The Minnesota Journal of Undergraduate Mathematics

Constructing subgroups of semi-direct products via generalized derivations

Jill Dietz, Asa Giannini, Akina Khan, and Michael Schroeder

St. Olaf College

The Minnesota Journal of Undergraduate Mathematics

Volume 4 (2018-19 Academic Year)

Sponsored by
School of Mathematics
University of Minnesota
Minneapolis, MN 55455

The Minnesota Journal of Undergraduate Mathematics

Volume 4 (2018-19 Academic Year)

Constructing subgroups of semi-direct products via generalized derivations

Jill Dietz, Asa Giannini, Akina Khan* , and Michael Schroeder

St. Olaf College

Abstract. There is a well-known correspondence due to Goursat between subgroups of a direct product of groups, $A \times B$, and triples of the form $(A_1/A_2, B_1/B_2, \sigma)$ where $A_2 \triangleleft A_1 \leq A$, $B_2 \triangleleft B_1 \leq B$, and $\sigma : A_1/A_2 \to B_1/B_2$ is an isomorphism. By contrast, there is a little known correspondence due to Usenko between subgroups of a semi-direct product $U \rtimes_\phi H$, where $\phi : H \to \operatorname{Aut} U$, and triples of the form (L, R, θ), where $L \leq U$, $R \leq H$, and $\theta : R \to U$ is a kind of generalized derivation (crossed homomorphism). While Goursat's theorem has been used many times to investigate subgroups of direct products, Usenko's theorem has not, perhaps due to the computational complexity of finding the generalized derivations. In our paper, we find ways of reducing the computational complexity, and show how to use Usenko's correspondence to determine all of the subgroups of a certain metacyclic p-group.

1. Introduction

In 1889, E. Goursat [1] established a correspondence between subgroups of a direct product of groups, $A \times B$, and triples of the form $(A_1/A_2, B_1/B_2, \sigma)$ where $A_2 \triangleleft A_1 \leq A$, $B_2 \triangleleft B_1 \leq B$, and $\sigma : A_1/A_2 \to B_1/B_2$ is an isomorphism. One hundred years later there were two attempts to describe the subgroups of a semi-direct product $U \rtimes_\phi H$, where H acts on U via $\phi : H \to \operatorname{Aut} U$, in terms of information about its components. In 1988, K. Rosenbaum [3] determined that a set S of elements in $U \rtimes H$ is a subgroup if and only if (i) $SU \cap H$ and $S \cap H$ are subgroups of UH, (ii) $S \cap U$ is a subgroup and $HS \cap U$ is a collection of $S \cap U$-cosets in U, and (iii) there is a function ϕ defined for all $h \in SU \cap H$ mapping $(S \cap H)h$ onto some coset $u(S \cap U)$ with $u \in U$ satisfying the condition $\phi(h_1 h_2) = h_2^{-1}\phi(h_1)h_2\phi(h_2)$ [2]. Three years later, V.M. Usenko [4] described subgroups Γ of $U \rtimes H$ in a manner analogous to Goursat's theorem by associating Γ with a triple (L, R, θ), where $L \leq U$, $R \leq H$, and $\theta : R \to U$ is a generalized derivation (described in detail below).

While Goursat's theorem has been used many times to investigate subgroups of direct products, neither the work of Rosenbaum nor Usenko has been cited much. Usenko's theory is particularly promising, but computationally exhausting because his generalized derivations are ubiquitous. In our paper, we find ways of reducing the computational complexity of using Usenko's correspondence.

* *Corresponding author*

The paper is organized as follows: In Section 2 we establish notation and describe Usenko's correspondence between subgroups of $U \rtimes H$ and triples of the form (L, R, θ); in Section 3 we show how to reduce the search for subgroups by reducing the number of functions θ one must consider; in Section 4 we apply our theory to find all subgroups of a particular metacyclic p-group; and we conclude our paper in Section 5.

2. Usenko's Correspondence

We begin with some definitions and notation.

