Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume **23** (2017). Number 2, pp. 204–215

Nonuniqueness of semidirect decompositions for semidirect products with directly decomposable factors and applications for dihedral groups

Peteris Daugulis

Communicated by I. Ya. Subbotin

Abstract. Nonuniqueness of semidirect decompositions of groups is an insufficiently studied question in contrast to direct decompositions. We obtain some results about semidirect decompositions for semidirect products with factors which are nontrivial direct products. We deal with a special case of semidirect product when the twisting homomorphism acts diagonally on a direct product, as well as with the case when the extending group is a direct product. We give applications of these results in the case of generalized dihedral groups and classic dihedral groups D_{2n}. For D_{2n} we give a complete description of semidirect decompositions and values of minimal permutation degrees.

1. Introduction

1.1. Background

The aim of this article is to study semidirect decompositions of groups both in general and special cases.

By the Krull-Remak-Schmidt theorem the multiset of isomorphism types of indecomposable direct factors for groups satisfying ascending

2010 MSC: 20E22, 20D40.

Key words and phrases: semidirect product, direct product, diagonal action, generalized dihedral group.

and descending chain conditions on normal subgroups does not depend on the order of factors. Thus direct decompositions of such groups, e.g. finite groups, may be considered understood.

Few results of this type are known for semidirect and Zappa-Szep decompositions. One can mention the Schur-Zassenhaus theorem as an example.

We consider cases when the base group or the extending group is a direct product. We present a general result which allows to characterize some semidirect decompositions in the case when the base group is a direct product and the twisting homomorphism acts diagonally, Proposition 1. We obtain a nonuniqueness result of semidirect decomposition in the case when the extending group is a direct product, Proposition 2. We give applications of some of these results in the case of finite dihedral groups, both classic and generalized.

We use traditional multiplicative notation for general groups and additive notation for abelian groups. In this article the dihedral group of order $m = 2n$ is denoted by D_m: $D_m = \langle a, x | a^n = e, x^2 = e, xax = a^{-1}\rangle$. For any $m|n$ we usually identify $\mathbb{Z}_m$ with the corresponding subgroup of $\mathbb{Z}_n$. Q_m denotes the dicyclic group of order $m = 4k$: $Q_m = \langle a, x | a^{2k} = e, x^2 = a^k, x^{-1}ax = a^{-1}\rangle$.

The cyclic group of order m is denoted by $\mathbb{Z}_m$, in additive notation we assume that $\mathbb{Z}_m = \langle 1\rangle$. In this article we identify elements of $\mathbb{Z}_m$ and corresponding minimal nonnegative integers. We use this identification for powers of group elements. For example, if $r \in \mathbb{Z}_3$ and $r \equiv 2 (\mathrm{mod}\ 3)$, then $a^r = a^2$ for any group element a.

1.2. Basic facts about semidirect products

We remind the reader that an external semidirect product of groups N (*base group*) and H (*extending group*) is the group $N \rtimes_\varphi H = (N \times H, \cdot)$ where the group product is defined on the Cartesian product $N \times H$ using a group homomorphism (*twisting homomorphism*) $\varphi \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ as follows: $(n_1, h_1) \cdot (n_2, h_2) = (n_1\varphi(h_1)(n_2), h_1h_2)$. Sets $\widetilde{N} = N \times \{e_H\}$ and $\widetilde{H} = \{e_N\} \times H$ are subgroups in $N \times H$.

A group G is an internal semidirect product of its subgroups N and H if N is a normal subgroup, $G = NH$ and $N \cap H = \{e\}$. If a group G is finite then for G to be an internal semidirect product $N \rtimes H$ is equivalent to 1) N being normal in G, 2) $|N| \cdot |H| = |G|$ and 3) $N \cap H = \{e\}$. In the internal case the twisting homomorphism $H \to \mathrm{Aut}(N)$ is given by the map $h \mapsto (n \to hnh^{-1})$, for any $n \in N$, $h \in H$.

Both expressions will be called semidirect decompositions of G. If the twisting homomorphism is not discussed, we omit it and use the notation $\rtimes$. We consider direct product to be a special case of semidirect product with the twisting homomorphism being trivial. For relevant treatment see [5], [6].

