Chapter 3.5: Supplementary notes on semi-direct products

Several times we used that in constructing semi-direct products that choosing different generators gives isomorphic groups. We also have used that in certain cases if $\phi_1, \phi_2 : K \rightarrow Aut(H)$ if one has that $\phi_1(K)$ and $\phi_2(K)$ are conjugate, then we get isomorphic groups. We summarize these results here, with proof. We begin with a simple lemma from undergraduate abstract algebra.

**Lemma:** Let $a, m, n \in \mathbb{Z}$ with $m|n$ and $gcd(a, m) = 1$. Then $gcd(a + xm, n) = 1$ for some integer $x$.

**Proof:** Write $n = ef$ where $e$ consists of the primes dividing $m$ and $f$ consists of the other primes. Then clearly we have,

$$gcd(a + xm, e) = 1$$

for if $p|e$ and $p|(a + xm)$ by construction we have $p|m$ and so $p|a$. This contradicts $gcd(a, m) = 1$.

Now since $gcd(m, f) = 1$ we know the congruence

$$a + xm \equiv 1 \pmod{f}$$

has solutions, namely, $x = m^{-1}(1 - a)$ where $m^{-1}$ is the inverse of $m$ modulo $f$. Since $gcd(e, f) = 1$, we can use the Chinese remainder theorem to find a solution to the congruence

$$a + xm \equiv 1 \pmod{n}$$

and we are done. □

Note that this lemma also gives the map

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \longrightarrow \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$$

is surjective for $n|m$.

**Theorem:** Let $K$ be a finite cyclic group and $\phi_1, \phi_2 : K \rightarrow Aut(H)$ homomorphisms. Suppose that $\phi_1(K)$ and $\phi_2(K)$ are conjugate in $Aut(H)$. Then

$$H \rtimes_{\phi_1} K \cong H \rtimes_{\phi_2} K$$
Proof: Write $K = \langle z \rangle$. There exists a $\sigma \in \text{Aut}(H)$ so that $\phi_2(K) = \sigma \phi_1(K) \sigma^{-1}$. Write $c_\sigma$ for the conjugation by $\sigma$ map in $\text{Aut}(H)$. Thus, we have

$$c_\sigma \cdot \phi_1(z) = \phi_2(y)$$

for some $y \in K$. Since $K$ is cyclic, there is an $a \in \mathbb{Z}$ so that $y = z^a$. Thus, we have

$$c_\sigma \cdot \phi_1(z) = \phi_2(z)^a.$$  

Let $x \in K$. Write $x = z^b$. Then

$$c_\sigma \cdot \phi_1(x) = c_\sigma \cdot \phi_1(z^b) = (c_\sigma \cdot \phi_1(z))^b = (\phi_2(z)^a)^b = \phi_2(z)^{ab} = \phi_2(x)^a.$$

Thus, $c_\sigma \cdot \phi_1(x) = \phi_2(x)^a$ for all $x \in K$. Define a map

$$\Psi : H \rtimes_{\phi_1} K \longrightarrow H \rtimes_{\phi_2} K$$

$$(h, x) \mapsto (\sigma(h), x^a).$$

We claim this is a homomorphism. Let $(h_1, x_1), (h_2, x_2)$ be elements in $H \rtimes_{\phi_1} K$. Then we have

$$\Psi((h_1, x_1)(h_2, x_2)) = \Psi((h_1 \phi_1(x_1)(h_2), x_1 x_2))$$

$$= (\sigma(h_1) \phi_1(x_1)(\sigma(h_2)), x_1^a x_2^a)$$

$$= (\sigma(h_1) \cdot \phi_1(x_1) \cdot \sigma^{-1}(\sigma(h_2)), x_1^a x_2^a)$$

$$= (\sigma(h_1) \phi_2(x_1^a)(\sigma(h_2)), x_1^a x_2^a)$$

$$= (\sigma(h_1), x_1^a)(\sigma(h_2), x_2^a)$$

$$= \Psi(h_1, x_1) \Psi(h_2, x_2).$$

Thus, $\Psi$ is a homomorphism. Note that we have not used that $K$ is finite to this point, so we will quote up to this point in the next theorem. We will
now use the lemma to complete the proof by showing $\Psi$ has a 2-sided inverse.

