April 15, 2008

Math 320 — Exam III

Make sure your reasoning is clear, that your writing is at least legible, and that I can find your answers to all the questions. TURN OVER — there are five questions.

1. *(24 points)* Which of the following functions are homomorphisms? For those that are, which are monomorphisms, epimorphisms or isomorphisms? For those that are homomorphisms, what are the kernel, the image, and the two groups that are isomorphic according to the Fundamental Theorem of Group Homomorphisms?

   (a) $(\mathbb{R}, +) \to (\mathbb{R}^+, \cdot) : x \mapsto 2^x$

   (b) $(\mathbb{Z}_{12}, \oplus) \to (\mathbb{Z}_{12}, \oplus) : x \mapsto 3x$

   (c) $\det : GL(2, \mathbb{R}) \to \mathbb{R} - \{0\}$

   (d) For a group G and a fixed element a of G, $G \to G : g \mapsto ag$

2. *(20 points)* Let G be a group for which $|G| = 18$.

   (a) What are the possible orders of elements of G?

   (b) We will show that, up to isomorphism, an abelian group must be a direct product of cyclic groups $\mathbb{Z}_q$ where the q's are powers of prime numbers. Up to isomorphism, how are all the abelian groups of cardinality 18 represented in this form?

   (c) We will also show that any group G of cardinality 18 has a subgroup H of cardinality 9 and a subgroup K of cardinality 2. Give short reasons for the following facts:

      (i) H is abelian.

      (ii) H is normal in G.

      (iii) If k is the non-identity element of K, then conjugation by k is its own inverse automorphism.

   (d) Suppose $H = \{a^i b^j : i = 0, 1, 2,\ j = 0, 1, 2\}$ where $a^3 = e = b^3$ and $ab = ba$, and $ka = bk$ (for k as in (c)(iii)). This gives an nonabelian group G of order 18. What is the order of the element $a^i b^j k$? (It may be useful (1) to notice that $H \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, (2) to find kb, and (3) to break into two cases, depending on whether $i + j$ a multiple of 3.)

   (e) We already know of an nonabelian group D_9 of cardinality 18, where $H = \langle f \rangle \cong \mathbb{Z}_9$ and $K = \langle g \rangle$. Is D_9 isomorphic to the group G in (d)? Explain your answer.

3. *(20 points)* Let G be a finite group.

   (a) Explain why, if a subgroup H of G has prime index in G, then there are no subgroups properly between H and G.

   (b) Explain why, if $Z(G)$ is a proper subgroup of G, then there is a subgroup properly between $Z(G)$ and G.

4. *(16 points)* Find the class equation of D_5.

5. *(20 points)* Let G be a group.

(a) Let H, K be subgroups of G. Assume that:

(i) for all h in H and k in K, we have $hk = kh$ (so that $HK = \{hk : h \in H,\ k \in K\}$ is a subgroup of G, but you don't need to prove that),

(ii) $H \cap K = \{e\}$, and

(iii) $HK = G$.

Prove that $H \times K$ is isomorphic to G. (In this case, G is called the "internal direct product" of H and K.)

(b) Suppose G is abelian, let m be a positive integer, and let $H = \{h \in G : o(h)|m\}$. Prove that H is a subgroup of G.

(c) Now suppose G is finite abelian, and that $|G| = mn$ where $\gcd(m, n) = 1$. Let H be as in (b) and $K = \{k \in G : o(k)|n\}$ (also a subgroup of G, by (b)).

(i) Prove that $H \cap K = \{e\}$.

(ii) Prove that $HK = G$. (Hint: For g in G, write $o(g) = rs$ where $r|m$ and $s|n$, and $1 = ar + bs$. Set $h = g^{bs}$ and $k = g^{ar}$.)

(Because (i) of (a) is clearly satisfied, we have $G \cong H \times K$. It follows by induction that a finite abelian group G is the direct product of its subgroups $G(p)$, where p varies over the primes that divide $|G|$ and $G(p)$ is the set of elements of G whose orders are powers of p.)

Solutions to Exam III

1. (a) Isomorphism: Kernel $\{0\}$, image $\mathbb{R}^+$, $\mathbb{R} \cong \mathbb{R}^+$.
   (b) Homomorphism: Kernel $\langle 4\rangle$, image $\langle 3\rangle$, $\mathbb{Z}_{12}/\langle 4\rangle \cong 3\mathbb{Z}_{12}$.
   (c) Epimorphism: Kernel $SL(2,\mathbb{R})$, image $\mathbb{R}-\{0\}$, $GL(2\mathbb{R})/SL(2,\mathbb{R}) \cong \mathbb{R}-\{0\}$.
   (d) Not a homomorphism: It is one-to-one function from G onto itself, the image of a under the monomorphism $\psi : G \to \mathcal{S}(G)$ used in Cayley's Theorem, but it does not respect the operation on G.