A nontrivial semidirect product may admit more than one semidirect decomposition. Examples are abundant starting from groups of order 8.

Example 1. Twisting homomorphisms are not given in these examples.

$$D_8 \simeq \mathbb{Z}_4 \rtimes \mathbb{Z}_2 \simeq \mathbb{Z}_2^2 \rtimes \mathbb{Z}_2, \qquad \Sigma_4 \simeq A_4 \rtimes \mathbb{Z}_2 \simeq \mathbb{Z}_2^2 \rtimes \Sigma_3.$$

There are semidirect products such that $\mathbb{Z}_3 \rtimes Q_8 \simeq Q_{24}$, but $Q_8 \rtimes \mathbb{Z}_3 \simeq SL(2, \mathbb{F}_3)$. On the other hand, there is a group G_{32} of order 32, such that $G_{32} \simeq D_8 \rtimes \mathbb{Z}_2^2 \simeq \mathbb{Z}_2^2 \rtimes D_8$.

Finally, there is a group G_{24} of order 24 which can be decomposed in 5 different ways:

$$G_{24} \simeq \mathbb{Z}_3 \rtimes D_8 \simeq \mathbb{Z}_2^2 \rtimes \mathbb{Z}_3 \simeq D_{12} \rtimes \mathbb{Z}_2 \simeq (\mathbb{Z}_3 \times \mathbb{Z}_2^2) \rtimes \mathbb{Z}_2 \simeq Q_{12} \rtimes \mathbb{Z}_2.$$

2. Main results

2.1. Diagonal semidirect products

Automorphisms of direct products. We introduce a linear algebra style notation for direct products of groups.

Let $G = G_1 \times G_2$. Encode the element (g_1, g_2) as a column $\left[\frac{g_1}{g_2}\right]$. If $\varphi \in \mathrm{Aut}(G)$, then

$$\varphi\left(\left[\frac{g_1}{g_2}\right]\right) = \left[\frac{\varphi_1(g_1, g_2)}{\varphi_2(g_1, g_2)}\right].$$

One can check, that for all relevant parameter values φ_i satisfy the following properties:

1) $\varphi_i(ab, e) = \varphi_i(a, e)\varphi_i(b, e)$,
2) $\varphi_i(e, ab) = \varphi_i(e, a)\varphi_i(e, b)$,
3) $\varphi_i(a, b) = \varphi_i(a, e)\varphi_i(e, b) = \varphi_i(e, b)\varphi_i(a, e)$,

Define $\varphi_{11}(g_1) = \varphi_1(g_1, e)$, $\varphi_{12}(g_2) = \varphi_1(e, g_2)$, $\varphi_{21}(g_1) = \varphi_2(g_1, e)$, $\varphi_{22}(g_2) = \varphi_2(e, g_2)$, for all $g_i \in G_i$. All functions φ_{ij} are group homomorphisms. Thus $\varphi_i(g_1, g_2) = \varphi_i(g_1, e)\varphi_i(e, g_2) = \varphi_{i1}(g_1)\varphi_{i2}(g_2)$.

We can encode action of φ as follows:

$$\varphi\left(\left[\begin{array}{c} g_1 \\ \hline g_2 \end{array}\right]\right) = \left[\begin{array}{c|c} \varphi_{11}(g_1) & \varphi_{12}(g_2) \\ \hline \varphi_{21}(g_1) & \varphi_{22}(g_2) \end{array}\right].$$

Thus an automorphism $\varphi \in \mathrm{Aut}(G_1 \times G_2)$ is determined by 4 group homomorphisms $\varphi_{ij} : G_j \to G_i$.

Definition 1. We call $\varphi \in \mathrm{Aut}(G_1 \times G_2)$, $G_1 \neq \{e\}$, $G_2 \neq \{e\}$, a *diagonal automorphism* if φ_{12} and φ_{21} are trivial homomorphisms.

Definition 2. We call $(G_1 \times G_2) \rtimes_\varphi H$ a *diagonal semidirect product* if $\varphi(h)$ is a diagonal $G_1 \times G_2$-automorphism for any $h \in H$. Explicitly, there are group homomorphisms $\varphi_{ii}(h) : G_i \to G_i$ such that $\varphi(h)(g_1, g_2) = (\varphi_{11}(h)(g_1), \varphi_{22}(h)(g_2))$.

