Math 120. Groups and Rings
Midterm Exam (November 8, 2017)

2 Hours

Name: _______________________

Please read the questions carefully. You will not be given partial credit on the basis of having misunderstood a question, and please show all work.

If your solution does not fit in the indicated space, please use the back of the same page. This is a closed book exam.

There are 7 questions giving a total of 105 points in this midterm.

You must sign below (indicating your agreement with) the following honor pledge: I pledge my honor that I have not used electronic machines of any sort, contact with other human beings, or any references for mathematical assistance in connection with my work on this exam.

<table>
<thead>
<tr>
<th>Question</th>
<th>Possible</th>
<th>Actual</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>105</td>
<td></td>
</tr>
</tbody>
</table>
1. The cycle type of a permutation $\sigma \in S_n$ is the list $(m_1, \ldots, m_r)$, where the $m_i$ are the lengths of disjoint cycles in the complete factorization of $\sigma$, ordered such that $m_1 \leq m_2 \leq \ldots \leq m_r$.

(i) (10 pts) Suppose two permutations $\sigma$ and $\sigma'$ in $S_n$ are conjugate (i.e. $\sigma' = g \sigma g^{-1}$ for some $g \in S_n$). Show that $\sigma$ and $\sigma'$ have the same cycle type.

**Answer:** If $\alpha, \beta \in S_n$ then $(g \alpha g^{-1})(g \beta g^{-1}) = g \alpha \beta g^{-1}$. Now observe
\[ g(\alpha_1, \ldots, \alpha_r)g^{-1} = (g(\alpha_1), \ldots, g(\alpha_n)). \]
Thus if $(\alpha_1, \ldots, \alpha_r)$ is an $r$-cycle, then $g(\alpha_1, \ldots, \alpha_r)g^{-1}$ is an $r$-cycle, and disjoint cycles are left disjoint under conjugation.

This formula will be used again in Q2.

(i) (5 pts) Show that any two 3-cycles in $A_n$ are conjugate for $n \geq 5$.

**Answer:** See notes to Lecture 12, page 1.
2. (i) (12 pts) Show that $S_n$, $n \geq 2$ is generated by the two elements $(1, 2, \ldots, n)$ and $(1, 2)$.

**Answer:** We need to show $\langle (1, 2, \ldots, n), (1, 2) \rangle$ includes all permutations $(i, j)$. Applying the formula we worked out in the course of Q1(i),

$$(1, \ldots, n)(i, i + 1)(1, \ldots, n)^{-1} = (i + 1, i + 2),$$

so $\langle (1, 2, \ldots, n), (1, 2) \rangle$ includes $(1, 2), (2, 3), \ldots, (n - 1, n)$. Next $(2, 3)(1, 2)(2, 3)^{-1} = (1, 3), (3, 4)(1, 3)(3, 4)^{-1} = (1, 4)$ etc, so $\langle (1, 2, \ldots, n), (1, 2) \rangle$ includes $(1, 2), (1, 3), \ldots, (1, n)$. Lastly, $(i, j) = (1, i)(1, j)(1, i)^{-1}$.

(ii) (3 pts) Show that the alternating group $A_n$ is generated by 3-cycles for $n \geq 3$.

**Answer:** See notes to Lecture 12, page 2.
3. (i) (2 pts) Show $S_n$ has the same number of even permutations as of odd permutations.

   **Answer:** See notes to Lecture 9, page 7.

   (ii) (2 pts) Let $H$ be a subgroup of a group $G$. Show that the number of *left* cosets of $H$ in $G$ equals the number of *right* cosets of $H$.

   **Answer:** See notes to Lecture 6, page 8.

   (iii) (2 points) Do there exist groups of infinite order such that each element has *finite* order? Justify with either a proof or an example.

   **Answer:** Yes, e.g. $\mathbb{Q}/\mathbb{Z}$.

   (iv) (2 pts) Show that if $G$ is a group such that every non-identity element has order 2, then $G$ is abelian.

   **Answer:** We have $a^{-1} = a$ for all $a \in G$. So $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.

   (v) (3 pts) State and prove the Class Equation on the order of a finite group.

   **Answer:** See notes to Lecture 13, page 9.


   **Answer:** See notes to Lecture 15, page 9.
4. (i) (10 pts) A Mersenne prime is a prime number \( p = 2^n - 1 \) for some integer \( n \). Suppose \( 2^n - 1 \) is a Mersenne prime and \( G \) is a finite group of order \( 2^n(2^n - 1) \). Show that \( G \) is not simple.

Answer: Suppose \( G \) is simple. Then \( n_p > 1 \), \( n_p = 1 \mod p \) and \( n_p \) divides \( |G| \), so \( n_p = 2^n \). This gives \( 2^n(p-1) \) elements of order \( p \). But any Sylow 2-group has \( 2^n \) elements, none of which have order \( p \), so we have found \( |G| = 2^n(p-1) + 2^n \) elements. In particular, \( n_2 = 1 \) contradicting that \( G \) is simple.

(ii) (5 pts) Prove if that if a prime number \( p \) does not divide an integer \( a \) then \( a^{p-1} = 1 \mod p \).

Answer: See notes to Lecture 8, page 7.
5. (i) (6 pts) Let $H$ be a finite abelian $p$-group, for a prime $p$ (i.e. $|H| = p^n$ for some $n \geq 1$). Let $r_H$ denote the number of elements of order $p$ in $H$. Show $r_H = -1 \mod p$.

**Answer:** The set $S = \{1\} \cup \{\text{elements of order } p\}$ forms a subgroup, hence $|S| = 0 \mod p$ and thus $1 + r_H = 0 \mod p$.

