Notes to accompany the discussion of $(\mathbb{Z}/m)^c \rtimes S_c$

September 15, 2003

In class I defined a map

\[ \Phi : S_c \longrightarrow \text{Aut}_{\text{group}}((\mathbb{Z}/m)^c) \]

\[ \sigma \longrightarrow \phi_{\sigma}, \]

where

\[ \phi_{\sigma}(z_1, \ldots, z_c) = (z_{\sigma(1)}, \ldots, z_{\sigma(n)}). \]

As an in-class exercise, I asked you to verify that each $\phi_{\sigma}$ was a group automorphism. But much to my embarrassment, $\Phi$ is not a homomorphism! Here is why.

Take $\sigma$ and $\tau$ in $S_c$. If $\Phi$ is a homomorphism, then

\[ \Phi(\sigma \tau) = \Phi(\sigma) \circ \Phi(\tau). \]

By definition, this means that for all $(z_1, \ldots, z_c) \in (\mathbb{Z}/m)^c$,

\[ \phi_{\sigma \tau}(z_1, \ldots, z_c) = (\phi_{\sigma} \circ \phi_{\tau})(z_1, \ldots, z_c). \]  \hfill (1)

Let's work out the left-hand side of (1),

\[ \phi_{\sigma \tau}(z_1, \ldots, z_c) = (z_{\sigma \tau(1)}, \ldots, z_{\sigma \tau(c)}). \]  \hfill (2)

Now turn to the right-hand side,

\[ (\phi_{\sigma} \circ \phi_{\tau})(z_1, \ldots, z_c) = \phi_{\sigma}(\phi_{\tau}(z_1, \ldots, z_c)) \]

\[ = \phi_{\sigma}(z_{\tau(1)}, \ldots, z_{\tau(c)}). \]

Now set $(y_1, \ldots, y_c) = (z_{\tau(1)}, \ldots, z_{\tau(c)})$. So

\[ (\phi_{\sigma} \circ \phi_{\tau})(z_1, \ldots, z_c) = \phi_{\sigma}(y_1, \ldots, y_c) \]

\[ = (y_{\sigma(1)}, \ldots, y_{\sigma(c)}). \]

Since $y_j = z_{\tau(j)}$, by definition, then $y_{\sigma(i)} = z_{\tau(\sigma(i))}$. Thus previous equation reads

\[ (\phi_{\sigma} \circ \phi_{\tau})(z_1, \ldots, z_c) = (z_{\tau \sigma(1)}, \ldots, z_{\tau \sigma(c)}). \]  \hfill (3)
Comparing (2) and (3), together with (1), shows that $\Phi$ is not a homomorphism. Thus the semidirect product I was manipulating in class, $(\mathbb{Z}/m)^c \rtimes S_c$ isn’t well-defined! (This accounts for a lot of my confusion on Friday.) Here is how to fix things.

Instead define

$$
\Phi'(\sigma) : S_c \to \text{Aut}_{\text{group}}((\mathbb{Z}/m)^c)
$$

where

$$
\phi'_\sigma(z_1, \ldots, z_c) = (z_{\sigma^{-1}(1)}, \ldots, z_{\sigma^{-1}(m)}).
$$

The in-class exercise again shows that each $\phi'_\sigma$ is a group automorphism. And this time $\Phi'$ is a homomorphism! Here’s why; we need to check

$$
\Phi'((\sigma \tau)) = \Phi'((\sigma)) \circ \Phi'((\tau)).
$$

By definition, this means that for all $(z_1, \ldots, z_c) \in (\mathbb{Z}/m)^c$,

$$
\phi'_{\sigma \tau}(z_1, \ldots, z_c) = (\phi'_{\sigma} \circ \phi'_{\tau})(z_1, \ldots, z_c).
$$

The left-hand side is

$$
\phi_{\sigma \tau}(z_1, \ldots, z_c) = (z_{(\sigma \tau)^{-1}(1)}, \ldots, z_{(\sigma \tau)^{-1}(c)}) = (z_{\tau^{-1}(1) \sigma^{-1}(1)}, \ldots, z_{\tau^{-1}(c) \sigma^{-1}(c)}).
$$

Now turn to the right-hand side; we can trace through the same steps as above to conclude that

$$
(\phi'_{\sigma} \circ \phi'_{\tau})(z_1, \ldots, z_c) = (z_{\tau^{-1} \sigma^{-1}(1)}, \ldots, z_{\tau^{-1} \sigma^{-1}(c)}).
$$

So, indeed, $\Phi'$ is a homomorphism. This also explains the recent update to Problem #4 on the problem set.

Thus (using $\Phi'$) we can talk about the semidirect product $(\mathbb{Z}/m)^c \rtimes S_c$. Because of the mistake above, I feel obliged to give a correct account of my “hand waving” on Friday. When possible, I stuck to the notation on Friday, but sometimes I needed new (or different notation.) My apologies.