Remark 1. Note that G_i may not be indecomposable as direct factors. Described encodings and diagonal semidirect products can be generalized to cases when the base groups splits into an arbitrary finite number of direct factors. Similar encodings can be used considering internal semidirect products.

Semidirect decompositions of diagonal semidirect products. We present a proposition showing nonuniqueness of semidirect decomposition for diagonal semidirect products. Vaguely speaking, any direct factor of the base group which is invariant with respect to the initial twisting homomorphism can be moved to the extending group (nonnormal semidirect factor) to enlarge it. The new twisting homomorphism is such that the moved direct factor acts trivially on the remaining part of the base group.

Proposition 1. *Let N_1, N_2, H be groups. Let $G = (N_1 \times N_2) \rtimes_\varphi H$ be a diagonal semidirect product, $\varphi(h)(g_1, g_2) = (\varphi_{11}(h)(g_1), \varphi_{22}(h)(g_2))$. Then the following statements hold.*

1. $G \simeq N_1 \rtimes_{\Phi_{11}} (\underbrace{N_2 \rtimes_{\varphi_{22}} H})$, *for some* $\Phi_{11} \in \mathrm{Hom}(N_2 \rtimes_{\varphi_{22}} H, \mathrm{Aut}(N_1))$.
2. $\mathrm{Ker}(\Phi_{11}) = \widetilde{N_2}\mathrm{Ker}(\varphi_{11})$.
3. *If* $\varphi_{11}(h) = id_{N_1}$, *for any* $h \in H$, *i.e.*

$$\varphi(h)\left(\left[\begin{array}{c} g_1 \\ \hline g_2 \end{array}\right]\right) = \left[\begin{array}{c|c} g_1 & e \\ \hline e & \varphi_{22}(h)(g_2) \end{array}\right],$$

then $G \simeq N_1 \times (N_2 \rtimes_{\varphi_{22}} H)$.

Proof. 1. Consider $N_1 \rtimes_{\Phi_{11}} (N_2 \rtimes_{\varphi_{22}} H)$ where $\Phi_{11}(n_2, h) = \varphi_{11}(h)$. It is directly checked that $\Phi_{11} \in \mathrm{Hom}(N_2 \rtimes H, \mathrm{Aut}(N_1))$. We will prove that

$$(N_1 \times N_2) \rtimes_{\varphi} H \simeq N_1 \rtimes_{\Phi_{11}} (N_2 \rtimes_{\varphi_{22}} H).$$

Define a bijective map $f : (N_1 \times N_2) \rtimes_{\varphi} H \to N_1 \rtimes_{\Phi_{11}} (N_2 \rtimes_{\varphi_{22}} H)$ by $f((n_1, n_2), h) = (n_1, (n_2, h))$, for all $n_i \in N_i$, $h \in H$. We prove that f is a group homomorphism.

Let $a, a' \in N_1$, $b, b' \in N_2$, $h, h' \in H$. We have that

$$\begin{aligned}((a, b), h) \cdot ((a', b'), h') &= ((a, b)\varphi(h)(a', b'), hh')\\ &= ((a, b)(\varphi_{11}(h)(a'), \varphi_{22}(h)(b')), hh')\\ &= ((a\varphi_{11}(h)(a'), b\varphi_{22}(h)(b')), hh').\end{aligned}$$

On the other hand,

$$\begin{aligned}(a, (b, h)) \cdot (a', (b', h')) &= (a\Phi_{11}(b, h)(a'), (b, h) \cdot (b', h'))\\ &= (a\varphi_{11}(h)(a'), (b\varphi_{22}(h)(b'), hh')).\end{aligned}$$

We see that f is a group isomorphism.

2. $\mathrm{Ker}(\Phi_{11}) = \{(n_2, h) | h \in \mathrm{Ker}(\varphi_{11})\} = \widetilde{N_2}\widetilde{\mathrm{Ker}(\varphi_{11})}$.