- Throughout the paper, $G = U \rtimes_\phi H$ will be a semi-direct product of groups with the action of H on U given by the homomorphism $\phi : H \to \operatorname{Aut} U$. We will also write $U \rtimes H$ when the action is clear. We will typically write elements of G in the form (u, h), where $u \in U$ and $h \in H$.
- For $h \in H$ and $u \in U$, we will denote the action of h on u by u^h.
- The product in G is given by
$$(u_1, h_1)(u_2, h_2) = (u_1 u_2^{h_1}, h_1 h_2),$$
where $u_i \in U$ and $h_i \in H$.
- Let $R \leq H$. A *derivation* $\delta : R \to U$ is a function satisfying $\delta(r_1 r_2) = \delta(r_1)\delta(r_2)^{r_1}$ for all $r_i \in R$. Derivations are also called *crossed homomorphisms* in the literature. The set of all derivations $R \to U$ will be denoted $\operatorname{Der}(R, U)$.
- Let $L \leq U$. An *L-reduced* derivation $\delta : R \to U$ satisfies the property that for all $r_i \in R$ there exists $\lambda \in L$ such that
$$\delta(r_1 r_2) = \lambda \delta(r_1)\delta(r_2)^{r_1}. \tag{1}$$
The set of all L-reduced derivations $R \to U$ will be denoted $\operatorname{Der}_L(R, U)$.
- A *normal* L-reduced derivation $\delta : R \to U$ further satisfies
$$\delta(r) \cdot l^r \cdot \delta(r)^{-1} \in L \tag{2}$$
for all $r \in R$ and $l \in L$. The set of all normal L-reduced derivations $R \to U$ will be denoted $\operatorname{NDer}_L(R, U)$ and we will say δ is "NLR."
- A *normal L-reduced triple*, or NLR triple, in $U \rtimes H$ is (L, R, θ), where $L \leq U$, $R \leq H$, and $\theta : R \to U$ is NLR.
- The *fiber-product* of an NLR triple (L, R, θ) is
$$L \bowtie R = \{(l\theta(r), r) \mid l \in L, r \in R\}.$$
We will also use the notation $L \bowtie^\theta R$ and $L \bowtie_\phi^\theta R$ when we need to call attention to either the NLR θ or the action given by ϕ.
- We will use the dihedral group of order 12, which we denote D_{12}, to provide illustrations of some results in what follows. We consider $D_{12} = U \rtimes H$ where $U = \langle \sigma \rangle \cong \mathbb{Z}_6$ and $H = \langle \tau \rangle \cong \mathbb{Z}_2$, with σ a rotation of order 6 and τ a reflection. The action of H on U is given by $\sigma^\tau = \sigma^{-1}$.

Usenko describes a correspondence between subgroups Γ of $U \rtimes H$ and NLR triples (L, R, θ). The correspondence is not bijective; we will see that many NLR derivations give rise to the same subgroup.

On one hand, if (L,R,θ) is an NLR triple in $U \rtimes H$, then the fiber-product $L \bowtie R$ is easily seen to be a subgroup of $U \rtimes H$ of order $|L||R|$.

On the other hand, given a subgroup $\Gamma \leq U \rtimes H$ we will associate it with a triple. Let

$$U_\Gamma = \Gamma \cap U = \{u \in U \,|\, (u,e) \in \Gamma\} \text{ and}$$
$$\Gamma_H = \{h \in H \,|\, (u,h) \in \Gamma \text{ for some } u \in U\}.$$

It is easy to prove that $U_\Gamma \triangleleft \Gamma$, and $\Gamma/U_\Gamma \cong \Gamma_H$. Let $x \in \Gamma_H$ correspond to the coset $U_\Gamma(y,x)$, where $y \in U$, and define $\theta_\Gamma(x) = y$ to obtain a map $\theta_\Gamma : \Gamma_H \to U$. If (u,x) is any other representative of the same coset then $(u,x) = (v,e)(y,x) = (vy,x)$ for some $v \in U_\Gamma$. Indeed,

$$(u,x) = (u\theta_\Gamma(x)^{-1}\theta_\Gamma(x), x)$$

where $u\theta_\Gamma(x)^{-1} \in U_\Gamma$.

Lemma 2.1. *As defined above, $\theta_\Gamma : \Gamma_H \to U$ is a normal U_Γ-reduced derivation.*

Proof. Usenko proves this in his Proposition 1.3.2, but we include a proof here for completeness.

We will simply denote θ_Γ as θ when the association with Γ is clear. Let $x_1, x_2 \in \Gamma_H$ with $x_1x_2 = x_3 \in \Gamma_H$. Set $\theta(x_i) = y_i \in U$, where $(y_i, x_i) \in \Gamma$. Since $(y_1,x_1)(y_2,x_2) = (y_1y_2^{x_1}, x_3)$ we know from above that $y_1y_2^{x_1} = y_1y_2^{x_1}\theta(x_3)^{-1}\theta(x_3)$, where $y_1y_2^{x_1}\theta(x_3)^{-1} \in U_\Gamma$. Thus, θ satisfies equation (1) and is a U_Γ-reduced derivation.

