Math 521B Final Exam Solutions

May 14, 2008

1. (10 pts) A card-shuffling machine always rearranges cards in the same way relative to the order in which they were given to it. All of the hearts arranged in order from ace to king were put into the machine, and then the shuffled cards were put into the machine again to be shuffled. If the cards emerged in the order 10, 9, Q, 8, K, 3, 4, A, 5, J, 6, 2, 7, in what order were the cards after the first shuffle?

   Let α be the permutation which gives the order of the cards after they go through the machine once. For convenience, number the cards A through K by 1 through 13. Then we have that

   $$\alpha^2 = (1, 10, 11, 6, 3, 12, 2, 9, 5, 13, 7, 4, 8).$$

   Since this is a 13-cycle, $\alpha^{26} = (\alpha^2)^{13} = ()$. Hence $|\alpha|$ divides 26. It cannot be 1 or 2 because $\alpha^2 \neq ()$. It cannot be 26 either because there are only 13 cards to shuffle and S_{13} has no element of order 26. This is because the disjoint cycle representation of an element of order 26 must have at least one cycle whose length is divisible by 2, and at least one cycle (possibly the same) whose length is divisible by 13. But 13 objects are not enough to have a disjoint 2-cycle and 13-cycle, or a 26-cycle. Hence $|\alpha| = 13$.

   Then

   $$\alpha = \alpha^{14} = (\alpha^2)^7 = (1, 9, 10, 5, 11, 13, 6, 7, 3, 4, 12, 8, 2).$$

   After the first shuffle, the cards come out in the order 9, A, 4, Q, J, 7, 3, 2, 10, 5, K, 8, 6.

2. (10 pts) Let ϕ be an automorphism from G to $\overline{G}$. Prove that if K is a subgroup of G, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of $\overline{G}$.

   First notice that $e = \phi(e) \in \phi(K)$. Now let $a, b \in \phi(K)$. Then there exist $x, y \in K$ such that $a = \phi(x)$ and $b = \phi(y)$. Since K is a subgroup, $xy^{-1} \in K$, and hence

   $$ab^{-1} = \phi(x)\phi(y)^{-1} = \phi(xy^{-1}) \in \phi(K).$$

   Therefore $\phi(K)$ is a subgroup by the One-Step Subgroup Test.

   Note that the only property of ϕ we needed for this proof is that it is operation preserving. Therefore the statement and the proof remain valid for any homomorphism $\phi : G \to \overline{G}$.

3. (10 pts) Let G be a finite abelian group and let n be a positive integer that is relatively prime to $|G|$. Show that the mapping $a \mapsto a^n$ is an automorphism of G.

   Let $a, b \in G$. Then

   $$\phi(ab) = (ab)^n = (ab)(ab)\cdots(ab) = a^n b^n = \phi(a)\phi(b)$$

   where we used the commutativity of G to move all the a's to the left and all the b's to the right. Hence ϕ is operation preserving.

   Since $\gcd(|G|, n) = 1$, there exist $s, t \in \mathbb{Z}$ such that $s|G| + tn = 1$. Let $\sigma : G \to G$ be the map $a \mapsto a^t$. Recall that $a^{|G|} = e$ for all $a \in G$ because the order of a divides $|G|$. Hence

   $$a = a^{s|G|+tn} = (a^{|G|})^s a^{tn} = a^{tn}.$$

It follows that

$$\sigma\phi(a) = (a^n)^t = a^{nt} = a$$
$$\phi\sigma(a) = (a^t)^n = a^{nt} = a.$$

Hence ϕ and σ are inverses. So ϕ is a one-to-one correspondence.

Here is an alternate way to prove that ϕ is a one-to-one correspondence.
Suppose $\phi(a) = \phi(b)$. Then

$$e = \phi(a)\phi(b)^{-1} = \phi(ab^{-1}) = (ab^{-1})^n.$$

Therefore $|ab^{-1}|$ divides n. Since $ab^{-1} \in G$, its order must also divide $|G|$. But n and $|G|$ are relatively prime, so $|ab^{-1}|$ must be 1. Therefore $ab^{-1} = e$ and hence $a = b$. This shows ϕ is one-to-one. Since G is finite, this also implies ϕ is onto by Exercise 5.10.

4. (10 pts) Choose one of the following two problems to solve.
   (a) Determine $\mathrm{Aut}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$. (Here $\oplus$ stands for the external direct product.)