3. In notations given above, $\varphi_{11}(h) = id_{N_1}$ implies $\Phi_{11}(n_2, h) = id_{N_1}$, for any $n_2 \in N_2$, $h \in H$. Thus it is the direct product. $\square$

Example 2. Let $G = (\mathbb{Z}_7 \times \mathbb{Z}_9) \rtimes_{\varphi} \mathbb{Z}_3$, where $\varphi(1)\left(\left[\begin{array}{c} g_1 \\ \hline g_2 \end{array}\right]\right) = \left[\begin{array}{c|c} g_1^2 & e \\ \hline e & g_2^4 \end{array}\right]$.

In additive notation this can be simplified as follows

$$\varphi(1)\left(\left[\begin{array}{c} g_1 \\ \hline g_2 \end{array}\right]\right) = \left[\begin{array}{c|c} 2g_1 & 0 \\ \hline 0 & 4g_2 \end{array}\right] = \left[\begin{array}{c|c} 2 & 0 \\ \hline 0 & 4 \end{array}\right] \left[\begin{array}{c} g_1 \\ \hline g_2 \end{array}\right].$$

G can be defined as the subgroup of Σ_{16} generated by three permutations:

a) $(1, \ldots, 7)$ (generating $\mathbb{Z}_7$),
b) $(8, \ldots, 16)$ (generating $\mathbb{Z}_9$) and
c) $\underbrace{(1, 2, 4)(3, 6, 5)}_{\mathbb{Z}_7} \underbrace{(8, 11, 14)(9, 15, 12)}_{\mathbb{Z}_9}$
(generating action of $\mathbb{Z}_3$ on $\mathbb{Z}_7 \times \mathbb{Z}_9$).

We have that $G \simeq \mathbb{Z}_7 \rtimes (\mathbb{Z}_9 \rtimes_4 \mathbb{Z}_3) \simeq \mathbb{Z}_9 \rtimes (\mathbb{Z}_7 \rtimes_2 \mathbb{Z}_3)$.

2.2. Directly decomposable extending groups

We show that a direct factor of the extending group can be transferred to the base group.

Proposition 2. *Let N, H_1, H_2 be groups Then*

$$N \rtimes_\varphi (H_1 \times H_2) \simeq (N \rtimes_{\varphi_1} H_1) \rtimes_{\varphi_2} H_2,$$

where $\varphi_1(h_1)(n) = \varphi(h_1, e_{H_2})(n)$ and $\varphi_2(h_2)(n, h_1) = (\varphi(e_{H_1}, h_2)(n), h_1)$, for all $n \in N$, $h_i \in H_i$.

Proof. It is checked that φ_i are group homomorphisms.

We prove that the map $f : N \rtimes (H_1 \times H_2) \longrightarrow (N \rtimes H_1) \rtimes H_2$ given by $f(n, (h_1, h_2)) = ((n, h_1), h_2)$ is a group homomorphism.

Let $n, n' \in N$, $h_i, h_i' \in H_i$.

Consider the product $(n, (h_1, h_2)) \cdot (n', (h_1', h_2'))$ in $N \rtimes_\varphi (H_1 \times H_2)$:

$$(n, (h_1, h_2)) \cdot (n', (h_1', h_2')) = (n\varphi(h_1, h_2)(n'), (h_1h_1', h_2h_2')).$$

Consider the product $((n, h_1), h_2) \cdot ((n', h_1'), h_2')$ in $(N \rtimes H_1) \rtimes H_2$:

$$\begin{aligned} ((n, h_1), h_2) \cdot ((n', h_1'), h_2') &= (((n, h_1)\varphi_2(h_2)(n', h_1')), h_2h_2') \\ &= (((n, h_1)(\varphi(e, h_2)(n'), h_1')), h_2h_2') \\ &= ((n\varphi_1(h_1)(\varphi(e, h_2)(n')), h_1h_1'), h_2h_2') \\ &= ((n\varphi(h_1, h_2)(n'), h_1h_1'), h_2h_2'). \end{aligned}$$

We see that both products have equal corresponding components and thus f is a group isomorphism. □

Example 3. Let $G = \mathbb{Z}_7 \rtimes_\varphi (\mathbb{Z}_2 \times \mathbb{Z}_3)$ where $\varphi(x, y)(1) \equiv (-1)^x 2^y (\text{mod } 7)$. G can be defined as the subgroup of Σ_7 generated by three permutations:

a) $(1, \dots, 7)$ (generating $\mathbb{Z}_7$),

b) $(1, 6)(2, 5)(3, 4)$ (generating action of $\mathbb{Z}_2$ on $\mathbb{Z}_7$) and

c) $(1, 2, 4)(3, 6, 5)$ (generating action of $\mathbb{Z}_3$ on $\mathbb{Z}_7$).