Let $r \in \Gamma_H$ and $l \in U_\Gamma$. Set $g_1 = (u\theta(r), r)$ and $g_2 = (l\theta(x), x)$, where $u \in U_\Gamma$ and $x \in \Gamma_H$, then $g_i \in \Gamma$. As above, we have

$$g_1g_2 = (u\theta(r)l^r\theta(x)^r\theta(rx)^{-1}\theta(rx), rx)$$

where $u\theta(r)l^r\theta(x)^r\theta(rx)^{-1} \in U_\Gamma$. Now $u\theta(r)l^r\theta(x)^r\theta(rx)^{-1} = uv_1v_2$ where $v_1 = \theta(r)l^r\theta(r)^{-1}$ and $v_2 = \theta(r)\theta(x)^r\theta(rx)^{-1}$. We know $v_2 \in U_\Gamma$ by the argument above showing that θ is a U_Γ-reduced derivation. By assumption $u \in U_\Gamma$, hence $v_1 \in U_\Gamma$. We have shown that θ satisfies equation (2) and is a normal U_Γ-reduced derivation. □

The lemma above shows that $(U_\Gamma, \Gamma_H, \theta_\Gamma)$ is a normal U_Γ-reduced triple (or NLR triple, where $L = U_\Gamma$).

Example 2.2. In D_{12}, let $L = \langle\sigma^2\rangle$, $R = \langle\tau\rangle$, and define $\theta : R \to U$ by $\theta(e) = \sigma^2$ and $\theta(\tau) = \sigma$. One can check that $\theta \in \mathrm{NDer}_L(R,U)$. The fiber-product $L \bowtie R$ will have order 6 and

$$\begin{aligned} L \bowtie R &= \{l\theta(r), r) \,|\, l \in L, r \in R\} \\ &= \{(e,e),(\sigma^2,e),(\sigma^4,e),(\sigma,\tau),(\sigma^3,\tau),(\sigma^5,\tau)\} \\ &= \langle\sigma^2, \sigma\tau\rangle. \end{aligned}$$

On the other hand, if

$$\Gamma = \{(e,e),(\sigma^3,e),(\sigma^2,\tau),(\sigma^5,\tau)\} = \langle\sigma^3, \sigma^2\tau\rangle,$$

then $L = U_\Gamma = \langle\sigma^3\rangle$ and $R = \Gamma_H = \langle\tau\rangle$. The element $e \in \Gamma_H$ corresponds to the coset $U_\Gamma(e,e) = \{(e,e),(\sigma^3,e)\}$, while $\tau \in \Gamma_H$ corresponds to $U_\Gamma(\sigma^2,\tau) = \{(\sigma^2,\tau),(\sigma^5,\tau)\}$. We can define θ :

$R \to U$ in four different ways, one of which is given by $\theta(e) = e$ and $\theta(\tau) = \sigma^2$. It is routine to check that $\theta \in \mathrm{NDer}_L(R,U)$ and $L \bowtie R = \Gamma$.

As mentioned earlier, a particular subgroup of $U \rtimes H$ can be associated with many different NLR derivations. We can see in the definition of θ_Γ that it does not depend on the coset representative of $x \in \Gamma_H$ mod U_Γ. We make this notion more precise in the next proposition.

Theorem 2.3. *Let $L \leq U$, $R \leq H$ and $\theta_i : R \to U$, $i = 1,2$, be two NLR derivations in $U \rtimes H$. We have $L \bowtie^{\theta_1} R = L \bowtie^{\theta_2} R$ if and only if $L\theta_1(r) = L\theta_2(r)$ for all $r \in R$.*

Proof. First assume $L\theta_1(r) = L\theta_2(r)$ for all $r \in R$. Let $(x\theta_1(r), r) \in L \bowtie^{\theta_1} R$ for some $x \in L$ and $r \in R$. There exists $x_1 \in L$ such that $\theta_1(r) = x_1\theta_2(r)$. Now $(x\theta_1(r), r) = (xx_1\theta_2(r), r) \in L \bowtie^{\theta_2} R$. Thus $L \bowtie^{\theta_1} R \subseteq L \bowtie^{\theta_2} R$. Similarly, $L \bowtie^{\theta_2} R \subseteq L \bowtie^{\theta_1} R$.

Next assume that $L \bowtie^{\theta_1} R = L \bowtie^{\theta_2} R$. Let $r \in R$ and $x \in L$ so that $(x\theta_1(r), r) \in L \bowtie^{\theta_1} R$. There exist $x_1 \in L$ and $r_1 \in R$ such that $(x\theta_1(r), r) = (x_1\theta_2(r_1), r_1)$. Clearly $r_1 = r$, hence $x\theta_1(r) = x_1\theta_2(r)$ and $\theta_1(r)$ is equivalent to $\theta_2(r)$ mod L. □

Example 2.4. In D_{12}, let $L = \langle \sigma^2 \rangle$ and $R = \langle \tau \rangle$. Define $\theta_1 : R \to U$ by $\theta_1(e) = \sigma^2$ and $\theta(\tau) = \sigma$ as in Example 2.2. Define $\theta_2 : R \to U$ by $\theta_2(e) = \sigma^2$ and $\theta(\tau) = \sigma^3$. Then the image of θ_1 is equivalent to the image of θ_2 mod L, and one can see that

$$L \bowtie^{\theta_1} R = L \bowtie^{\theta_2} R = \{(e,e), (\sigma^2, e), (\sigma^4, e), (\sigma, \tau), (\sigma^3, \tau), (\sigma^5, \tau)\}.$$