2. (a) The divisors of 18: 1, 2, 3, 6, 9 and 18.
   (b) $18 = 2 \cdot 3^2$, so the possible groups, up to isomorphism, are $\mathbb{Z}_2 \times \mathbb{Z}_9$ and $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.
   (c) (i) It has order a square of a prime. (ii) It has index 2. (iii) k is its own inverse, so its image under the natural homomorphism of G onto $\text{Inn}(G)$ must also have that property. Or, more simply, for all g in G, $k(kgk^{-1})k^{-1} = k^2gk^{-2} = g$ because $k^2 = e$.
   (d) We have $kb = ak$ by pre- and post-multiplying $ka = bk$ by k. So $(a^ib^jk)^2 = a^ib^jka^ib^jk = a^ib^jb^ia^jkk = a^{i+j}b^{i+j}$, which is the identity if $i+j$ is a multiple of 3 and an element of order 3 otherwise. Now $(a^ib^jk)^3 = a^{2i+j}b^{i+2j}k \neq e$, so a^ib^jk has order 2 if $i+j$ is divisible by 3 and order 6 otherwise.
   (e) No, they are not isomorphic: D_9 has no elements of order 6, but we have just seen that some elements of the G in (d) have order 6.

3. (a) For a subgroup K between H and G, we have $|H|[K:H] = |K|$, so $|H|$ divides $|K|$. But we also have $|K|[G:K] = |G| = |H|[G:H]$, so cancelling $|H|$ from both ends, we see that $[G:K]$ divides $[G:H]$. We are assuming that the last number is prime, so its only divisors are itself and 1, i.e., $[G:K] = [G:H]$ or 1, i.e., $K = H$ (because $H \subseteq K$) or $K = G$.
   (b) Let x be an element of G not in $\mathbb{Z}(G)$. Then the centralizer $Z(x)$ of x contains both x itself and $Z(G)$, so it properly contains $Z(G)$; but it is not all of G because $x \notin Z(G)$.

4. Because $Z(f)$ is at least $\langle f\rangle$ and is not all of D_5 (because g is not in it), we have $Z(f) = \langle f\rangle$, and f has $[D_5 : \langle f\rangle] = 2$ conjugates: itself and $gfg^{-1} = f^4gg = f^4$. Similarly, f^2, f^3 are conjugates. And g has $[D_5 : \langle g\rangle] = 5$ conjugates, the elements of order 2. Finally, $Z(D_5) = \{e\}$. So the class equation is $10 = 1 + 2(2) + 5$.

5. (a) Define $\varphi : H \times K \to G : (h,k) \mapsto hk$. Then φ is a homomorphism because G is abelian:
   $$\varphi((h_1,k_1)(h_2,k_2)) = \varphi((h_1h_2,k_1k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \varphi((h_1,k_1))\varphi((h_2,k_2)) \ .$$
   And $(h,k) \in \ker(\varphi)$ iff $hk = e$, i.e., $h = k^{-1}$, so h and k must both be in $H \cap K$, i.e., $h = k = e$; thus, φ is one-to-one. Finally, φ has image $HK = G$, so φ is an epimorphism and hence an isomorphism.
   (b) $o(e) = 1|m$, so $e \in H$, so $H \neq \emptyset$. If $x, y \in H$, then $o(x), o(y)|m$, so $x^m = e = y^m$, so, using the fact that G is abelian, $(xy)^m = x^my^m = ee = e$, so $o(xy)|m$, so $xy \in H$. If $x \in H$, then $o(x^{-1}) = o(x)|m$, so $x^{-1} \in H$. So H is a subgroup of G.
   (c) (i) If $g \in H \cap K$, then $o(g)$ divides both m, n, so it divides their gcd, 1; so $g = e$. (ii) Take any g in G; then $o(g)||G| = mn$, and because m, n are relatively prime, they have no prime factors in common. So we can factor $o(g)$, which divides mn, as rs where the

prime factors of r divide m and those of s divide n. Then $\gcd(r, s) = 1$ also, so we can write $1 = ar + bs$ where $a, b \in \mathbb{Z}$. Because r is a factor of m, $o(g) = rs$ is a factor of bsm, so $(g^{bs})^m = e$, i.e., $g^{bs} \in H$; and similarly $g^{ar} \in K$. Thus, $g = (g^{bs})(g^{ar}) \in HK$.