Then $G \simeq D_{2\cdot 7} \rtimes \mathbb{Z}_3 \simeq (\mathbb{Z}_7 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$.

3. Applications

3.1. Generalized dihedral groups

We remind the reader that an external semidirect product $D(A) = A \rtimes_\varphi \mathbb{Z}_2$ is called *generalized dihedral group* provided 1) A is abelian and

2) $\varphi(1)(g) = -g$ for any $g \in A$, in additive notation. We can also denote $D(A)$ by $A \rtimes_{-1} \mathbb{Z}_2$.

Using the classification of finite abelian groups we can assume that $A = \bigoplus_{i=1}^{n} \mathbb{Z}_{m_i}$. We use linear algebra style encoding — we encode $(g_1, \dots, g_n) \in A$ as a column vector $\left[\begin{array}{c} g_1 \\ \hline \dots \\ \hline g_n \end{array}\right]$. Notations introduced in section 2.1 are modified for additive group notation. The action of the twisting homomorphism is given by scalar or matrix multiplication:

$$\varphi(1)\left(\left[\begin{array}{c} g_1 \\ \hline \dots \\ \hline g_n \end{array}\right]\right) = \left[\begin{array}{c|c|c} (-g_1) & 0 & 0 \\ \hline 0 & \dots & 0 \\ \hline 0 & 0 & (-g_n) \end{array}\right] = - \left[\begin{array}{c} g_1 \\ \hline \dots \\ \hline g_n \end{array}\right] = (-\mathbf{E}_n) \cdot \left[\begin{array}{c} g_1 \\ \hline \dots \\ \hline g_n \end{array}\right],$$

where $\mathbf{E}_n$ is the $n \times n$ identity matrix.

Remark 2. Generalized dihedral groups are diagonal semidirect products with an injective twisting homomorphism.

Proposition 3. *Let $A = \bigoplus_{i=1}^{n} \mathbb{Z}_{m_i}$, let $A = A_1 \oplus A_2$, where $A_1 = \bigoplus_{i=1}^{n_1} \mathbb{Z}_{m_i}$, $A_2 = \bigoplus_{i=n_1+1}^{n} \mathbb{Z}_{m_i}$. Then*

$$D(A) \simeq A_1 \rtimes (A_2 \rtimes_{-1} \mathbb{Z}_2) = A_1 \rtimes D(A_2) \simeq A_1 \rtimes D(A/A_1).$$

Proof. $D(A) = (A_1 \oplus A_2) \rtimes_{\varphi} \mathbb{Z}_2$, where $\varphi(1)(g) = -g$, for any $g \in A$. Thus $\varphi(g_1, g_2) = (-g_1, -g_2)$, for any $g_i \in G_i$. It follows that $D(A)$ is a diagonal semidirect product with respect to $A_1 \oplus A_2$ decomposition. According to Proposition 1 we have that $D(A) \simeq A_1 \rtimes_{\Phi_{11}} (A_2 \rtimes_{\varphi_{22}} \mathbb{Z}_2) = A_1 \rtimes D(A_2)$, where $\Phi_{11}(g_2, 1)(g_1) = \varphi_{11}(1)(g_1) = -g_1$. □

Example 4. Let $G = D(\mathbb{Z}_3 \oplus \mathbb{Z}_5)$. G can be defined as a subgroup of Σ_8 generated by permutations $(1, 2, 3)$, $(4, 5, 6, 7, 8)$ and $(1, 2)(4, 7)(5, 6)$. Then $G \simeq \mathbb{Z}_3 \rtimes D_{2 \cdot 5} \simeq \mathbb{Z}_5 \rtimes D_{2 \cdot 3}$.

3.2. Dihedral groups

Classic dihedral groups are special cases of generalized dihedral groups when the base group is a cyclic group. We give a complete description of semidirect decompositions of D_{2n} using both Proposition 1 and ad hoc computations.

