Math 521B Exam 2 Solutions

Mar 22, 2010

1. (5 pts) Let G_1 and G_2 be groups, and let G be the direct product $G_1 \times G_2$. Let $H = \{(x_1, e) \mid x_1 \in G_1\}$ and $K = \{(e, x_2) \mid x_2 \in G_2\}$.
   Show that H and K are subgroups of G.

   Since $e \in G_1$, $(e, e) \in H$. Now

   $$(x_1, e), (y_1, e) \in H \implies x_1, y_1 \in G_1 \implies x_1 y_1 \in G \implies (x_1, e)(y_1, e) = (x_1 y_1, e) \in H,$$

   and

   $$(x_1, e) \in H \implies x_1 \in G_1 \implies x_1^{-1} \in G \implies (x_1, e)^{-1} = (x_1^{-1}, e) \in H.$$

   Therefore H contains the identity and is closed under multiplication and inverses, hence H is a subgroup of G.

   An analogous argument shows K is a subgroup too.

2. (10 pts) Let G be a finite group, and let H and K be subgroups of G. Prove that

   $$|HK| = \frac{|H||K|}{|H \cap K|}.$$

   Since H and K are finite, so is $H \cap K$ and we can let $n = |H \cap K|$. Define the map $\phi : H \times K \to HK$ by $\phi(h, k) = hk$. Since

   $$HK = \{hk | h \in H, k \in K\}$$

   ϕ is onto. Now let $\sim$ be the relation on $H \times K$ defined by $(h, k) \sim (h', k')$ if and only if $\phi(h, k) = \phi(h', k')$. By Theorem 2.2.7, ϕ induces a one-to-one correspondence between the set of equivalence classes $(H \times K)/\sim$ and HK. We will now show that each equivalence class has exactly $n = |H \cap K|$ elements.

   Let $(h, k) \in H \times K$. We will prove that the equivalence class $[(h, k)]$ has n elements by constructing a one-to-one correspondence $\phi : H \cap K \to [(h, k)]$. For $x \in H \cap K$, define $\phi(x) = (hx, x^{-1}k)$. First, we verify that $\phi(x) \in [(h, k)]$. Since $x \in H \cap K$, $hx \in H$ and $x^{-1}k \in K$. So $\phi(x) \in H \times K$. Notice

   $$(hx)(x^{-1}k) = h(xx^{-1})k = hk \implies \phi(x) \sim (h, k) \implies \phi(x) \in [(h, k)].$$

   Now define $\sigma : [(h, k)] \to H \cap K$ by $\sigma(h', k') = h^{-1}h'$. Notice

   $$\sigma\phi(x) = \sigma(hx, x^{-1}k) = h^{-1}hx = x$$

   and

   $$\phi\sigma(h', k') = \phi(h^{-1}h') = (h(h^{-1}h'), (h^{-1}h')^{-1}k) = (h', (h')^{-1}hk).$$

   But

   $$(h', k') \in [(h, k)] \implies (h, k) \sim (h', k') \implies hk = h'k' \implies (h')^{-1}hk = h'^{-1}h'k' = k'.$$

   So $\phi\sigma(h', k') = (h', k')$. This shows ϕ and σ are inverses, so ϕ is a one-to-one correspondence and $|[(h, k)]| = |H \cap K| = n$.

   Now, every equivalence class in $H \times K$ has n elements, so there are

   $$\frac{|H \times K|}{n} = \frac{|H||K|}{|H \cap K|}$$

   equivalence classes and consequently the same number of elements in HK.

Note: This proof is almost the same as the one you all found on the internet. It uses fancier language and does not rely on listing the elements of H and K, so it works in some sense even if H or K are infinite. I say in some sense because if H or K is infinite, then HK is also infinite. But as long as $H \cap K$ is finite, at least we know that there is an n-to-1 correspondence $H \times K \to HK$.

3. (10 pts) Let $G = \mathbb{R} \setminus \{-1\}$. Define $*$ on G by $a * b = a + b + ab$. Show that G is isomorphic to the multiplicative group $\mathbb{R}^*$. (Hints: It may help to notice that $a+b+ab = (a+1)(b+1)-1$. Remember that an isomorphism maps identity to identity. Use this fact to help find the necessary mapping.)

   Notice that 0 is the identity in G. Therefore any isomorphisms $\phi : G \to \mathbb{R}^*$ has to map 0 to 1. This suggests the idea that perhaps $\phi(x) = x + 1$ is an isomorphism. First of all, it is indeed a map $G \to \mathbb{R}^*$. Second, it has an obvious inverse $\sigma : \mathbb{R}^* \to G$ defined by $\sigma(x) = x - 1$. This shows ϕ is a one-to-one correspondence. Finally,

   $$\phi(a * b) = (a + b + ab) + 1 = (a + 1)(b + 1) = \phi(a)\phi(b)$$

   for all $a, b \in G$. So ϕ is indeed an isomorphism $G \to \mathbb{R}^*$.