On the other hand, if we define $\theta_3 : R \to U$ by $\theta_3(e) = \sigma^2$ and $\theta(\tau) = \sigma^4$ then one can show that $\theta_3 \in \mathrm{NDer}_L(R,U)$, but $L\theta_1(\tau) \neq L\theta_3(\tau)$. Moreover,

$$L \bowtie^{\theta_3} R = \{(e,e), (\sigma^2, e), (\sigma^4, e), (e, \tau), (\sigma^2, \tau), (\sigma^4, \tau)\} \neq L \bowtie^{\theta_1} R.$$

3. Finding NLR triples

Our main goal is to construct subgroups of $U \rtimes H$ from information about the component groups U and H. The three necessary ingredients are subgroups of U, subgroups of H, and normal reduced derivations. It is the latter item that is particularly vexing since typical group-theoretic tools are not at our disposal. If $R \leq H$, we begin with $|U|^{|R|}$ possible functions $R \to U$, although not all of them will be NLR for any $L \leq U$. In this section we aim to reduce the number of NLR's one must consider in order to construct all subgroups of $U \rtimes H$.

Our first important result is that we need only consider an NLR θ that satisfies $\theta(e) = e$. Before proving the result, we need a lemma.

Lemma 3.1. *Let (L, R, θ) be an NLR triple in $U \rtimes H$, then we must have $\theta(e) \in L$.*

Proof. Assume θ is a normal L-reduced derivation $R \to U$ and let $r \in R$. Since θ is L-reduced, we know there exists $l \in L$ such that

$$\theta(r) = \theta(er) = l\theta(e)\theta(r)^e.$$

Since e acts trivially on $\theta(r)$ we see that $\theta(e) = l^{-1} \in L$ as desired. □

To show it suffices to assume that an NLR maps the identity to itself, we will show that a fiber-product is precisely equal to one constructed under the condition that $e \mapsto e$.

Theorem 3.2. *Let (L, R, θ) be an NLR triple in $U \rtimes H$. Define $\theta' : R \to U$ by*

$$\theta'(r) = \begin{cases} e & \text{when } r = e, \\ \theta(r) & \text{when } r \neq e. \end{cases}$$

Then θ' is NLR and $L \bowtie^{\theta} R = L \bowtie^{\theta'} R$.

Proof. First we will show that θ' is an NLR derivation. Equation (1) is clearly satisfied by θ' when none of r_1, r_2, nor $r_1 r_2$, where $r_i \in R$, is equal to the identity. If either r_1 or r_2 is the identity, then it is easy to check that equation (1) holds. Now suppose $r_1 \neq e$ and $r_2 = r_1^{-1}$. On one hand, $\theta'(r_1 r_2) = \theta'(e) = e$. On the other hand,

$$\theta'(r_1)\theta'(r_2)^{r_1} = \theta(r_1)\theta(r_2)^{r_1} = l\theta(r_1 r_2)$$

for some $l \in L$ since θ is L-reduced. Further, $\theta(r_1 r_2) = \theta(e) = l_1$ for some $l_1 \in L$ by Lemma 3.1. Thus, $\theta'(r_1 r_2) = (l l_1)^{-1}\theta'(r_1)\theta'(r_2)^{r_1}$ and we see that θ' is L-reduced.

Equation (2) is clearly satisfied by θ' whether $r = e$ or not. Thus θ' is an NLR derivation.

Finally, by Theorem 2.3 we see that $L \bowtie^{\theta} R = L \bowtie^{\theta'} R$ if and only if $L\theta(r) = L\theta'(r)$ for all $r \in R$. When $r \neq e$ the cosets are equal because $\theta(r) = \theta'(r)$. When $r = e$ the cosets are equal because $\theta(e) \in L$ by Lemma 3.1. □

The upshot of the theorem above is that we need only consider functions $R \to U$ satisfying $e \mapsto e$, thus reducing the number of possibilities by a factor of $|U|$.

It is possible to say a bit more about NLR derivations when L is invariant under the action of R, given by ϕ.

Definition 3.3. In $U \rtimes H$, let $L \leq U$ and $R \leq H$. We say that L is "R-stable" if $l^r \in L$ for all $l \in L$ and $r \in R$.

If L is R-stable, it is easy to see that $L \rtimes_{\phi} R$ is a subgroup of $U \rtimes_{\phi} H$. Moreover, the subgroup is associated with the triple $(L, R, 1)$, where $1(r) = e$ for all $r \in R$. Of course the trivial derivation is not necessarily the only NLR derivation for the pair (L, R), so there can be other "diagonal" subgroups of $U \rtimes H$ generated by L and R. The next two results show how to narrow the search for elements of $\mathrm{NDer}_L(R, U)$ when L is R-stable.

