Math 521B Exam 2 Solutions

Mar 24, 2008

1. (10 pts) Prove or disprove that $U(20)$ and $U(24)$ are isomorphic.

   They are not isomorphic. First, look at the elements of $U(24)$:
   $$U(24) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}\}.$$
   Notice that
   $$|\overline{1}| = 1$$
   $$|\overline{5}| = |\overline{7}| = |\overline{11}| = |\overline{13}| = |\overline{17}| = |\overline{19}| = |\overline{23}| = 2$$
   On the other hand, $\overline{3}$ is an element of $U(20)$ whose order is 4. If there were an isomorphism $\sigma : U(20) \to U(24)$, it would have to send $\overline{3}$ to an element of order 4 in $U(24)$. But there is no such element, so no such isomorphism can exist.

2. (10 pts) Find $\mathrm{Aut}(\mathbb{Z})$.

   Let $\sigma \in \mathrm{Aut}(\mathbb{Z})$. Note that $\mathbb{Z}$ is a cyclic group. Any isomorphism from a cyclic group to a cyclic group has to map generators to generators (see Theorem 6.2.4). We know that $\mathbb{Z}$ is cyclic and has two generators, 1 and -1. So $\sigma(1) = \pm 1$. If $n \in \mathbb{Z}$, then $n = n \cdot 1$ and
   $$\sigma(n) = \sigma(n \cdot 1) = n\sigma(1)$$
   (by Theorem 6.2.2). If $\sigma(1) = 1$, this gives $\sigma(n) = n$, which is $\mathrm{Id}_{\mathbb{Z}}$. Obviously, this is an automorphism. If $\sigma(1) = -1$, then $\sigma(n) = -n$. In fact, $\sigma(\sigma(n)) = -(-n) = n$ for all $n \in \mathbb{Z}$, so σ is its own inverse, and therefore a one-to-one correspondence. Finally,
   $$\sigma(n + k) = -(n + k) = -n - k = \sigma(n) + \sigma(k)$$
   which shows that σ is operation preserving.

   Hence $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}_{\mathbb{Z}}, \sigma\}$, where σ is the map $n \mapsto -n$.

3. (10 pts) Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ is an automorphism if and only if G is abelian.

   First, notice that $\alpha(\alpha(g)) = (g^{-1})^{-1} = g$. Hence $\alpha \circ \alpha = \mathrm{Id}_G$. This immediately gives that α is a one-to-one correspondence. So the only property in question is if α is operation preserving. In fact,
   $$\alpha(gh) = (gh)^{-1} = h^{-1}g^{-1}$$
   $$\alpha(g)\alpha(h) = g^{-1}h^{-1}.$$
   If G is abelian, then
   $$h^{-1}g^{-1} = g^{-1}h^{-1} \implies \alpha(gh) = \alpha(g)\alpha(h)$$
   Since this is true for all $g, h \in G$, α is an automorphism. Conversely, if α is an automorphism, then for all $g, h \in G$
   $$\alpha(gh) = \alpha(g)\alpha(h) \implies$$
   $$h^{-1}g^{-1} = g^{-1}h^{-1} \implies$$
   $$(h^{-1}g^{-1})^{-1} = (g^{-1}h^{-1})^{-1} \implies$$
   $$gh = hg.$$

Hence G is abelian.

By the way, we proved in problem 2 that this map is an automorphism in the special case of the abelian group $\mathbb{Z}$.

4. (20 pts)
   (a) State Cayley's Theorem.

   Every group is isomorphic to a group of permutations.

   (b) We proved Cayley's Theorem by constructing the map $\phi(g) = T_g$ from a group G to $\mathrm{Sym}(G)$, where $T_g : G \to G$ is defined by $T_g(x) = gx$.
   Prove that T_g is a permutation.

   Notice that T_g has an obvious inverse in $T_{g^{-1}}$. Indeed
$$T_{g^{-1}}T_g(x) = T_{g^{-1}}(gx) = g^{-1}gx = x$$
$$T_gT_{g^{-1}}(x) = T_g(g^{-1}x) = gg^{-1}x = x$$
   for all $x \in G$. Hence $T_{g^{-1}}T_g = T_gT_{g^{-1}} = \mathrm{Id}_G$. Therefore T_g is a one-to-one correspondence.

   (c) Prove that the map ϕ defined in part (b) is operation preserving (i.e. it is a homomorphism).

   Let $g, h \in G$. Then
$$T_gT_h(x) = g(hx) = (gh)x = T_{gh}(x)$$
   for all $x \in G$. So
$$\phi(gh) = T_{gh} = T_gT_h = \phi(g)\phi(h).$$

5. (10 pts) Let $G = S_3$ and $H = \{(), (2\,3)\}$. Find the left and the right cosets of H in G.

   The three left cosets are
$$H = \{(), (2\,3)\} = (2\,3)H$$
$$(1\,2)H = \{(1\,2), (1\,2\,3)\} = (1\,2\,3)H$$
$$(1\,3)H = \{(1\,3), (1\,3\,2)\} = (1\,3\,2)H.$$
   The three right cosets are
$$H = \{(), (2\,3)\} = H(2\,3)$$
$$H(1\,2) = \{(1\,2), (1\,3\,2)\} = H(1\,3\,2)$$
$$H(1\,3) = \{(1\,3), (1\,2\,3)\} = H(1\,2\,3).$$

6. (15 pts) **Extra credit problem.** Let G be a group and $H \subseteq G$ a subgroup. Let $\alpha : G \to G$ be the map $\alpha(g) = g^{-1}$. (You have already met this map today in problem 3.)
   (a) Prove that α maps left cosets of H to right cosets of H and vice versa. That is for all $a \in G$, $\alpha(xH) = Hy$ for some $y \in G$. And for all $x \in G$, $\alpha(Hx) = yH$ for some $y \in G$.

   Notice that $\alpha(xh) = (xh)^{-1} = h^{-1}x^{-1}$. Since $h^{-1} \in H$, $\alpha(xh) \in Hx^{-1}$. Also, $\alpha(hx^{-1}) = (hx^{-1})^{-1} = xh^{-1}$. Since $h^{-1} \in H$, $\alpha(hx^{-1}) \in xH$. We have just shown $\alpha(xH) = Hx^{-1}$.
   A symmetric argument shows that $\alpha(Hx) = x^{-1}H$.

(b) Let L be the set of left cosets of H in G and R be the set of right cosets of H in G. That is

$$L = \{gH | g \in G\}$$
$$R = \{Hg | g \in G\}.$$

Prove that the map $\sigma : L \to R$ defined by $\sigma(xH) = \alpha(xH)$ is a one-to-one correspondence.

Notice that what we proved in part (a) is that σ is indeed a map $L \to R$. Similarly, we can define $\phi : R \to L$ by letting $\phi(Hx) = \alpha(Hx)$. We will now show that σ and ϕ are inverses. For any $x \in G$,

$$\sigma\phi(Hx) = \alpha(\alpha(Hx)) = \alpha(x^{-1}H) = Hx$$
$$\phi\sigma(xH) = \alpha(\alpha(xH)) = \alpha(Hx^{-1}) = xH.$$

This shows $\sigma\phi = \mathrm{Id}_R$ and $\phi\sigma = \mathrm{Id}_L$. Hence σ is a one-to-one correspondence.

(c) What is the inverse of the map σ defined in part (b)?

It is $\phi : R \to L$ defined by $\phi(Hx) = \alpha(Hx)$. See part (b) for the proof.