Mathematics 402 Exam

Solutions

1. (10 points) Determine the group of automorphisms of $C_5 = \{1, a, a^2, a^3, a^4 \mid a^5 = 1\}$.

   Solution. By problem 4(a), every homomorphism f from C_5 to itself is determined by where a goes. If $f(a) = 1$, then f sends every element to 1, and this is not an automorphism. Since 5 is prime, a^i is a generator of C_5 when $i = 1, 2, 3, 4$, so if $f(a)$ is any of these, then the resulting homomorphism is an automorphism.

   Thus there are four automorphisms of C_5:

   - f_1, defined by $f_1(a) = a$. This is the identity map, and so is the identity element in the group of automorphisms.
   - f_2, defined by $f_2(a) = a^2$.
   - f_3, defined by $f_3(a) = a^3$.
   - f_4, defined by $f_4(a) = a^4$.

   Since the automorphism group has four elements, it must be isomorphic to either C_4 or to the Klein 4-group, $C_2 \times C_2$. I claim that the element f_2 has order 4:

   $$(f_2 \circ f_2)(a) = f_2(f_2(a)) = f_2(a^2) = a^4,$$

   so $f_2^2 = f_2 \circ f_2 = f_4$.

   $$(f_2 \circ f_2 \circ f_2)(a) = f_2(a^4) = a^8 = a^3,$$

   so $f_2^3 = f_2 \circ f_2 \circ f_2 = f_3$. I can also compute f_2^4 and show that it's the identity map, or I can observe that since I'm working in a group of order 4, the fourth power of every element is the identity. Since no smaller power of f_2 equals f_1, I conclude that f_2 has order 4. Therefore the automorphism group is isomorphic to C_4.

2. (10 points) Let p be a prime number and let G be a group of order p^2. Prove that G is isomorphic to either C_{p^2} or $C_p \times C_p$.

   You may use the following fact (which we will prove later in the quarter): every group of order p^2 is abelian.

   It may also be helpful to recall this fact about products: if H and K are normal subgroups of a group G such that $H \cap K = \{1\}$ and $HK = G$, then $G \approx H \times K$.

   [If you can't do this in general, you can get up to 7 points for doing the case when $p = 3$. If you can't do that, you can get up to 4 points for doing the case when $p = 2$.]

   Solution. By Lagrange's theorem, the order of any element of G must divide $|G| = p^2$. Since p is prime, this means that the orders of the elements of G can be 1, p, or p^2. Only the identity element has order 1, of course, so the other elements all have order p or p^2.

   If G contains an element g of order p^2, then G is cyclic: if g has order p^2, then the cyclic subgroup generated by g has order p^2. Since it's a subgroup of G, and since G has order p^2, it must be all of G.

   Otherwise, every non-identity element of G has order p. Choose some such element h, and let H be the cyclic subgroup generated by h. Then $|H| = p$, and since p is prime, $H \approx C_p$. The elements of

H account for only p of the p^2 elements of G, so there must be other elements in G. So choose some element k which is in G but not in H, and let K be the subgroup generated by k. Since $k \neq 1$ (because $1 \in H$ and $k \notin H$), k has order p; thus $|K| = p$, and $K \approx C_p$.

I want to use the theorem about products described above. First, by the "fact" above, I may assume that G is abelian. Every subgroup of an abelian group is normal, and thus H and K are normal subgroups of G.

Next, $H \cap K$ is a subgroup of K, and so its order must divide $|K| = p$. Since p is prime, this means that $|H \cap K|$ is either 1 or p. If it's p, then $H \cap K = K$, which means that $k \in H \cap K \subseteq H$. But I chose k so that $k \notin H$. Therefore $|H \cap K| = 1$, so $H \cap K = \{1\}$.

Alternatively, suppose that $a \in H \cap K$. Since $a \in H$, then $a = h^i$ for some i. Since $a \in K$, then $a = k^j$ for some j. This means that $h^i = k^j$. Since p is prime, every non-identity element of K generates K, so if $k^j \neq 1$, then some power of k^j equals k; say $k^{jm} = k$. But since $h^i = k^j$, I find that $h^{im} = k$. This is a contradiction, though, because I chose k so that $k \notin H$, and h^{im} is in H.