Proposition 3.4. *In $U \rtimes H$, let $L \triangleleft U$ be R-stable, where $R \leq H$. If $\theta : R \to U$ is an L-reduced derivation, then it is normal L-reduced.*

Proof. Since L is invariant under the action of R and is a normal subgroup of U, it is easy to see that equation (2) holds for all $l \in L$ and $r \in R$. □

In practice, checking that a function $R \to U$ satisfies equation (1) is much easier than checking equation (2), so Proposition 3.4 can be useful. The next result shows how to construct new NLR derivations from existing ones.

Proposition 3.5. *Let (L, R, θ_1) be an NLR triple in $U \rtimes H$, where $L \lhd U$ is R-stable. Define $\theta_2 : R \to U$ as any function satisfying $L\theta_1(r) = L\theta_2(r)$ for all $r \in R$. Then θ_2 is also a normal L-reduced derivation.*

Proof. By Proposition 3.4 we need only show that $\theta_2 \in \mathrm{Der}_L(R, U)$. Let $r_1, r_2 \in R$ with $r_3 = r_1 r_2$. There exist $l_i \in L$ such that $\theta_1(r_i) = l_i \theta_2(r_i)$. Checking equation (1), we have

$$\begin{aligned}
\theta_2(r_1 r_2) &= l_3^{-1}\theta_1(r_1 r_2) \\
&= l_3^{-1}\lambda\theta_1(r_1)\theta_1(r_2)^{r_1}, \text{ for some } \lambda \in L \\
&= l_3^{-1}\lambda l_1\theta_2(r_1)(l_2\theta_2(r_2))^{r_1} \\
&= l_3^{-1}\lambda l_1\theta_2(r_1)l_2^{r_1}\theta_2(r_2)^{r_1} \\
&= l_3^{-1}\lambda l_1\theta_2(r_1)l_4\theta_2(r_2)^{r_1}, \text{ for some } l_4 \in L \\
&= l_3^{-1}\lambda l_1 l_5\theta_2(r_1)\theta_2(r_2)^{r_1}, \text{ for some } l_5 \in L \\
&= \lambda'\theta_2(r_1)\theta_2(r_2)^{r_1}, \text{ where } \lambda' = l_3^{-1}\lambda l_1 l_5 \in L.
\end{aligned}$$

□

Rather than using Proposition 3.5 to create additional NLR derivations, we use it to reduce the number of possibilities one must consider when trying to construct such functions.

We conclude this section with one more result concerning subgroups of $U \rtimes_\phi H$ of the form $L \rtimes_\phi R$.

Theorem 3.6. *In $U \rtimes_\phi H$, let $L \leq U$ be R-stable for some $R \leq H$. Any function $\theta : R \to L$ is an NLR derivation with associated fiber-product equal to $L \rtimes_\phi R$.*

Proof. As above, the function $1 : R \to U$ defined by $1(r) = e$ for all $r \in R$ is clearly an NLR derivation with corresponding fiber-product

$$L \bowtie_\phi^1 R = \{l1(r), r))|l \in L, r \in R\}.$$

As a set, $L \bowtie^1 R$ is equal to $L \times R$, and the product is determined by the action of R on L given by the restriction of ϕ. If $\theta : R \to L$, then it is easy to see that θ satisfies equations (1) and (2) because all computations are inside L. Finally, by Theorem 2.3 we know

$$L \bowtie_\phi^\theta R = L \bowtie_\phi^1 R = L \rtimes_\phi R.$$

□

4. Subgroups of a metacyclic p-group

A group G is *metacyclic* if it has a cyclic normal subgroup N so that G/N is also cyclic. A metacyclic group is *split* if the extension

$$1 \to N \to G \to G/N \to 1$$

splits. In this case, we can find $Q \leq G$ such that $G = N \rtimes Q$. We will consider the metacyclic p-group, $p > 2$, of the form

$$P = U \rtimes H$$

where $U = \langle x\rangle \cong \mathbb{Z}_{p^2}$, $H = \langle y\rangle \cong \mathbb{Z}_p$, and the action of H on U is given by $x^y = x^{p+1}$. The group P is extraspecial of order p^3 and has presentation

$$P = \langle x, y \,|\, x^{p^2} = e, y^p = e, yxy^{-1} = x^{p+1}\rangle.$$

The group P is well-known and for small values of p has small order, so its subgroups are well-known too; still, we will find all of the subgroups of P to illustrate the theory developed in Section 3.

