Math 236H  Final exam  
May 4, 2010

Be sure to write your name on your bluebook. Use a separate page (or pages) for each problem. Show all of your work.

1. (10 points) Let \( f(x) = x^4 + 7x^2 + rx + 1 \in \mathbb{Z}[x] \). For which integers \( r \) is \( f(x) \) irreducible? Prove your answer.

Solution: If \( a \) is a zero of \( f(x) \), then \( x - a \) is a factor of \( f(x) \), \( f(a) = 0 \) and \( a \) must be \( \pm 1 \) since the constant term in \( f(x) \) is one. Since \( f(1) = 9 + r \), and \( f(-1) = 9 - r \), \( f(x) \) has a zero if \( r = \pm 9 \). The factorizations are

\[
\begin{align*}
x^4 + 7x^2 + 9x + 1 &= (x + 1)(x^3 - x^2 + 8x + 1) \\
and \quad x^4 + 7x^2 - 9x + 1 &= (x - 1)(x^3 + x^2 + 8x - 1).
\end{align*}
\]

Now suppose that \( f(x) \) has two quadratic factors,

\[
f(x) = (x^2 + ax + b)(x^2 + cx + d)
= x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd.
\]

The coefficient of \( x^3 \) is zero, so \( c = -a \) and we have

\[
f(x) = x^4 + (b + d - a^2)x^2 + a(b - d)x + bd.
\]

Since \( bd = 1 \), \( b = d = \pm 1 \), and the coefficient of \( x \) is zero. This means that \( r = 0 \) and the coefficient of \( x^2 \) is \(-a^2 \pm 2 = 7 \), or \( a^2 = -7 \pm 2 < 0 \), but there is no integer \( a \) that satisfies this condition. Therefore, \( f(x) \) is irreducible unless \( r = \pm 9 \).

2. (10 points) Prove that in a finite \( G \)-set \( X \), if \( g \) and \( g' \) are conjugate elements in \( G \), then their fixed point sets \( X_g \) and \( X_{g'} \) have the same cardinality.

Solution: Since \( g' \) is conjugate to \( g \), \( g' = hgh^{-1} \) for some \( h \in G \). Now suppose \( x \in X_g \).

Then

\[
g'(h(x)) = hgh^{-1}h(x) = hg(x) = h(x),
\]

so \( h(x) \in X_{g'} \). Similarly, if \( x' \in X_{g'} \), then \( h^{-1}(x') \in X_g \). Hence the action of \( h \) gives a one-to-one correspondance between \( X_g \) and \( X_{g'} \), so \( |X_g| = |X_{g'}| \).
3. (15 points) You are painting blocks that are shaped like regular tetrahedra. Each block has four triangular faces. You have \( n \) colors to choose from for each of the 4 faces. Use Burnside’s formula to determine the number of distinguishable blocks that can be made in this way. How big does \( n \) have to be in order to get 50 distinguishable blocks?

**Solution:** The symmetry group of the tetrahedron (which is isomorphic to \( A_4 \)) consists of the identity element, 3 edge centered rotations and 8 vertex/face centered rotations. Our \( A_4 \)-set has \( n^4 \) elements. Each nontrivial element fixes \( n^2 \) of them. It follows that Burnside’s sum is \( n^4 + 11n^2 \), so the number of orbits is \( (n^4 + 11n^2)/12 \). The following table shows this number for small \( n \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>( (n^4 + 11n^2)/12 )</td>
<td>1</td>
<td>5</td>
<td>15</td>
<td>25</td>
<td>75</td>
</tr>
</tbody>
</table>

Hence we need 5 colors to get 50 distinguishable blocks.

4. (15 points) Prove that every finite integral domain \( D \) is a field.

**Solution:** Suppose \( |D| = n \) and

\[
D = \{0, 1, a_1, a_2, \ldots a_{n-2}\},
\]

so the set of nonzero elements in \( D \) is

\[
D^* = \{1, a_1, a_2, \ldots a_{n-2}\}
\]

For \( x \in D^* \), consider the set

\[
xD^* = \{x, xa_1, xa_2, \ldots xa_{n-2}\}.
\]

Since \( D \) is a domain, this set does not contain 0. Its elements are all distinct since \( xa_i = xa_j \) for \( i \neq j \) would mean \( x(a_i - a_j) = 0 \), which would make \( x \) a zero divisor. Hence \( xD^* \) has all \( n - 1 \) nonzero elements of \( D \), including 1. This means that \( x \) has an inverse, so \( D \) is a field.