(ii) (1 pt) Let $G$ be a finite $p$-group, not necessarily abelian. If $g \in G$ has order $p$, show the same is true for all of its conjugates $hgh^{-1}$, $h \in G$.

**Answer:** $(hgh^{-1})^p = hg^p h^{-1}$.

(iii) (6 pts) Let $G$ be as in (ii). Show that the number of elements $r_G$ of order $p$ in $G$ satisfies $r_G = -1 \mod p$.

**Answer:** The number of elements $x \in Z(G)$ of order $p$ equals $-1$ modulo $p$. Now suppose $x \notin Z(G)$ has order $p$. By the above, its entire conjugacy class consists of elements of order $p$, and this conjugacy class has size a positive power of $p$, i.e. this class has size equal to 0 modulo $p$. Thus $r_G = -1 \mod p$. 

(iv) (2 pts) Let $G$ be as in (ii), (iii). Let $S_G$ be the number of subgroups of $G$ of order $p$. Show $S_G = 1 \mod p$.

**Answer:** By the usual counting trick, $S_G(p - 1) = r_G$ which immediately gives the claim.
6. (i) (5 pts) Let \( G \) be a group and let \( Z(G) = \{g \in G \mid hg = gh \text{ for all } h \in G\} \) denote the center. Prove that if \( G/Z(G) \) is cyclic then \( G \) is abelian.

**Answer:** This is done in Lecture 14, page 5.

(ii) (5 pts) Let \( G \) be a finite \( p \)-group, for a prime \( p \) (i.e. \( |G| = p^n \) for \( n \geq 1 \)). Show that \( Z(G) \) is non-trivial.

**Answer:** This is done in Lecture 14, page 4.

(iii) (5 pts) Let \( G \) be a group of order \( p^2 \), for a prime \( p \). Show that \( G \) is abelian.

**Answer:** This is done in Lecture 14, page 4.
7. Let $F$ be a field and consider the polynomial ring $F[x]$ in one variable. Recall that for any $\alpha \in F$, the evaluation homorphism $ev_\alpha : F[x] \to F$ is defined by $ev_\alpha(p(x)) = p(\alpha)$ for any polynomial $p(x) \in F[x]$.

(i) (3 points) Prove that the kernel of $ev_\alpha$ is the ideal $(x - \alpha) = \{r(x - \alpha) \mid r \in F[x]\}$.

You may use without proof the following fact: any ideal $I \subseteq F[x]$ is generated by a single polynomial $f(x) \in F[x]$, i.e. $I = (f(x))$.

**Answer:** The kernel is not everything (why?), so ker($ev_\alpha$) = $(f(x))$ where deg($f$) > 0 and $(x - \alpha) \in$ ker($ev_\alpha$), so $(x - \alpha) = g(x)f(x)$. Comparing degrees, must have deg($g$) = 0 so $(x - \alpha) = (f(x))$.

(ii) (2 points) A root of a polynomial $p(x) \in F[x]$ is an element $\alpha \in F$ such that $ev_\alpha(p(x)) = 0$.

Let $p(x) \in F[x]$. Show that we may write $p(x) = q(x)r(x)$ for polynomials $q(x), r(x) \in F[x]$ with deg $q(x) = 1$ if and only if $p(x)$ has a root in $F$ (deg denotes the degree of the polynomial).

**Answer:** If $p(x)$ has a root $\alpha$, $p(x) \in (x - \alpha)$ by (i) so $p(x) = (x - \alpha)r(x)$. Conversely, if $p(x) = (x - \alpha)r(x)$ for some $\alpha$ then obviously $p(x)$ has a root $\alpha$. 
(iii) (10 points) A polynomial \( p(x) \in F[x] \) is said to be irreducible if there do not exist polynomials \( q(x), r(x) \in F[x] \) with \( \deg q(x) \geq 1, \deg r(x) \geq 1 \) and \( p(x) = q(x)r(x) \).

Let \( F = \mathbb{Z}/2\mathbb{Z} \). Find all irreducible polynomials \( p(x) \in F[x] \) with \( \deg(p(x)) \leq 4 \).

**Answer:** This was intended mostly as a bonus question (a few people did at least sincerely attempt it).

Firstly, the constant polynomials 0, 1 and the linear polynomials \( x, x+1 \) are irreducible. For higher degrees, note that by (ii) any irreducible polynomial has no roots, i.e. \( f(0) \neq 0 \) (so the constant term is nonzero) and \( f(1) \neq 0 \). So let \( f(x) = x^2 + ax + 1 \) be a quadratic. It is irreducible if and only if \( f(1) \neq 0 \) (using (ii)), which happens precisely for \( x^2 + x + 1 \). For cubics \( f(x) = x^3 + ax^2 + bx + 1 \), then again (ii) shows \( f(x) \) is irreducible if and only if \( f(1) \neq 0 \) (*why?*), so \( x^3 + x^2 + 1, x^3 + x + 1 \) are all the irreducible cubics.

Lastly consider quartics \( f(x) = x^4 + ax^3 + bx^2 + cx + 1 \) with \( f(1) \neq 0 \) (which is necessary, but no longer sufficient, for irreducibility). By (ii) the only way such an \( f(x) \) could fail to be irreducible is if \( f(x) = g(x)h(x) \) for two quadratics with no roots, i.e. we must have \( f(x) = (x^2 + x + 1)^2 = x^4 + x^2 + 1 \). Thus \( x^4 + x^3 + x^2 + x + 1, x^4 + x^3 + 1, x^4 + x + 1 \) are all the irreducible quartics.