The only subgroups of H are $\{e\}$ and $\langle y\rangle$. If $R = \{e\}$ and we insist that $\theta(e) = e$ because of Theorem 3.2, then $\theta = 1$ is an NLR derivation for all $L \leq U$ by Theorem 3.6, and $L \bowtie R = L$. This gives us the following three subgroups of P: $\{e\}$, $\langle x^p\rangle$, and $\langle x\rangle$.

If $R = \langle y\rangle$ then the fact that both U and H are cyclic gives us two helpful results: (i) the only options for subgroups L of U are $\{e\}$, $\langle x^p\rangle$, and $\langle x\rangle$; and (ii) the subgroups $\{e\}$ and $\langle x\rangle$ are clearly R-stable, and $(x^p)^y = x^{p(p+1)} = x^p$ shows that $\langle x^p\rangle$ is also R-stable.

We first use equation (1) to say something about the image of θ mod L.

Proposition 4.1. *In P, let $L \leq U$ and $R = H$. Let $\theta : R \to U$ be a function satisfying $\theta(e) = e$ and $\theta(y) = x^i$ for some $x^i \in U$. Then $\theta \in \mathrm{NDer}_L(R, U)$ if and only if both conditions below hold.*

(1) *For all $k = 1, 2, \ldots, p$, $\theta(y^k) \in Lx^{t_k}$, where*

$$t_k = i(1 + \alpha + \alpha^2 + \cdots + \alpha^{k-1})$$

with $\alpha = p + 1$.

(2) *When $L = \{e\}$, $i \equiv 0 \mod p$; and when $L = \langle x\rangle$ or $\langle x^p\rangle$, there are no restrictions on i.*

Proof. If $\theta \in \mathrm{NDer}_L(R, U)$, then we prove by induction that $\theta(y^k) \in Lx^{t_k}$. The result clearly holds for $k = 1$. Assume the result holds for k, we will show it also holds for $k + 1$. Now

$$\begin{array}{rcl} \theta(y^{k+1}) & = & \theta(yy^k) \\ & = & \lambda_1\theta(y)\theta(y^k)^y, \text{ for some } \lambda_1 \in L \\ & = & \lambda_1 x^i(\lambda_2 x^{t_k})^y, \text{ for some } \lambda_2 \in L \\ & = & \lambda_1 x^i \lambda_2^y (x^{t_k})^y \\ & = & \lambda_1 x^i \lambda_3 x^{\alpha t_k}, \text{ for some } \lambda_3 \in L \\ & = & \lambda_4 x^{t_{k+1}}, \text{ for some } \lambda_4 \in L. \end{array}$$

Property (2) comes from the fact that $y^p = e$, hence $\theta(y^p) \in L$. By property (1), we must have $x^{t_p} \in L$. Now

$$1 + \alpha + \alpha^2 + \cdots + \alpha^{p-1} = \frac{\alpha^p - 1}{\alpha - 1}.$$

Since $\alpha = (p + 1)$, we know that p^2 is the highest power of p that divides $\alpha^p - 1$. Let $\alpha^p - 1 = qp^2$ where $p \nmid q$, then

$$t_p = i(1 + \alpha + \alpha^2 + \cdots + \alpha^{p-1}) = i(\frac{qp^2}{p}) = iqp.$$

If $L = \langle x \rangle$ or $\langle x^p \rangle$, then $x^{iqp} \in L$. If $L = \{e\}$, then $x^{iqp} \in L$ if and only if $iqp \equiv 0 \mod p^2$. Hence $i \equiv 0 \mod p$.

On the other hand, if the function $\theta : R \to U$ satisfies properties (1) and (2), then we must show it is a normal L-reduced derivation. Since all subgroups $L \leq U$ are R-stable by our comment above, by Proposition 3.4 we need only check that equation (1) holds.

Let $y^a, y^b \in R$ for some $a, b = 0, 1, \ldots, p-1$ with $\theta(y^a) = l_a x^{t_a}$ and $\theta(y^b) = l_b x^{t_b}$ for some $l_a, l_b \in L$. Then

$$\begin{aligned}
\theta(y^a)\theta(y^b)^{y^a} &= l_a x^{t_a}(l_b x^{t_b})^{y^a} \\
&= l_a x^{t_a} l_b^{y^a} (x^{t_b})^{y^a} \\
&= l_a x^{t_a} l_c (x^{t_b})^{y^a}, \text{ for some } l_c \in L \\
&= l_d x^{t_a} (x^{t_b})^{y^a}, \text{ for some } l_d \in L \\
&= l_d x^{t_a + \alpha^a t_b} \\
&= l_d x^{i(1+\alpha+\cdots+\alpha^{a-1}) + i\alpha^a(1+\alpha+\cdots+\alpha^{b-1})} \\
&= l_d x^{i(1+\alpha+\cdots+\alpha^{a+b-1})} \\
&= l_d x^{t_{a+b}}.
\end{aligned}$$

Hence $\theta(y^{a+b}) = \lambda\theta(y^a)\theta(y^b)^{y^a}$ for some $\lambda \in L$. □

By Theorem 2.3, we know that any two NLR derivations whose images are equivalent mod L give rise to the same fiber-product. By Proposition 4.1, when $R = \langle y \rangle$ an NLR derivation must satisfy $\theta(y^k) \in Lx^{t_k}$, so we will choose to consider only those functions $\theta_i : R \to U$ satisfying $\theta_i(e) = e$ and $\theta_i(y^k) = x^{t_k}$ for all $k = 1, 2, \ldots, p$ (in particular, $\theta_i(y) = y^i$).

