MATH 257: Homework #6

Jesse Farmer

10 November 2004

1. *Let G be a finite abelian group with order $n = mk$ where $(m, k) = 1$. Define $G(r) = \{g \in G \mid g^r = 1\}$. Prove that $G = G(m)G(k)$.*

   Since $(m, k) = 1$ there exist integers a, b such that $am + bk = 1$. Then

   $$g = g^{am+bk} = g^{am}g^{bk}$$

   but $(g^{am})^k = g^{amk} = g^{an} = (g^n)^k = 1$, so that $g^{am} \in G(k)$. Similarly $g^{bk} \in G(m)$, and therefore $G \subseteq G(m)G(k)$. The opposite inclusion is obvious and our statement is proven.

2. *Let H and K be groups, $\varphi : K \to Aut(H)$ be a group homomorphism. Prove that $C_{\tilde{K}})(H) = \ker\varphi$, where H and K are isomorphic copies of H and K in $H \rtimes_\varphi K$.*

   From theorem 10 part 5, $khk^{-1} = \varphi(k)(h)$. Denote the identity map by I, then

   $$\begin{aligned} \ker\varphi &= \{k \in K \mid \varphi(k) = I\} \\ &= \{k \in K \mid \varphi(k)(h) = h,\, \forall h \in H\} \\ &= \{k \in K \mid khk^{-1} = h,\, \forall h \in H\} \\ &= C_K(H) \end{aligned}$$

   Note that in truth $\ker\varphi$ contains elements of K while $C_K(H)$ contains elements of the subgroup isomorphic to K, so that in actuality $\ker\varphi \cong C_K(H)$.

3. *Let $H = (\mathbb{Z}_n, +)$ and $A = (\mathbb{Z}_n^\times, \cdot)$. Define $\tau(a, b) : \mathbb{Z}_n \to Z_n$ by $\overline{x} \mapsto \overline{ax + b}$ with $(a, n) = 1$ and $b \in \mathbb{Z}$ and $G = \{\tau(a, b) \mid a, b \in \mathbb{Z},\, (a, n) = 1\}$.*

   (a) *Define $\phi_{\overline{a}} : H \to H$ by $\overline{h} \mapsto \overline{ha}$. Show that $\phi_{\overline{a}} \in Aut(H)$.*

   Denote $\phi_{\overline{a}}$ by φ for brevity's sake. φ is surjective since there exists an $\overline{h'} = \overline{ha^{-1}}$ such that $\varphi\left(\overline{h'}\right) = \overline{h}$ for all $\overline{h} \in H$. It is trivially injective since every a has an inverse by construction.

   That it is a homomorphism is also equally obvious:

   $$\varphi\left(\overline{h_1} + \overline{h_2}\right) = \varphi\left(\overline{h_1 + h_2}\right) = \overline{(h_1 + h_2)a} = \overline{h_1 a} + \overline{h_2 a} = \varphi\left(\overline{h_1}\right) + \varphi\left(\overline{h_2}\right)$$

(b) *Show that $\phi : A \to Aut(H)$ is an injective group homomorphism.*

ϕ is a homomorphism since

$$\phi\left(\overline{a_1 a_2}\right)\left(\overline{h}\right) = \overline{h a_1 a_2} = \phi\left(\overline{a_2}\right)\left(\overline{h a_1}\right) = \left(\phi\left(\overline{a_1}\right) \circ \phi\left(\overline{a_2}\right)\right)\left(\overline{h}\right)$$

If $\phi\left(\overline{a_1}\right) = \phi\left(\overline{a_2}\right)$ then $\overline{ha_1} = \overline{ha_2}$ for every $h \in H$. In particular this is true for $h = 1$, so $\overline{a_1} = \overline{a_2}$. Therefore ϕ is an injective group homomorphism.

(c) *Show that for $\overline{a} \in A$ and $\overline{b} \in H$, $\tau(1,b)^{\tau(a,0)} = \tau(1,ab)$.*

We will identify a with $\overline{a}$ and b with $\overline{b}$. Let $x \in \mathbb{Z}_n$ then

$$\begin{aligned}
\left(\tau(a,0)\tau(1,b)\tau(a,0)^{-1}\right)(x) &= \left(\tau(a,0)\tau(1,b)\right)\left(a^{-1}x\right) \\
&= \left(\tau(a,0)\right)\left(a^{-1}x + b\right) \\
&= x + ab \\
&= \tau(1,ab)(x)
\end{aligned}$$

(d) *Show that $G \cong H \rtimes_\phi A$.*

Once again we identify a with $\overline{a} \in A$ and b with $\overline{b} \in H$. Define the map $\psi : H \rtimes_\phi A \to G$ by $(a,b) \mapsto \tau(a,b)$. Note that in general $\tau(a_1,b_1) \circ \tau(a_2,b_2) = \tau(a_1a_2, b_1a_2 + b_2)$. Recall that the operation on H is addition and the operation on A is multiplication modulo n. Then

$$\begin{aligned}
\psi(a_1,b_1)(a_2,b_2) &= \psi(a_1a_2, \phi(a_2)(b_1) + b_2) \\
&= \tau(a_1a_2, \phi(a_2)(b_1) + b_2) \\
&= \tau(a_1a_2, a_2b_1 + b_2) \\
&= \tau(a_1,b_1) \circ \tau(a_2,b_2)
\end{aligned}$$

and therefore ψ is a homomorphism. ψ is trivially surjective from our construction. It is injective since if $\tau(a_1,b_2)(x) = \tau(a_2,b_2)(x)$ for all $x \in \mathbb{Z}_n$ then $a_1x + b_1 = a_2x + b_2$ for all $x \in \mathbb{Z}_n$, including $x = 0$ and $x = 1$. Hence $a_1 = a_2$ and $b_1 = b_2$ in $\mathbb{Z}_n$. Therefore $G \cong H \rtimes_\phi A$.