**Theorem 7** Fix a conjugacy class $C$ in $G := S_{cm}$ corresponding to the cycle structure that consists of $c$ disjoint cycles of size $m$. Then $G$ acts transitively on $C$ by the conjugation action, and for $x \in C$ there is an isomorphism

$$(\mathbb{Z}/m)^c \rtimes S_c \simeq \text{Stab}_G(x).$$

The rest of these notes is devoted to a proof. The statement that the action is transitive is clear: after all, a conjugacy class, by definition, consists precisely of all conjugates of any element in the class. To treat the remaining statement, it is helpful to fix $x$. In cycle notation, we define

$$
x = (1 \ 2 \ \cdots \ m)(m+1 \ m+2 \ \cdots \ 2m) \cdots (cm-c+1 \ cm-c+1 \ \cdots \ mc).
$$

Now set $\sigma_1$ be the first $m$ cycle

$$
\sigma_1 = (1 \ 2 \ \cdots \ m) \in S_{mc}.
$$
View \( \sigma_1 \) and element of \( S_{mc} \) (even though it looks like it could be an element of \( S_m \)). Similarly let \( \sigma_2 \) be the cycle in \( S_{mc} \) that is second in the expression for \( x \),

\[
\sigma_2 = (m+1 \ldots 2m) \in S_{mc}.
\]

In general, let \( \sigma_k \) be the \( k \)th cycle in the expression for \( x \),

\[
\sigma_k = ((k-1)m+1 \ldots mk) \in S_{mc}.
\]

If we write \( \mathbb{Z}/m = \{0, 1, \ldots, m-1\} \) (as usual), this allows use to define a map

\[
\psi: (\mathbb{Z}/m)^c \longrightarrow S_{mc}
\]

\[
(\epsilon_1, \ldots, \epsilon_c) \longrightarrow \sigma_1^{\epsilon_1} \sigma_2^{\epsilon_2} \cdots \sigma_c^{\epsilon_c}.
\]

(In class, the map \( \psi \) corresponded to the “concatenation” \( \langle \epsilon_1 \cdots \epsilon_c \rangle \). The version with \( \psi \) is more precise.)

**Lemma 8** The map \( \psi \) is a homomorphism. Moreover, the image of \( \psi \) lands in the stabilizer of \( x \) in \( G = S_{mc} \).

**Proof of Lemma.** To show that \( \psi \) is a homomorphism we have to check

\[
\psi((\epsilon_1, \ldots, \epsilon_c)(\epsilon_1', \ldots, \epsilon_c')) = \psi(\epsilon_1, \ldots, \epsilon_c) \psi(\epsilon_1', \ldots, \epsilon_c').
\]

The left-hand side of (9) is

\[
\psi(\epsilon_1 \epsilon_1', \ldots, \epsilon_c \epsilon_c') = \sigma_1^{\epsilon_1 \epsilon_1'} \cdots \sigma_c^{\epsilon_c \epsilon_c'}
\]

\[
= \sigma_1^{\epsilon_1} \sigma_1^{\epsilon_1'} \cdots \sigma_1^{\epsilon_c} \sigma_1^{\epsilon_c'}.
\]

Now it is clear that the cycles \( \sigma_i \) and \( \sigma_j \) are disjoint (if \( i \neq j \)); so they (and all their powers) commute. So we can rearrange the terms of the previous equation to read

\[
\psi(\epsilon_1 \epsilon_1', \ldots, \epsilon_c \epsilon_c') = (\sigma_1^{\epsilon_1} \cdots \sigma_1^{\epsilon_c})(\sigma_1^{\epsilon_1'} \cdots \sigma_1^{\epsilon_c'}).
\]

But clearly this is just

\[
= \psi(\epsilon_1, \ldots, \epsilon_c) \psi(\epsilon_1', \ldots, \epsilon_c').
\]

So, indeed, \( \psi \) is a homomorphism.

To prove the assertion that \( \psi \) maps into the stabilizer, we argue as follows. Let \( a_i = (0, \ldots, 0, 1, 0, \ldots 0) \in (\mathbb{Z}/m)^c \) with the 1 in the \( i \)th position. So \( \psi(a_i) = \sigma_i \). From the definition of \( x \) and our knowledge of the conjugation action, we compute

\[
\psi(a_1)x\psi(a_1)^{-1} = \sigma_1 x \sigma_1^{-1} = (\sigma_1(1) \sigma_1(2) \cdots \sigma_1(m)) \cdots (\sigma_1(cm-c+1) \cdots \sigma_1(mc))
\]

\[
= (23 \cdots m)(m+1m+2 \cdots 2m) \cdots (cm-c+1 cm-c+1 \cdots mc)
\]

\[
= x.
\]

