 points).

(a) (6 points). How many elements of order 11 are there in A_{11}?

An element of order 11 in A_{11} must be an 11-cycle. Any 11-cycle can be written uniquely to start with a 1. For the next number in the cycle there are 10 choices. For the number after that there are 9, etc. Therefore there are 10! elements of order 11 in A_{11}. [Note that an 11-cycle is an even permutation, since every odd cycle is even.]

(b) (6 points). How many Sylow 11-subgroups does A_{11} have?

A Sylow 11-subgroup of A_{11} has order 11. It must contain 10 elements of order 11, and the identity. Moreover, if P_1 and P_2 are two different Sylow 11-subgroups of G, then $|P_1 \cap P_2| < 11$ and since by Lagrange's theorem the order of $P_1 \cap P_2$ must divide 11, we have that $P_1 \cap P_2 = 1$. Hence, an element of order 11 is contained in a unique subgroup of order 11 and so G contains $10!/10 = 9!$ Sylow 11-subgroups.

(c) (7 points). If P is a Sylow 11-subgroup of A_{11}, what is the order of the normalizer of P in A_{11}?

We have that $n_{11}(A_{11}) = |G : N_{A_{11}}(P)| = 9!$. Thus

$$|N_{A_{11}}(P)| = \frac{|G|}{|G : N_{A_{11}}(P)|} = \frac{11!/2}{9!} = \frac{11 \cdot 10}{2} = 55.$$

7. (19 points). Prove the third Sylow theorem. That is, prove that if G is a finite group with $|G| = p^e m$ where p is a prime number and $p \nmid m$, then $n_p(G)$, the number of Sylow p-subgroups of G satisfies $n_p(G)|m$ and $n_p(G) \equiv 1 \pmod{p}$. [You may use the first and second Sylow theorems in your proof.]

Let P be a Sylow p-subgroup of G. The number of conjugates of P is equal to the index of the stabilizer of P (when G acts on the conjugates of P by conjugation). This stabilizer is $N_G(P)$ and so the number of conjugates of P is $|G : N_G(P)|$. By the second Sylow theorem, all Sylow p-subgroups of G are conjugate, and so $n_p(G) = |G : N_G(P)|$. Since $P \subseteq N_G(P)$, we have that $p^e || N_G(P)|$ and so $|N_G(P)| = p^e n$. Since $|N_G(P)|$ divides $|G|$ we have that $n|m$. Thus,

$$n_p(G) = \frac{p^e m}{p^e n} = \frac{m}{n}$$

is a divisor of m.

Let P itself act by conjugation on the set of Sylow p-subgroups of G. Each orbit of this action has order a divisor of $|P|$ and so each orbit either has size 1, or has size a multiple of p. It suffices to count the orbits of size 1. Suppose that Q is an orbit of size 1. Then, $pQp^{-1} = Q$ for all $p \in P$ and so $P \in N_G(Q)$. Applying the second Sylow theorem to $N_G(Q)$, we see that Q must be conjugate to P in $N_G(Q)$. That is, there is a $g \in N_G(Q)$ so that $gQg^{-1} = P$. However, since $g \in N_G(Q)$, $gQg^{-1} = Q = P$ and so $P = Q$. This shows that P has exactly one fixed point acting on the set of Sylow p-subgroups of G, and so $n_p(G) \equiv 1 \pmod{p}$, as desired.

8. (19 points). Prove that if $|G| = 324$, then G is not simple.

We have $|G| = 2^2 \cdot 3^4$. We have $n_3(G)|4$ and $n_3(G) \equiv 1 \pmod 4$. Thus, $n_3(G) = 1$ or $n_3(G) = 4$. Let P be a Sylow 3-subgroup of G.

If $n_3(G) = 1$, then $P \trianglelefteq G$, which means G cannot be simple. If $n_3(G) = 4$, then if $H = N_G(P)$, then $|G : H| = 4$. If G acts on the left cosets of H this gives a homomorphism $\phi : G \to S_4$. We have $\ker \phi \subseteq H$ and ϕ cannot be injective because $|G| = 324$ does not divide 24. Thus, $N = \ker \phi$ is a non-trivial normal subgroup of G and so G is not simple.

9. (19 points). Give an example of a ring R and two different ideals I_1 and I_2 of R so that R/I_1 and R/I_2 are isomorphic.