5. (15 points) Recall that the third Sylow theorem says that if \( |G| = ps \) where \( p \) is prime and does not divide \( s \), then the number \( k_p \) of subgroups of order \( p \) divides \( s \) and is congruent to 1 modulo \( p \). Use it to prove that every group \( G \) of order 665 = 5 \cdot 7 \cdot 19 \) is cyclic.
Solution: For each of the three primes \( p \) dividing 665, there is a unique subgroup \( C_p \) of order \( p \), so it is normal. The order of quotient group is the product of the other two primes, and in each case Theorem 37.7 applies and says that it is abelian. (It is not true in general that a group \( H \) whose order is the product of 2 primes \( p \) and \( q \) is abelian. For example, \( |S_3| = 2 \cdot 3 \) but \( S_3 \) is not abelian. However such an \( H \) is abelian if neither prime is congruent to 1 modulo the other one.) This means that each \( C_p \) contains the commutator subgroup \( C(G) \). Hence \( C(G) \) is in the intersection of the three subgroups of prime order, so it is trivial. This means that \( G \) is abelian and hence cyclic.

An alternate approach is to show there is an element of order 665, which would make the group cyclic. This can be done by showing that not all elements of \( G \) have order less than 665. We know there is a single element of order 1 and \( p - 1 \) elements of order \( p \) for each of the three primes \( p \). There can be at most one subgroup of order 35 = 5 ⋅ 7, 95 = 5 ⋅ 19 or 133 = 7 ⋅ 19, because in each case multiple subgroups of any of these orders would lead to multiple subgroups of prime order. Thus the number of elements of order \( pq \) is less than \( pq \). The order of any element must divide 665, and there are fewer than 665 elements of order less than 665.

6. (10 POINTS) Find the largest integer \( m \) which divides \( n^{13} - n \) for all integers \( n \).

Solution: We will use Fermat’s little theorem, which says that if a prime \( p \) does not divide \( n \), then \( n^{p-1} \equiv 1 \mod p \). Since

\[
n^{13} - n = n(n^{12} - 1),
\]

if \( p - 1 \) divides 12, then \( n^{13} - n \) is divisible by \( p \). The primes \( p \) for which this is true are 2, 3, 5, 7 and 13. This means that \( n^{13} - n \) is always divisible by their product, 2730. For any other prime \( q \) there is an \( n \) such that neither \( n \) nor \( n^{12} - 1 \) are divisible by \( q \). For any prime \( p \), the number \( p^{13} - p = p(p^{12} - 1) \) is divisible by \( p \), but not by \( p^2 \). This means \( m \) is not divisible by the square of any prime (it is square free), so our \( m \) is 2730.

7. (15 POINTS) Let \( G \) be \( C_{30} \) (the cyclic group of order 30) and let \( a \) be a generator (so \( G = \langle a \rangle \)) and let \( e \in G \) be the identity element.

(a) list all elements of \( G \) or order 30.
(b) list all elements of \( G \) or order 10.
(c) list all elements of \( G \) or order 6.
(d) list all elements of \( G \) or order 5.
(e) list all elements of \( G \) or order 4.
(f) list all other elements of \( G \).
**Solution:** We will use additive notation. The answers are

(a) \(a, 7a, 11a, 13a, 17a, 19a, 23a, \) and \(29a.\)

(b) \(3a, 9a, 21a, \) and \(27a.\)

(c) \(5a \) and \(25a.\)

(d) \(6a, 12a, 18a, \) and \(24a.\)

(e) There are no elements of order 4 since 4 does not divide 30.

(f) There are 12 other elements: \(e, 2a, 4a, 8a, 10a, 14a, 15a, 16a, 20a, 22a, 26a, \) and \(28a.\) They have orders 1, 2, 3 and 15.

---

8. (10 POINTS) Let \(G\) be a finite group with a subgroup \(H\) such that \(|G| = 2|H|\).

(a) Prove that if \(a \in G\) is not in \(H\), then \(a^2 \notin H.\) (Hint: it suffices to show that \(a^2H \neq aH.\))

(b) Prove that if \(a\) is not in \(H\), then the order of \(a\) is even. (Hint: Show that \(a^n\) is not in \(H\) for any odd integer \(n\).)

**Solution:**

(a) \(G\) has two left \(H\)-cosets, namely \(H\) itself and its compliment \(G - H.\) If \(aH = a^2H,\) then \(H = aH,\) but if \(a\) is not in \(H,\) then \(aH = G - H.\) Hence \(aH \neq a^2H,\) so \(a^2H = H,\) which means that \(a^2 \in H.\)

(b) For an odd integer \(n = 2m + 1,\) \(a^n = a \cdot a^{2m} \in aH,\) so \(a^n\) is not in \(H.\) This means the order of \(a\) cannot be odd.