So \( \psi(a_1) \in \text{Stab}_G(x) \). A similar computation shows that \( \psi(a_j) \in \text{Stab}_G(x) \) for any \( j \). Now take a general element \( (\epsilon_1, \ldots, \epsilon_c) \in (\mathbb{Z}/m)^c \). Then we compute

\[
\psi(\epsilon_1, \ldots, \epsilon_c) = \psi(a_1^{\epsilon_1}, \ldots, a_1^{\epsilon_c}),
\]
and since $\psi$ is a homomorphism, this equals
\[ \psi(a_1)^{\epsilon_1} \cdots \psi(a_c)^{\epsilon_c}. \]

Now we have check that each $\psi(a_j) \in \text{Stab}_G(x)$. Since $\text{Stab}_G(x)$ is a group, this means that $\psi(a_1)^{\epsilon_1} \cdots \psi(a_c)^{\epsilon_c}$ and hence $\psi(\epsilon_1, \ldots, \epsilon_c)$ is in $\text{Stab}_G(x)$. \hfill \Box

Now define a map
\[ \eta : S_c \longrightarrow S_{mc} \]
\[ \sigma \longrightarrow \Sigma \]
as follows. First define
\[ \eta(12) = (1 m+1)(2 m+2) \cdots (m 2m); \]
so $\eta(12)$ swaps the first two “chunks” of coordinates. Define
\[ \eta(123 \cdots c) = (1 2m + 1 3m + 1 \cdots cm - m + 1)(2 2m + 2 3m + 2 \cdots cm - m + 2) \cdots (m 2m 3m \cdots cm); \]
so $\eta(123 \cdots c)$ takes the first chunk of coordinates to the second, the second chunk to the third, and so on, until the $c$th chunk gets sent back to the first chunk. Since $(12)$ and $(123 \cdots c)$ generate $S_c$, each element $\sigma \in S_c$ can be written as a product $\tau_1 \cdots \tau_k$ where each $\tau_i$ is either $(12)$ or $(123 \cdots c)$. Define
\[ \eta(\sigma) = \eta(\tau_1) \cdots \eta(\tau_k); \] (10)
since each $\eta(\tau_i)$ is already defined the right-hand side is defined. It takes a little checking to verify that $\eta$ is well-defined. This amounts to the observation that for general $\sigma$, the definition given above takes the $i$th chunk of coordinates to the $\sigma(i)$th chunk. We leave this for you to check. The definition in (10) automatically makes $\eta$ a homomorphism. (Check!) Summarizing, we conclude that $\eta$ is well-defined homomorphism from $S_c$ to $S_{mc}$.

**Lemma 11** For each $\sigma \in S_c$, $\eta(\sigma) \in \text{Stab}_G(x)$.

**Proof of Lemma.** Consider $\eta(\sigma)x\eta(\sigma)^{-1}$. From the discussion above this will move the $i$th cycle in the expression of $x$ to the $\sigma(i)$th cycle. But these cycles are disjoint, so the result is still $x$. \hfill \Box

**Theorem 12** Every element of $\text{Stab}_G(x)$ may be written as
\[ \psi(\epsilon_1, \ldots, \epsilon_c)\eta(\sigma) \]
for unique elements $(\epsilon_1, \ldots, \epsilon_c) \in (\mathbb{Z}/m)^c$ and $\sigma \in S_c$.

**Proof of theorem.** Suppose $g \in \text{Stab}_G(x)$. Then $gxg^{-1} = x$. Since we know how conjugation works, we conclude, for instance, that $g(1 2 \cdots m)g^{-1}$ must map to some other cycle
\[ (km+1 km+2 \cdots (k+1)m) \]
for some $k$. (That is, $g$ maps the first cycle to the $k + 1$st.) Then since we know how conjugation acts, we conclude that there exists $j_1$ such that
\[ g(1) = km+j_1+1; \quad g(2) = km+j_1+2; \quad \cdots; \]
here if $km + j_1 + l > (k+1)m$, we subtract off $m$. Define $\sigma(1) = k+1$ and $\epsilon_1 = j_1$. Continuing in this way by considering $g(m+1)^m + 2\cdots 2m)^{-1}$ to define $\sigma(2)$ and $\epsilon_2 = j_2$; and so on. This defines an element $\sigma \in S_c$ and $(\epsilon_1, \ldots, \epsilon_c) \in (\mathbb{Z}/m)^c$. By construction
\[ g = \psi(\epsilon_1, \ldots, \epsilon_c) \eta(\sigma), \]
and the elements $\sigma \in S_c$ and $(\epsilon_1, \ldots, \epsilon_c) \in (\mathbb{Z}/m)^c$ so constructed are unique. 