We use a classical presentation of dihedral groups:

$$D_{2n} = \langle a, x | a^n = e, x^2 = e, xax = a^{n-1} \rangle = \langle a \rangle \cup \langle a \rangle x.$$

We note that $D_2 \simeq \mathbb{Z}_2$ and $D_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, in all other cases D_{2n} is nonabelian.

Subgroups. Let $n \in \mathbb{N}$, $n \geqslant 3$, $d \in \mathbb{N}$, $d|n$, $m = \frac{n}{d}$. It is known that D_{2n} has the following subgroups, see [2].

1. For each $m \in \mathbb{N}$ such that $m|n$ there is a subgroup

$$A_m = \langle a^{\frac{n}{m}} \rangle = \langle a^d \rangle = \{e, a^d, a^{2d}, \ldots, a^{(m-1)d}\} \simeq \mathbb{Z}_m.$$

$A_m \trianglelefteq D_{2n}$ for all m. The number of such subgroups is $d(n)$ (the number of natural n-divisors).

2. For each $m \in \mathbb{N}$ such that $m|n$ and each $r \in \mathbb{Z}_{\frac{n}{m}} = \mathbb{Z}_d$ there is a subgroup

$$B_{2m,r} = \langle a^{\frac{n}{m}}, a^r x \rangle = \langle a^d, a^r x \rangle = \langle A_m, A_m(a^r x) \rangle \simeq D_{2m}.$$

Note that $r \in \mathbb{Z}_{\frac{n}{m}}$ is identified with an integer as described in the introduction.

The number of such subgroups is $\sigma(n)$ (the sum of natural n-divisors).

If $2|n$ then $B_{n,r} \trianglelefteq D_{2n}$. In all other cases, if $1 < m < n$ then $B_{2m,r} \ntrianglelefteq D_{2n}$.

Classical decompositions. It known that $D_{2n} \simeq \mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$ where the twisting homomorphism is $\varphi(1)(g) = -g$. In internal terms, $D_{2n} = A_n \rtimes B_{2,r}$, for all $r \in \mathbb{Z}_n$. If $2|n$ and $4 \not| n$, then $D_{2n} \simeq D_n \times \mathbb{Z}_2$, or, in internal terms, $D_{2n} = B_{n,r} \times A_2$. where $r \in \mathbb{Z}_2$. Again, note that second indices of B-type subgroups can be interpreted as both integers and residues.

External semidirect decompositions of D_{2n}. Using Proposition 1 we get an exaustive description of external semidirect decompositions of D_{2n}.

Proposition 4. 1. *$D_{2n} \simeq \mathbb{Z}_m \rtimes_\varphi D_{\frac{2n}{m}}$, for any $m \in \mathbb{N}$, $m|n$, such that* $\mathrm{GCD}(m, \frac{n}{m}) = 1$. *$\varphi$ is defined as follows: if $D_{\frac{2n}{m}} = \langle a, x | a^{\frac{n}{m}} = e, x^2 = e, xax = a^{-1} \rangle$ then $\varphi(a)(1) = 1$ and $\varphi(x)(1) = -1$.*

2. *$D_{2n} \simeq D_n \rtimes_\varphi \mathbb{Z}_2$, if $n = 2^\alpha q$, $\alpha \in \mathbb{N}$. φ is defined as follows: if $D_n = \langle a, x | a^{\frac{n}{2}} = e, x^2 = e, xax = a^{-1} \rangle$ then $\varphi(1)(a) = a^{-1}$ and $\varphi(1)(x) = ax$.*

3. *If $2|n$ and $4 \not| n$ then*

$$D_{2n} \simeq D_n \times \mathbb{Z}_2.$$

4. *There are no other nontrivial external semidirect decompositions of D_{2n} in the following sense. If $D_{2n} \simeq X \rtimes Y$, $|X| > 1$, $|Y| > 1$, then there are two possibilities:*

a) $X = \mathbb{Z}_m$ *and* $Y = D_{\frac{2n}{m}}$, *where* $m|n$, $\mathrm{GCD}(m, \frac{n}{m}) = 1$ *or*
b) $X = D_n$ *and* $Y = \mathbb{Z}_2$, *if* $2|n$.