Observe that since $\sigma \in \text{Aut}(H)$, we have $|\phi_2(K)| = |\phi_1(K)|$. Since $\phi_1(z)$ generates $\phi_1(K)$, we have that $c_{\sigma^{-1}} \circ \phi_2(z^a) = (c_{\sigma^{-1}} \circ \phi_2(z))^a$ generates $\phi_2(K)$. Thus, from our work on cyclic groups we have $\gcd(a,|\phi_2(K)|) = 1$. Since $K/\ker \phi_2 \cong \phi_2(K)$, we have $|\phi_2(K)|||K|$. We now apply the lemma with $n = |K|, m = |\phi_2(K)|$. Observe that $\phi_2(y)^{a+b\phi_2(K)} = \phi_2(y)^a$ for any integer $b$, so we can replace $a$ by $a+b|\phi_2(K)|$ for any integer $b$. Thus, the lemma allows us to assume that $\gcd(a,|K|) = 1$. Set $a^{-1}$ to be the inverse of $a$ modulo $|K|$. Define

$$
\Psi^{-1} : H \rtimes_{\phi_2} K \longrightarrow H \rtimes_{\phi_1} K
$$

$$(h, x) \mapsto (\sigma^{-1}(h), x^{a^{-1}})
$$

Then it is clear that $\Psi^{-1}$ is the 2-sided inverse of $\Psi$ and so we have the result. □

We now deal with the case that $K$ is infinite. In this case the argument about finding "$a^{-1}$" in the previous proof will not work. Thus, we must assume $\phi_1, \phi_2$ are injective.

**Theorem:** Let $K$ be an infinite cyclic group and let one of $\phi_1, \phi_2 : K \longrightarrow \text{Aut}(H)$ be a monomorphism, i.e., injective homomorphism. Suppose that $\phi_1(K)$ and $\phi_2(K)$ are conjugate in $\text{Aut}(H)$. Then

$$
H \rtimes_{\phi_1} K \cong H \rtimes_{\phi_2} K
$$

**Proof:** We use the results in the proof of the last theorem to construct a homomorphism

$$
\Psi : H \rtimes_{\phi_1} K \longrightarrow H \rtimes_{\phi_2} K
$$

$$(h, x) \mapsto (\sigma(h), x^a)
$$

We now need to construct a 2-sided inverse to this map. Assume $\phi_1$ is an injective homomorphism.
Let $x \in K$. We have that $c_\sigma \circ \phi_1(x) = \phi_2(x^a)$ so $\phi_1(x) = c_{\sigma^{-1}} \circ \phi_2(x^a)$. Thus, $\phi_1$ maps $x$ to the element $c_{\sigma^{-1}} \circ \phi_2(x^a)$ in $\text{Aut}(H)$. We can consider the set $\phi_1^{-1}(c_\sigma \circ \phi_2(x^a)) = \{y \in K : \phi_1(y) = c_{\sigma^{-1}} \circ \phi_2(x^a)\}$. In general this set can contain many elements; however, if $\phi_1$ is injective then we have

$$\phi_1^{-1}(c_\sigma \circ \phi_2(x^a)) = \{x\}.$$ 

In general, given $y \in K$, we have $c_{\sigma^{-1}} \circ \phi_2(y) \in \phi_1(K)$ since $\sigma \phi_1(K) \sigma^{-1} = \phi_2(K)$ i.e., $\phi_1(K) = \sigma^{-1} \phi_2(K) \sigma$. Thus, $\phi_1^{-1}(c_{\sigma^{-1}} \circ \phi_2(y))$ is non-empty, and since $\phi_1$ is injective we have that $\phi_1^{-1}(c_{\sigma^{-1}} \circ \phi_2(y))$ is a single element, so we have a well-defined map

$$\Phi : K \rightarrow K$$

$$x \mapsto \phi_1^{-1}(c_{\sigma^{-1}} \circ \phi_1(y)).$$

Define

$$\Psi^{-1} : H \rtimes_{\phi_2} K \rightarrow H \rtimes_{\phi_1} K$$

$$(h, x) \mapsto (\sigma^{-1}(h), \Phi(x)).$$

Then it is easy to see this is a 2-sided inverse to $\Psi$ by construction of $\Phi$.

If $\phi_2$ is injective instead of $\phi_1$, just reverse the argument. □

Finally we end with result that takes care of the case of choosing a different generator of the group.

**Theorem:** Let $\phi_1, \phi_2 : K \rightarrow \text{Aut}(H)$ be homomorphisms and suppose there are automorphisms $\psi \in \text{Aut}(K), \chi \in \text{Aut}(H)$ so that

$$\phi_2 = c_\chi \circ \phi_1 \circ \psi$$

where again $c_\chi$ is conjugation by $\chi$ in $\text{Aut}(H)$. Then

$$H \rtimes_{\phi_1} K \cong H \rtimes_{\phi_2} K.$$ 

**Proof:** Define

$$\Psi : H \rtimes_{\phi_1} K \rightarrow H \rtimes_{\phi_2} K$$

$$(h, x) \mapsto (\chi(x), \psi^{-1}(x)).$$
One can check this is a homomorphism by an analogous argument to the proof of the previous theorems. The 2-sided inverse here is given by

$$\Psi^{-1} : H \rtimes_{\phi_2} K \to H \rtimes_{\phi_1} K$$

$$(h, x) \mapsto (\chi^{-1}(h), \psi(x)).$$

$\square$