Now we can find the subgroups of P from NLR triples, when $R = \langle y \rangle$.

- If $L = \{e\}$ then we know from above that $\theta_i : R \to U$ defined by $\theta_i(y^k) = x^{t_k}$ is in $\mathrm{NDer}_L(R, U)$ if and only if $i = 0, p, 2p, \ldots, p(p-1)$. We get the following subgroups of P:
  - When $i = 0$, $\theta_0 = 1$ and $L \bowtie^{\theta_0} R = R = \langle y \rangle \cong \mathbb{Z}_p$.
  - When $i = p$,
  $$\begin{aligned} L \bowtie^{\theta_p} R &= \{(e,e), (x^p, y), (x^{2p}, y^2), \ldots, (x^{p(p-1)}, y^{p-1})\} \\ &= \langle x^p y \rangle \cong \mathbb{Z}_p. \end{aligned}$$
  - When $i = 2p$,
  $$\begin{aligned} L \bowtie^{\theta_{2p}} R &= \{(e,e), (x^{2p}, y), (x^{4p}, y^2), \ldots, (x^{2p(p-1)}, y^{p-1}\} \\ &= \langle x^{2p} y \rangle \cong \mathbb{Z}_p. \end{aligned}$$

  $\vdots$
  - When $i = p(p-1)$,
  $$\begin{aligned} L \bowtie^{\theta_{p(p-1)}} R &= \{(e,e), (x^{p(p-1)}, y), \ldots, (x^{p^2(p-1)^2}, y^{p-1})\} \\ &= \langle x^{p(p-1)} y \rangle \cong \mathbb{Z}_p. \end{aligned}$$

  Thus, when $L = \{e\}$ and $R = \langle y \rangle$, we get p subgroups isomorphic to $\mathbb{Z}_p$.

- If $L = \langle x^p \rangle$ then θ_i is in $\mathrm{NDer}_L(R, U)$ for all $i = 0, 1, \ldots, p^2 - 1$. In this case,

  $$L \bowtie^{\theta_i} R = L \bowtie^{\theta_j} R$$

  whenever $i \equiv j \mod p$, so we need only consider $\theta_i(y) = x^i$ for $i = 0, 1, \ldots, p-1$. Furthermore, since $\alpha^j \equiv 1 \mod p$ for all j we have $t_k \equiv ik \mod p$. Thus $x^{t_k} \in Lx^{ik}$ so we may assume $\theta_i(y^k) = x^{ik}$.

  - When $i = 0$, θ_0 is the trivial function and by Theorem 3.6 the corresponding fiber-product is

    $$L \bowtie^{\theta_0} R = L \rtimes R = L \times R = \langle x^p, y \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

  - When $i = 1$, we may assume $\theta_1(y^k) = x^k$ and we get

    $$\begin{aligned}
    \{(l\theta_1(e), e) \,|\, l \in L\} &= \{(e,e), (x^p, e), \ldots, (x^{(p-1)p}, e)\},\\
    \{(l\theta_1(y), y) \,|\, l \in L\} &= \{(x,y), (x^{p+1}, y), \ldots, (x^{(p-1)p+1}, y)\},\\
    \{(l\theta_1(y^2), y^2) \,|\, l \in L\} &= \{(x^2,y^2), (x^{p+2}, y^2), \ldots, (x^{(p-1)p+2}, y^2)\},\\
    &\vdots\\
    \{(l\theta_1(y^{p-1}), y^{p-1}) \,|\, l \in L\} &= \{(x^{p-1},y^{p-1}), \ldots, (x^{(p-1)p+p-1}, y^2)\}.
    \end{aligned}$$