---

9. (10 POINTS) Find all primes \(p\) such that \(x + 5\) is a factor of \(f(x) = x^4 + x^2 + 1\) in \(\mathbb{Z}/p[x].\)

**Solution:** \(x + 5\) is a factor of \(f(x)\) in \(\mathbb{Z}/p[x]\) iff \(f(-5) \equiv 0\) modulo \(p.\) We have

\[f(-5) = 5^4 + 5^2 + 1 = 625 + 25 + 1 = 651 = 3 \cdot 7 \cdot 31\]

so the primes are 3, 7 and 31.

---

10. (15 POINTS) Prove that the symmetric group \(S_4\) is generated by the three transpositions \((12), (13)\) and \((14).\)
Solution: We know that $S_4$ is generated by 6 transpositions: the three listed above along with (23), (24) and (34). Thus we need to show that each of these three is a product of the three listed above. Let the four letters being permuted by $A$, $B$, $C$ and $D$. Then we have

\[
\begin{align*}
(A, B, C, D) &\quad (A, B, C, D) &\quad (A, B, C, D) \\
(12) &\quad (12) &\quad (13) \\
(B, A, C, D) &\quad (B, A, C, D) &\quad (C, B, A, D) \\
(13) &\quad (14) &\quad (14) \\
(C, A, B, D) &\quad (D, A, C, B) &\quad (D, B, A, C) \\
(12) &\quad (12) &\quad (13) \\
(A, C, B, D) &\quad (A, D, C, B) &\quad (A, B, D, C)
\end{align*}
\]

These three columns show that (23), (24) and (34) are each products of the three generators.

11. (15 points) Let $p = 2s + 1$ be an odd prime bigger than 3 (so $s > 1$), and let $f(x) = \frac{x(x^s + 3p - 1)(x^s + 1)}{3p}$.

Prove that $f(x)$ is an integer whenever $x$ is.

Solution: This amounts to showing that the numerator is always divisible by three and always divisible by $p$. Modulo three it is

\[x(x^s - 1)(x^s + 1)\]

If $x$ is not divisible by 3, then $x^s \equiv \pm 1$ modulo 3, so the product is always divisible by 3. For divisibility by $p$, note that the numerator is

\[x(x^s + 3p - 1)(x^s + 1) \equiv x(x^s - 1)(x^s + 1) \equiv x^p - x \mod p,\]

and $x^p - x$ is divisible by $p$ by Fermat’s Little Theorem.

12. (15 points) List the even permutations of order 2 in $S_4$ and say how many there are in $S_5$ and $S_6$.

Solution: The only even permutations of order 2 in $S_4$ are the three double transpositions, (12)(34), (13)(24) and (14)(23). Double transpositions are also the only such permutations in $S_5$ and $S_6$. (There are triple transpositions in $S_6$ which have order 2, but they are odd.) In $S_5$ there are three for each of the five subsets with 4 elements, making 15 in all. In $S_6$ there are three for each of the fifteen subsets with 4 elements, making 45 in all.
13. (10 points) Prove that the intersection of two normal subgroups of $G$ is a normal subgroup.

**Solution:** Let $H_1$ and $H_2$ be normal subgroups of $G$. Let $g \in G$ and $h \in H_1 \cap H_2$. Then $ghg^{-1} \in H_1$ since $h \in H_1$, and similarly $ghg^{-1} \in H_2$. Hence $ghg^{-1} \in H_1 \cap H_2$, so $H_1 \cap H_2$ is normal.

14. (10 points) Determine the number of elements of order 4 in
   a. $C_8 \times C_8$
   b. $C_4 \times C_4 \times C_4$

**Solution:**
   a. All elements of order 4 or less are in the subgroup $C_4 \times C_4$, which has order 16, and all elements of order 2 or less are in the subgroup $C_2 \times C_2$, which has order 4, so the number of elements of order 4 is $16 - 4 = 12$.
   
   b. An element of $C_4 \times C_4 \times C_4$ has order 4 if it is not contained in $C_2 \times C_2 \times C_2$. The number of such elements is $4^3 - 2^3 = 56$.

15. (10 points) Prove that if $n$ is an odd integer, then $n^2 \equiv 1$ modulo 8 and $n^4 \equiv 1$ modulo 16.

**Solution:** Let $n = 2k + 1$. Then

\[
\begin{align*}
n^2 &= (2k + 1)^2 = 4k^2 + 4k + 1 \\
&= 4k(k + 1) + 1
\end{align*}
\]

and $k(k + 1)$ is even since it is the product of two consecutive integers. This means that $n^2$ is congruent to 1 modulo 8. Since $n^2 = 8s + 1$, we have

\[
\begin{align*}
n^4 &= (8s + 1)^2 = 64s^2 + 16s + 1 \\
&\equiv 1 \pmod{16}.
\end{align*}
\]