The last thing I need to do is to show that $HK = G$. There are several ways to do this. One of them is to cite problem 9 in section 2.8. I prefer to use problem 5 in section 2.7: since K is normal (or since H is normal), the product set HK is a subgroup of G. Its order must therefore be 1, p, or p^2. HK contains all of H, and it also contains the element k, so $|HK| > p$. Thus $HK = p^2$, and this means that $HK = G$.

You can also prove this directly: you need to show that the order of HK is p^2. Well, HK is equal to

$$\{h^i k^j | 0 \leq i \leq p-1,\ 0 \leq j \leq p-1\}.$$

If I knew that all of these elements were distinct, then I would have p^2 different elements, and so I could conclude that $HK = G$. So assume that $h^i k^j = h^m k^n$. Rearranging terms, I get $h^{i-m} = k^{n-j}$. The left side of this equation is in H, and the right side is in K; since they're equal, both sides must be in $H \cap K = \{1\}$, so both sides are equal to 1. That means that $h^i = h^m$ and $k^j = k^n$. In other words, as the exponents vary, the elements $h^i k^j$ are distinct.

By the fact about products stated above, I can conclude that $G \approx C_p \times C_p$.

3. (10 points) Prove that 2 has a multiplicative inverse modulo n if and only if n is odd. (By "2 has a multiplicative inverse modulo n," I mean that in $\mathbf{Z}/n\mathbf{Z}$, there exists an element $\bar{k}$ such that $\bar{k}\,\bar{2} = \bar{1}$.)

   Solution. If n is odd, then $n = 2k-1$ for some integer k. So n clearly divides $2k-1$, which means that $2k \equiv 1 \pmod{n}$; therefore if $k = (n+1)/2$, then $\bar{k}$ is the multiplicative inverse of $\bar{2}$ in $\mathbf{Z}/n\mathbf{Z}$.

   If 2 has a multiplicative inverse mod n, then there is an integer k so that $2k \equiv 1 \pmod{n}$. This means that n divides $2k-1$. The number $2k-1$ is odd, and every divisor of an odd number is odd; therefore n must be odd.

4. (10 points) Fix a positive integer n, let C_n be a cyclic group of order n generated by a, and let G be a group.

   (a) Prove that any homomorphism $f : C_n \to G$ is determined by $f(a)$: that is, if you know $f(a)$, you can figure out $f(b)$ for any $b \in C_n$.

   Solution. For any $b \in C_n$, b is of the form $b = a^k$ for some k. Since f is a homomorphism, $f(b) = f(a^k) = [f(a)]^k$. So if I know $f(a)$, I can compute $f(b) = f(a^k)$ just by raising $f(a)$ to its kth power.

(b) In this setting, $f(a)$ cannot be an arbitrary element of G; what restrictions are there on $f(a)$? (Equivalently, what properties must $f(a)$ have?)

Solution. Since a has order n, $a^n = 1$. Apply f: $f(a^n) = f(1) = 1$. Since f is a homomorphism, this means that $[f(a)]^n = 1$. This means that the order of $f(a)$ divides n.

(c) Describe all of the homomorphisms $C_4 \to C_8$. How many of them are onto? How many of them are one-to-one?

Solution. Let $C_4 = \{1, a, a^2, a^3\}$, and let $C_8 = \{1, b, b^2, \cdots, b_7\}$. By part (a), every homomorphism $f : C_4 \to C_8$ is determined by $f(a)$. By part (b), $f(a)$ must have order 1, 2, or 4. We can compute the orders of the elements in C_8:

element	1	b	b^2	b^3	b^4	b^5	b^6	b^7
order	1	8	4	8	2	8	4	8

So there are 4 homomorphisms: $a \mapsto 1$, $a \mapsto b^2$, $a \mapsto b^4$, and $a \mapsto b^6$. None of these is onto; after all, C_4 has 4 elements and C_8 has 8, so there are no surjective functions from C_4 to C_8. The maps $a \mapsto b^2$ and $a \mapsto b^6$ are one-to-one: if a gets sent to b^2, then a^2 gets sent to b^4, a^3 to b^6, and 1 to 1. Thus all elements of C_4 go to different places. The same goes for the map sending a to b^6. (Alternatively, the kernels of these maps are both $\{1\}$.)

The map defined by $a \mapsto 1$ is not one-to-one, because both 1 and a go to 1. The map defined by $a \mapsto b^4$ is not one-to-one, because both 1 and a^2 go to 1.

So there are no onto maps, and two one-to-one maps.