    Hence,

    $$L \bowtie^{\theta_1} R = \langle xy \rangle \cong \mathbb{Z}_{p^2}.$$

  - When $i = 2$, we may assume $\theta_2(y^k) = x^{2k}$ and we get

    $$\begin{aligned}
    \{(l\theta_2(e), e) \,|\, l \in L\} &= \{(e,e), (x^p, e), \ldots, (x^{(p-1)p}, e)\},\\
    \{(l\theta_2(y), y) \,|\, l \in L\} &= \{(x^2,y), (x^{p+2}, y), \ldots, (x^{(p-1)p+2}, y)\},\\
    \{(l\theta_2(y^2), y^2) \,|\, l \in L\} &= \{(x^4,y^2), (x^{p+4}, y^2), \ldots, (x^{(p-1)p+4}, y^2)\},\\
    &\vdots\\
    \{(l\theta_2(y^{p-1}), y^{p-1}) \,|\, l \in L\} &= \{(x^{2p-2},y^{p-1}), (x^{3p-2}, y^2), \ldots, (x^{p-2}, y^2)\},
    \end{aligned}$$

    Hence,

    $$L \bowtie^{\theta_2} R = \langle x^2 y \rangle \cong \mathbb{Z}_{p^2}.$$

  - Continuing in this manner, letting $\theta_i(y^k) = x^{ik}$ for $i = 3, 4, \ldots, p-1$, we end up with more subgroups of the form

    $$L \bowtie^{\theta_i} R = \langle x^i y \rangle \cong \mathbb{Z}_{p^2}.$$

  Thus, when $L = \langle x^p \rangle$ and $R = \langle y \rangle$, we get $p - 1$ subgroups isomorphic to $\mathbb{Z}_{p^2}$ and one isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

- If $L = \langle x \rangle$ then θ_i is in $\mathrm{NDer}_L(R, U)$ for all $i = 0, 1, \ldots, p^2 - 1$. Since the image of every θ_i is in L, we can take $\theta_0 = 1$ as representative of all of them. In this case,
$$L \bowtie^1 R = U \rtimes H = P.$$

Putting all the information together, we see that P has $2p + 4$ subgroups:

- $\{e\}$;
- $\{\langle x^p \rangle, \langle y \rangle, \langle x^p y \rangle, \langle x^{2p} y \rangle, \ldots, \langle x^{(p-1)p} y \rangle\}$, each isomorphic to $\mathbb{Z}_p$;
- $\{\langle x \rangle, \langle xy \rangle, \langle x^2 y \rangle, \ldots, \langle x^{p-1} y \rangle\}$, each isomorphic to $\mathbb{Z}_{p^2}$;
- $\langle x^p, y \rangle$, isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$; and
- P.

Moreover, instead of testing p^2 functions $R \to U$ when $R = \{e\}$ and $(p^2)^{p-1}$ when $R = \langle y \rangle$, we considered only $2p + 2$ different normal L-reduced derivations in total.

5. Conclusion

We can find subgroups of $G = U \rtimes H$ by considering products MS where $S \leq H$ and M is an S-invariant subgroup of U, but we will only find subgroups of G in this manner up to isomorphism type. Indeed, in the example in Section 4, the MS construction would yield the 5 distinct isomorphism types of subgroups of P, but not all $2p + 4$ distinct subgroups. We need normal L-reduced derivations to determine subgroups of G precisely. *A priori*, there are many functions that might turn out to be in $\mathrm{NDer}_L(R, U)$ given $L \leq U$ and $R \leq H$, but we have shown how to substantially reduce the number of computations needed to find all the subgroups of $U \rtimes H$.

One can say quite a bit more about subgroups of $U \rtimes H$ when U and H are both cyclic. More generally, the NLR derivation idea may help to determine conjugacy classes of subgroups of a semi-direct product. These are both good areas for further lines of research.

6. Acknowledgments

We would like to thank the referees for a careful reading of the paper and several helpful suggestions.

References

[1] E. Goursat, Sur les substitutions orthogonales et les divisions regulieres de l'espace, *Ann. Sci. Ecole Norm. Sup.*, **6** (1889) 9-102.

[2] H. Heineken, review of "Die Untergruppen von halbdirekten Produkten" by K. Rosenbaum, *Mathematical Reviews*, MR0991728 (90c:20032).

[3] K. Rosenbaum, Die Untergruppen von halbdirekten Produkten, *Rostock. Math. Kolloq.*, **35** (1988) 21-30.

[4] V.M. Usenko, Subgroups of semi direct products, *Ukranian Math. J.*, **43** (1991) 982-988.

Student biographies

Akina Khan: (*Corresponding author:* akina.khan@mitchellhamline.edu) Akina graduated from St. Olaf College in May 2016 with a B.A. in mathematics and philosophy. Currently she is pursuing a J.D. at Mitchell Hamline School of Law (St. Paul, Minnesota), but still enjoys math on a recreational level.

Asa Giannini: Asa graduated from St. Olaf College in May 2016 with a B.A. in mathematics. He is currently pursuing a degree in graphics design at the University of Wisconsin–Stout.

Michael Schroeder Michael graduated from St. Olaf College in May 2016 with a B.A. in mathematics and chemistry. He is currently in medical school at the Sanford School of Medicine in South Dakota.