4. (10 pts) Let F be any field. Prove that the set of invertible $n \times n$ matrices $\mathrm{GL}_n(F)$ is a group under matrix multiplication.

   First, recall that matrix multiplication is associative. The $n \times n$ identity matrix I is its own inverse, hence $I \in \mathrm{GL}_n(F)$. If $A \in \mathrm{GL}_n(F)$ then A has an inverse A^{-1}. Obviously, A^{-1} is also an invertible $n \times n$ matrix, hence $A^{-1} \in \mathrm{GL}_n(F)$.

   The product of two $n \times n$ matrices is also an $n \times n$ matrix. If $A, B \in \mathrm{GL}_n(F)$, then A^{-1} and B^{-1} exist and are $n \times n$ matrices, hence $B^{-1}A^{-1}$ is also an $n \times n$ matrix. Since $(AB)(B^{-1}A^{-1}) = I$ and $(B^{-1}A^{-1})(AB) = I$, AB is invertible. Hence $AB \in \mathrm{GL}_n(F)$.

   Therefore $\mathrm{GL}_n(F)$ is a group.

5. (a) (3 pts) Define group isomorphism.

   See Definition 3.4.1.

   (b) (6 pts) Prove that the inverse of an isomorphism $\phi : G \to H$ is also an isomorphism.

   See Proposition 3.4.2(a).

   (c) (6 pts) Find two groups of order 6 that are not isomorphic to each other. Be sure to prove that your two groups are not isomorphic.

   Z_6 and S_3 are groups of order 6. Since Z_6 is abelian and an isomorphism maps an abelian group to an abelian group (by Prop 3.4.3(b)), Z_6 cannot be isomorphic to S_3.

6. (10 pts) **Extra credit problem.** An *automorphism* is an isomorphism of a group to itself, i.e. an isomorphism $\phi : G \to G$. One approach to studying an abstract group is to study its automorphisms, which themselves turn out to form a group under composition. (This should be easy to see in light of the results we have proved in class.) Find all automorphisms of S_3. Be sure to prove that you have found all of them. How many different ones are there? When you count them, make sure they are different from each other. (Hint: You proved on the HW and on your last quiz that $\phi_a(x) = axa^{-1}$ is an isomorphism.)

First, suppose that ϕ is an automorphism of S_3. Let $x = \phi((1,2))$ and $y = \phi((1\,3))$. Notice x and y determine all other values of ϕ because

$$\begin{aligned}\phi(()) &= () \\ \phi((1\,2\,3)) &= \phi((1\,3)(1\,2)) = \phi((1\,3))\phi((1\,2)) = yx \\ \phi((1\,3\,2)) &= \phi((1\,2)(1\,3)) = \phi((1\,2))\phi((1\,3)) = xy \\ \phi((2\,3)) &= \phi((1\,2)(1\,3)(1\,2)) = \phi((1\,2))\phi((1\,3))\phi((1\,2)) = xyx\end{aligned}$$

Since $(1\,2)$ and $(1\,3)$ are both of order 2, x and y must also be of order 2. The only elements of order 2 in S_3 are the three transpositions. Therefore there are 3 choices for x and 2 for y (remember $x \neq y$ because ϕ is one-to-one). That leaves only 6 possibilities for ϕ.

We will now show that those 6 maps are indeed all isomorphisms. We could do this by explicitly writing down these 6 maps and verifying that each is an isomorphism. But that takes a lot of computation: 72 multiplications for each map. So we will take a more clever approach. By Exercise 3.4.15, the map $\phi_a(x) = axa^{-1}$ is an automorphism of S_3 for every $a \in S_3$. This immediately gives six candidates of automorphisms, one for each element of S_3. But are they really six different maps? We can check that they are by looking at where they map $(1\,2)$ and $(1\,3)$:

ϕ	$\phi((1\,2))$	$\phi((1\,3))$
$\phi_{()}$	$(1\,2)$	$(1\,3)$
$\phi_{(1\,2)}$	$(1\,2)$	$(2\,3)$
$\phi_{(1\,3)}$	$(2\,3)$	$(1\,3)$
$\phi_{(2\,3)}$	$(1\,3)$	$(1\,2)$
$\phi_{(1\,2\,3)}$	$(2\,3)$	$(1\,2)$
$\phi_{(1\,3\,2)}$	$(1\,3)$	$(2\,3)$

So indeed, these six isomorphisms all do different things to $(1\,2)$ and $(1,\ 3)$, so they are the six possible different automorphisms of S_3.

Note: Automorphisms of the form $\phi_a(x) = axa^{-1}$ are called the inner automorphisms of a group. Not all automorphisms need to be inner automorphisms. Those that are not are called outer automorphisms. E.g. $\mathbb{Z}$ is an abelian group, so its only inner automorphism is the identity map (this should be obvious, think about it). But there is also a nontrivial outer automorphism $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(x) = -x$, which should be familiar from Exercise 3.4.16.

The automorphisms of any group form a group themselves. The inner automorphisms are a subgroup of the group of automorphisms. In the case of S_3, the group of automorphisms is itself isomorphic to S_3. (Try proving this.)