Let $R = \mathbb{R}[x, y]$, $I_1 = (x)$ and $I_2 = (y)$. Let $\phi_1 : R \to \mathbb{R}[y]$ be given by $\phi_1(p(x, y)) = p(0, y)$ and $\phi_2 : R \to \mathbb{R}[x]$ be given by $\phi_2(p(x, y)) = p(x, 0)$.

Claim: $\ker \phi_1 = I_1$ and $\ker \phi_2 = I_2$.

Proof: If $p \in \ker \phi_1$, then $p(0, y) = 0$. If we represent $p(x, y) \in \mathbb{R}[y][x]$, say

$$p(x, y) = c_0(y) + c_1(y)x + c_2(y)x^2 + \cdots + c_n(y)x^n$$

then $p(0, y) = 0$ means that $c_0(y) = 0$. Hence

$$p(x, y) = c_1(y)x + c_2(y)x^2 + \cdots + c_n(y)x^n = x(c_1(y) + c_2(y)x + \cdots + c_n(y)x^{n-1}) \in I_1.$$

A completely analogous argument shows that $\ker \phi_2 = I_2$.

By the first isomorphism theorem for rings, $R/I_1 \approx \mathbb{R}[y]$ and $R/I_2 \approx \mathbb{R}[x]$ (since ϕ_1 and ϕ_2 are both surjective). Thus, $R/I_1 \approx R/I_2$ since the map $\psi : \mathbb{R}[x] \to \mathbb{R}[y]$ given by

$$\psi\left(a_0 + a_1x + \cdots + a_nx^n\right) = a_0 + a_1y + \cdots + a_ny^n$$

is an isomorphism.

On the other hand, $I_1 \neq I_2$, since $y \notin I_1$. If $y \in I_1$ then $\phi_1(y) = y = 0$, and this is a contradiction.

[Another slightly more complicated example is $R = \mathbb{Z}[x]$, $I_1 = (x^2 + 1)$ and $I_2 = (x^2 + 2x + 2)$. Then $R/I_1 \approx \mathbb{Z}[i] \approx \mathbb{Z}[1+i] \approx R/I_2$, but again $I_1 \neq I_2$. Other examples are ones like $R = \mathbb{F}_2[x]$, $I_1 = (x)$, $I_2 = (x + 1)$. Finally, one can even find an example where I_1 is a subset of I_2, but this requires R to be a polynomial ring in infinitely many variables.]

10. (19 points). Identify the ring $R = \mathbb{Z}[x]/(x^2+1, 2)$. (Describe the ring R as accurately and precisely as you can. Is it finite? Is it infinite? Is it a field?)

Let $\mathcal{R} = \mathbb{F}_2[x]$ and let $\phi : R \to \mathcal{R}$ be the reduction mod 2 homomorphism. We have $f \in \ker \phi$ if and only if all its coefficients are even. This means $f = 2g$ for $g \in \mathbb{Z}[x]$ and so $\ker \phi = (2)$.

Let $I = (x^2+1, 2)$. Since $\ker \phi$ contains I, and ϕ is surjective, the correspondence theorem for rings gives that $R/I \approx \mathcal{R}/\mathcal{I}$, where $\mathcal{I} = \phi(I) = (x^2+1)$. Thus, $R/I \approx \mathbb{F}_2[x]/(x^2+1)$.

If $f \in \mathbb{F}_2[x]$, we may write $f(x) = (x^2+1)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) \leq 1$ and is unique. In $\mathbb{F}_2[x]/(x^2+1)$, we have $f(x) + \mathcal{I} = r(x) + \mathcal{I}$ (because $f(x) - r(x) \in \mathcal{I}$). Hence, $\mathbb{F}_2[x]/(x^2+1)$ has four elements. Moreover, since $x^2+1 = x^2+2x+1 = (x+1)^2$ in $\mathbb{F}_2[x]$, $(x+1)$ is an ideal larger than (x^2+1) and so (x^2+1) is not a maximal ideal and $\mathbb{F}_2[x]/(x^2+1)$ is not a field. The four elements are 0, 1, x and $x+1$, where addition is done modulo 2. For multiplication, we have $x^2 = x^2+1-1 = 0-1 = -1 = 1$, $x(x+1) = x^2+x = x+1$ and $(x+1)^2 = x^2+2x+1 = 0$.

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.]

I feel confident that all of my answers are complete and correct.