Let $\sigma \in \mathrm{Aut}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$. Then $\sigma(\overline{0}, \overline{0}) = (\overline{0}, \overline{0})$. So σ must permute the three nonidentity elements $(\overline{1}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{1})$ among themselves. The question is which of the 6 possible permutations are operation preserving. We will show that they all are.
Let $\sigma \in \mathrm{Sym}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$ such that $\sigma(\overline{0}, \overline{0}) = (\overline{0}, \overline{0})$. For σ to be an automorphism, it must satisfy

$$\sigma(x + y) = \sigma(x) + \sigma(y)$$

for any $x, y \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Certainly, if either x or y is the identity, the equality holds. So the interesting cases are when x and y are both nonidentity elements.
If $x = y$, then we have $\sigma(x + x) = \sigma(x) + \sigma(x)$, which will always hold as $x + x = (\overline{0}, \overline{0})$ for any element of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.
Now, let x and y be two different nonidentity elements of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Notice that $x + y$ is always the third nonidentity element regardless of how you choose x and y. Since $\sigma(x)$ and $\sigma(y)$ are also two different nonidentity elements of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\sigma(x) + \sigma(y)$ is the third one. Note that $\sigma(x + y) \neq \sigma(x), \sigma(y)$ because σ is one-to-one. Hence $\sigma(x + y) = \sigma(x) + \sigma(y)$.
We have just shown that σ is operation preserving. So $\mathrm{Aut}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$ has six elements corresponding to the six permutations on the set $\{(\overline{1}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{1})\}$. In fact, this makes it clear that $\mathrm{Aut}(\mathbb{Z}_2 \oplus \mathbb{Z}_2) \cong S_3$.

   (b) Let G be a finite group and let H be an odd-order subgroup of G of index 2. Show that the product of all the elements of G (taken in any order) cannot belong to H.

Since $[G : H] = 2$, H is normal in G (see for example exercise 7.(b) on this exam). So we can form the quotient group G/H. Let $g_1 g_2 \cdots g_n$ be a product of all elements in G. If this product belongs to H, then the coset $g_1 g_2 \cdots g_n H$ must be equal to H. But

$$g_1 g_2 \cdots g_n H = (g_1 H)(g_2 H) \cdots (g_n H).$$

Each $g_i H$ must be one of two things: if $g_i \in H$, then $g_i H = H$, otherwise $g_i H = G \setminus H$. But $g_i \in H$ for exactly half of the g_i because H is half of G. These $g_i H$ act as the identity in G/H. The remaining $g_i H$ are all equal to $G \setminus H$, which is an element of order 2 in $G \setminus H$. But there are an odd number of such $g_i H$, so when they are multiplied together, the result is again $G \setminus H$. Since $g_1 g_2 \cdots g_n H = G \setminus H$, $g_1 g_2 \cdots g_n \notin H$.

5. (10 pts) Consider the alternating group A_6. If $\sigma \in A_6$, determine all possibilities for $|\sigma|$. Give an example of an element of each possible order.

The solution is very similar to how we listed the orders of the elements of S_5 in class, only we need to be careful to list only even permutations.

We know that a k-cycle is even if and only if k is odd. So A_6 will have the identity, 3-cycles, and 5-cycles. These will have orders 1, 3, and 5 respectively.

We can also get even permutations by multiplying two disjoint 2-cycles, a 2-cycle and a disjoint 4-cycle (the product of two odd permutations is even), or two disjoint 3-cycles (the product of two even permutations is also even). We know that the order of a permutation is the lcm of its disjoint cycles. So these last three types have orders 2, 4, and 3 respectively. This exhausts all the possibilities in A_6. Here are the possible orders with examples

order	example
1	()
2	(1 2)(3 4)
3	(1 2 3) or (1 2 3)(4 5 6)
4	(1 2)(3 4 5 6)
5	(1 2 3 4 5)

6. (10 pts) Let G be a finite group. Prove that the order of any element of G divides the order of G. (This is Lagrange's Theorem for an element.)

Let $g \in G$. Let $H = \langle g \rangle$ be the cyclic subgroup generated by g. Then $|H| = |g|$. Note that the left cosets of H partition G and they are all the same size as H. Hence $|G|$ is divisible by $|H| = |g|$.

7. (20 pts)
   (a) Let G be a group (finite or infinite) and $H \subseteq G$ a subgroup. Define what it means for H to be normal in G.

   H is normal in G if $gH = Hg$ for all $g \in G$, that is each left coset is equal to the corresponding right coset.

   (b) Let G be a group (finite or infinite) and $H \subseteq G$ a subgroup of index 2. Prove that H must be normal.

   Since $[G : H] = 2$, H has only two cosets. One of these is H itself. Since the cosets form a partition of G, the other coset must be the complement, $G \setminus H$.
   Let $g \in G$. If $g \in H$, then $gH = H$ and $Hg = H$, so $gH = Hg$. If $g \notin H$, then $gH = G \setminus H$ and $Hg = G \setminus H$, so $gH = Hg$ in this case too.

