Math 322 Homework 7

Xander Naumenko

23/10/23

Question 10. Let $g \in G$. Define $A^{-1}g = \{a^{-1}g : a \in A\}$. Since $|A^{-1}g| = A$, we have $\left|A^{-1}g\right| + B > |G| \implies \exists a \in A$ s.t. $a^{-1}g = b \implies g = ab$. Since this is true of all $g \in G$, we have that $G = AB$.

Question 11. As the hint suggests, using exercise 13 on page 36 (which we proved in a previous homework), there exists $a \in G$ such that $a^2 = 1$. Consider G_L, the group of left translations, since $G_L < S_{2k}$ is isomorphic to G it suffices to show that there is a subgroup of index 2 in G_L. Since a_L has order 2, it is the disjoint union of k transpositions. Let H be the group of all even elements of G_L (it is a group since 1 is even and the product of two even cycles is even) and let $g_L \in G_L$. If sg $g_L = 1$ then $g_L \in H$. Otherwise if sg $g_L = -1$ then $g_L a_L^{-1} \in H \implies g_L = Ha_L$. Thus $G_L = H \cup Ha_L \implies [G : H] = 2$ as required.

Question 2. Identity:

$$(0,0,0)(k,l,m) = (k+0+0, l+0, m+0) = (k,l,m) = (k,l,m)(0,0,0).$$

Associativity:

$$(k_1,l_1,m_1)\left((k_2,l_2,m_2)(k_3,l_3,m_3)\right) = (k_1+k_2+l_2m_3+l_1(m_2+m_3), l_1+l_2+l_3, m_1+m_2+m_3)$$

$$\left((k_1,l_1,m_1)(k_2,l_2,m_2)\right)(k_3,l_3,m_3).$$

Invertibility:

$$(k,l,m)(-k+lm,-l,-m) = (0,0,0) = 1.$$

For any $g = (k,l,m) \in G$, we have that for all $c = (t,0,0) \in C$, $gcg^{-1} = (k,l,m)(t,0,0)(-k+lm,-l,-m) = (k+t(-k+lm)-lm,0,0) \in C$, so C is normal. I claim that $\phi : G/C \to Z^{(2)}$ defined as $\phi(k,l,m) = (l,m)$ is bijective. It is well defined, since $C(k,l,m) = C(k',l,m)$. It is injective and onto, since unique choices of l,m uniquely determine the input and output of the function. Thus $G/C \cong \mathbb{Z}^{(2)}$.

Question 4. Let $G = \langle a \rangle$ with infinite order, and let ϕ be an automorphism on G. a and a^{-1} are generators of G, the only possibilities are that $\phi(a) = a$ or $\phi(a) = a^{-1}$ and hence $\phi(x) = x$ or $\phi(x) = x^{-1}$

Let $G = \langle a \rangle$ with $|G| = 6$. For an automorphism ϕ on G, by the definition of a homomorphism we have that $\phi(a^k) = \phi(a)^k$. Since $\phi(G) = G$, it must be that $|\phi(a)| = 6$. Specifically, by theorem 1.3 this implies that $\phi(a) = a^m$ for some m such that $(m,6) = 1$, i.e. $m = 1$ or 5. Clearly ϕ is uniquely determined by the choice of $\phi(a)$, and for any such m we have that ϕ is an injective map from G to G, so ϕ is an automorphism.

Finally for a general finite cyclic group G, following the exact same logic as part ii shows that ϕ is an automorphism if and only if $\phi(a) = a^m$ for some m with $(m,|G|) = 1$.

Question 5. Note that the elements $a = (123)$ and $b = (12)$ generate S_3. Powers of each individually generate 4 elements of S_3, while $ab = (13)$ and $ba = (23)$. Thus any automorphism ϕ is completely determined by $\phi(a)$ and $\phi(b)$ by theorem 1.7. Since there are 2 elements of order $3 = |a|$ and 3 elements of order $2 = |b|$, there are at most 6 possible automorphisms. Directly trying them all, we see that the possibilities are listed in table 1. Since there are at most 6 automorphisms and we've found 6 that work, we're done.

Table 1: Possibilities for choices of automorphisms of S_3 in question 5.

$\phi(a)$	$\phi(b)$
a	b
a	ab
a	a^2b
a^2	b
a^2	ab
a^2	a^2b

Question 8. For some element $a \in G$ consider the map $\phi : x \to axa^{-1}$. ϕ is an automorphism, since $\phi(xy) = axya^{-1} = axa^{-1}aya^{-1} = \phi(x)\phi(y)$. Since Aut $G = 1$, we have that $axa^{-1} = x \implies ax = xa$ for all $x \in G$. Thus G is abelian. Also since G is abelian the map $\psi : x \to x^{-1}$ is an automorphism, since $\psi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \psi(x)\psi(y)$. Again since Aut $G = 1$, we then have $x = x^{-1} \implies x^2 = 1$ for all $x \in G$.

To prove the last part, as the hint suggests we will show that there exists unique representation of each element in terms of a fixed set of elements. This property will be shown by induction on subgroups $H_n \leq G$ with $|H_n| = n$. Clearly for $n = 1$ the result holds choosing $H = \{1\}$ and $a_1 = 1$. Assume that H_n has a set of elements $a_1, a_2, \ldots, a_n$ with each element $h \in H$ uniquely represented as $a_1^{k_1} \cdots a_n^{k_n}, k_i = 0, 1$. Clearly these generate H so $H = \langle a_1, \ldots, a_n \rangle$. Choose $a_{n+1} \in G - H$. Since $|a_{n+1}| = 2$, $\langle a_{n+1} \rangle \cap H = 1$. Also because G is abelian and $|a_{n+1}| = 2$ any element $h \in \langle H, a_{n+1} \rangle$ can be written as $ha_{n+1}^{k_{n+1}}$. This representation is unique, since if $ha_{n+1}^{k_{n+1}} = h'a_{n+1}^{k'_{n+1}} \implies h(h')^{-1} = a_{n+1}^{k_{n+1} - k'_{n+1}} \implies h = h', k_{n+1} = k'_{n+1}$ (since $H \cap \langle a_{n+1} \rangle = 1$. Thus $\langle H, a_{n+1} \rangle$ is a subgroup with the required property, and so the property holds for all n including $n = |G|$.

Therefore the map $\phi : a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} \to a_2^{k_1} a_1^{k_2} \cdots a_n^{k_n}$ is an automorphism since it just involves relabeling interchangeable generating elements. Since by assumption Aut $G = 1$, the only way to avoid such a map is if $G = \langle a \rangle$, and since $|a| = 2$, G can only either have 1 or 2 elements.