**Lemma 13** Fix $\sigma$ and $\sigma'$ in $S_c$ and $(\epsilon_1, \ldots, \epsilon_c)$ and $(\epsilon_1', \ldots, \epsilon_c')$ and in $(\mathbb{Z}/m)^c$. Then in $S_m c$
\[ \psi(\epsilon_1, \ldots, \epsilon_c) \eta(\sigma) \psi(\epsilon_1', \ldots, \epsilon_c') \eta(\sigma') = \psi(\epsilon_1, \ldots, \epsilon_c) \psi(\epsilon_{\sigma^{-1}(1)'}, \ldots, \epsilon_{\sigma^{-1}(m)}') \eta(\sigma) \eta(\sigma'). \]

**Proof of Lemma.** After canceling $\psi(\epsilon_1, \ldots, \epsilon_c)$ on the left and $\eta(\sigma')$ on the right in the conclusion of the lemma, we must prove
\[ \eta(\sigma) \psi(\epsilon_1', \ldots, \epsilon_c') = \psi(\epsilon_{\sigma^{-1}(1)'}, \ldots, \epsilon_{\sigma^{-1}(m)}') \eta(\sigma). \]
(This is Ron’s favorite argument in disguise.) We compute where the left-hand side sends each index, and verify that this is where the right-hand side sends the index. Start with the index 1. The left hand side first rearranges 1 according to $\sigma_1'$ and then takes the result and moves it into the $\sigma(1)$st chunk of coordinates. Meanwhile, the right-hand side takes 1, moves it into the $\sigma(1)$st chunk of coordinates and then rearranges it according to the power of $\sigma_{\sigma(1)}$ that the $\sigma(1)$ entry of
\[ \left( \epsilon_1', \ldots, \epsilon_{\sigma^{-1}(m)}' \right) \]
specifies. But this power is $\epsilon_{\sigma^{-1}(\sigma(1))} = \epsilon_1$. So, indeed, the right-hand side maps 1 to the same place that the left-hand side does. We can repeat the same analysis for all the other indices $2, \ldots, mc$. The lemma follows.

**Proof of Theorem 7.** Define a map
\[ \Psi : (\mathbb{Z}/m)^c \times S_c \longrightarrow \text{Stab}_G(x) \]
via
\[ ((\epsilon_1, \ldots, \epsilon_c), \sigma) \longrightarrow \psi(\epsilon_1, \ldots, \epsilon_c) \eta(\sigma). \]
Theorem 12 says that for every $g \in \text{Stab}_G(x)$, there exists $(\epsilon_1, \ldots, \epsilon_c)$ and $\sigma$ such that
\[ g = \psi(\epsilon_1, \ldots, \epsilon_c) \eta(\sigma); \]
so $\Psi$ is surjective. Theorem 12 also says that $(\epsilon_1, \ldots, \epsilon_c)$ and $\sigma$ are unique; so $\Psi$ is injective.

It remains to check that $\Psi$ is a homomorphism. This is essentially Lemma 13, as we now show. Fix
\[ ((\epsilon_1, \ldots, \epsilon_c), \sigma) \text{ and } ((\epsilon_1', \ldots, \epsilon_c'), \sigma') \in (\mathbb{Z}/m)^c \times S_c. \]
Their product, according to the definition of the semidirect product defined by $\Phi'$ is,
\[ \left( \epsilon_1 \epsilon_{\sigma^{-1}(1)}, \ldots, \epsilon_c \epsilon_{\sigma^{-1}(c)}, \sigma \sigma' \right) \tag{14} \]
We compute:

\[ \Psi ((\epsilon_1, \ldots, \epsilon_c), \sigma) \Psi ((\epsilon'_1, \ldots, \epsilon'_c), \sigma') = \psi(\epsilon_1, \ldots, \epsilon_c) \eta(\sigma) \psi(\epsilon'_1, \ldots, \epsilon'_c) \eta(\sigma') \]
\[ = \psi(\epsilon_1, \ldots, \epsilon_c) \psi(\epsilon'_{\sigma^{-1}(1)}, \ldots, \epsilon'_{\sigma^{-1}(m)}) \eta(\sigma) \eta(\sigma') \]
\[ = \Psi \left( (\epsilon_1 \epsilon'_{\sigma^{-1}(1)}, \ldots, \epsilon_c \epsilon'_{\sigma^{-1}(c)}), \sigma \sigma' \right) \]
\[ = \Psi \left( ((\epsilon_1, \ldots, \epsilon_c), \sigma)((\epsilon'_1, \ldots, \epsilon'_c), \sigma') \right). \]

The first equality follows by definition of \( \Psi \); the second is Lemma 13; the third is again the definition of \( \Psi \); and the last is Equation (14). Reading the above string of equations left to right shows \( \Psi \) is a homomorphism. This completes the proof of Theorem 7. \( \square \)