   (c) Show that A_n is the only subgroup of S_n of index 2. (Hint: show that any subgroup of index 2 has to contain all of the even permutations.)

   Since A_n contains exactly half of the permutations in S_n, its index in S_n is 2.
   We will now show that A_n is the only such subgroup. Let $H \subseteq S_n$ be a subgroup of index 2. H must be normal by part (b). Hence we can form the quotient group S_n/H. Note that $|S_n/H| = [S_n : H] = 2$. So there are only two cosets of H, namely H and $S_n \setminus H$. Note that the order of $S_n \setminus H$ in S_n/H must be 2. We will first show that H can contain no transpositions. Notice that all transpositions are conjugates of each other.

For example, if $\sigma = (a\,b)$ and $\phi = (c\,d)$ then

$$\sigma = ((a\,c)(b\,d))\phi((a\,c)(b\,d))^{-1}.$$

Since H is normal, it is closed under conjugation. So it either contains all transpositions or none of them. If H contained all transpositions, then H would have to be all of S_n since every permutation is a product of transpositions. But $H \neq S_n$, so none of the transpositions are in H.
Now let σ be an even permutation. That is $\sigma = \sigma_1\sigma_2\cdots\sigma_k$ for some transpositions σ_i and k is even. Then

$$\sigma H = (\sigma_1 H)(\sigma_2 H)\cdots(\sigma_k H) = (S_n \setminus H)^k,$$

as each $\sigma_i H = S_n \setminus H$. But $|S_n \setminus H|$ divides k, hence $\sigma H = (S_n \setminus H)^k = H$, which implies $\sigma \in H$. We have just shown that every even permutation is in H. That is $A_n \subseteq H$. Since $|A_n| = |H|$, this proves $H = A_n$.

8. (15 pts) **Extra credit problem.** Let G be a group and $H \subseteq G$ a subgroup. For $a, b \in G$, define $a \sim b$ if $ab^{-1} \in H$.
   (a) Prove that $\sim$ is an equivalence relation.

   Reflexivity: For any $a \in G$, $aa^{-1} = e \in H$, hence $a \sim a$.

   Symmetry: Suppose $a \sim b$. Then $ab^{-1} \in H$. Since H is a subgroup, it is closed under inverses. Hence $ba^{-1} = (ab^{-1})^{-1} \in H$. So $b \sim a$.

   Transitivity: Suppose $a \sim b$ and $b \sim c$. Then $ab^{-1}, bc^{-1} \in H$. Since H is a subgroup, $ac^{-1} = ab^{-1}bc^{-1} \in H$. So $b \sim c$.

   (b) Prove that for all $a \in G$, the equivalence class of a is the right coset Ha.

   Notice that

$$\begin{aligned} b \in [a] &\iff b \sim a \iff ba^{-1} \in H \\ &\iff ba^{-1} = h \text{ for some } h \in H \iff b \in Ha. \end{aligned}$$

   Hence $[a] = Ha$.

   (c) Conclude that the right cosets form a partition of G.

   We know that the eqivalence classes of an equivalence relation form a partition. In part (b), we showed that the right cosets are the equivalence classes of an equivalence relation. Therefore they must partition G.

9. (15 pts) **Extra credit problem.** Let G be a group. For $g \in G$, let $\phi_g : G \to G$ be conjugation by g. That is $\phi_g(x) = gxg^{-1}$. Let $T : G \to \mathrm{Inn}(G)$ be the map given by $T(g) = \phi_g$.
   (a) Prove that T is a homomorphism.

   First notice that

$$\phi_{gh}(x) = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = g(hxh^{-1})g^{-1} = \phi_g\phi_h(x)$$

   for any $x \in G$. This shows $\phi_{gh} = \phi_g\phi_h$. But

$$T(gh) = \phi_{gh} = \phi_g\phi_h = T(g)T(h).$$

(b) Prove that $\ker(T) = Z(G)$.

$g \in \ker(T) \iff T(g) = 1_G \iff gxg^{-1} = x \ \forall x \in G \iff gx = xg \ \forall x \in G.$

(c) Conclude that $\mathrm{Inn}(G) \cong G/Z(G)$.

The First Isomorphism Theorem says that $\mathrm{im}(T) \cong G/\ker(T)$. The image of T contains all inner automorphisms by definition. We showed in part (b) that $\ker(T) = Z(G)$. Hence $\mathrm{Inn}(G) \cong G/Z(G)$.