Proof. Statements 1, 2 and 3 are proved by exhibiting a suitable internal semidirect decomposition.

1. We use the primary decomposition theorem for cyclic groups: if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, then $\mathbb{Z}_n \simeq \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i^{\alpha_i}}$. The statement follows from Proposition 1. Note that $\mathrm{Ker}(\varphi) = \langle a \rangle$.

Alternatively, we prove the same statement using the information about D_{2n}-subgroups. We show that if $\mathrm{GCD}(m, \frac{n}{m}) = 1$ then $D_{2n} = A_m \rtimes B_{\frac{2n}{m},r}$.

We have that $A_m \trianglelefteq D_{2n}$ and $|A_m| \cdot |B_{\frac{2n}{m},r}| = 2n = |D_{2n}|$. $A_m \cap B_{\frac{2n}{m}} \leqslant \langle a^{\frac{n}{m}} \rangle$. Considering subgroups of $\langle a^{\frac{n}{m}} \rangle$ it follows that $A_m \cap B_{\frac{2n}{m}} = \{e\}$. Thus $D_{2n} = A_m \rtimes B_{\frac{2n}{m},r} \simeq \mathbb{Z}_m \rtimes_\varphi D_{\frac{2n}{m}}$. A direct computation shows that φ is as stated: $(a^m)a^d(a^{-m}) = a^d$, $(a^r x)a^d(a^r x) = a^{-d}$.

Note that if $2|n$ and $4 \not| n$ then $A_2 \cap B_{n,r} = \{e\}$, $r \in \mathbb{Z}_2$, hence $D_{2n} = A_2 \times B_{n,r} \simeq \mathbb{Z}_2 \times D_n$. In this case there are no nontrivial semidirect decompositions of type $\mathbb{Z}_2 \rtimes D_n$.

2. This case is not covered by Proposition 1, we show directly that $D_{2n} = B_{n,0} \rtimes B_{2,1}$.

If $2|n$, then $B_{n,0} \trianglelefteq D_{2n}$. $|B_{n,0}| \cdot |B_{2,1}| = |D_{2n}|$. It can be checked that $B_{n,0} \cap B_{2,1} = \{e\}$: $B_{n,0} = \langle a^2, x \rangle$, $B_{2,1} = \langle ax \rangle$.

Thus $D_{2n} \simeq D_n \rtimes \mathbb{Z}_2$. A direct computation shows that φ is as stated: $(ax)a^2\ (ax) = a^{-2}$ (the generator a^2 gets inverted), $(ax)x(ax) = a^2 x$ (the generator x gets multiplied by the other generator a^2).

3. Using Proposition 1 we see that $D_{2n} = D(\mathbb{Z}_n) = (\mathbb{Z}_2 \oplus \ldots) \rtimes \mathbb{Z}_2 \simeq \mathbb{Z}_2 \times D(\mathbb{Z}_n/\mathbb{Z}_2) \simeq \mathbb{Z}_2 \times D_n$.

It can also be proved using the list of subgroups. We remind that $D_{2n} = B_{n,0} \times A_2 \simeq D_n \times \mathbb{Z}_2$ for the following reasons. Both subgroups are normal. $|B_{n,0}| \cdot |A_2| = |D_{2n}|$. $B_{n,0} = \langle a^2, x \rangle$, $A_2 = \langle a^{\frac{n}{2}} \rangle$, $\frac{n}{2}$ is odd, therefore $B_{n,0} \cap A_2 = \{e\}$.

4. Consider all possible internal semidirect decompositions of D_{2n}.

If $D_{2n} = X \rtimes Y$ then X must be a normal subgroup of D_{2n} therefore X must be A_m or $B_{n,r}$ with $2|n$.

If $X = A_m$ then Y must be $B_{m',r}$ ir order to generate D_{2n}, with $m' = \frac{2n}{m}$. $A_m \cap B_{\frac{2n}{m},r} = \{e\}$ iff $\mathrm{GCD}(n, \frac{n}{m}) = 1$.

Let $X = B_{n,r}$ with $2|n$, $r \in \mathbb{Z}_2$. There are $n + 1$ subgroups of D_{2n} having order 2: $B_{2,r}$, $r \in \mathbb{Z}_n$ and $A_2 = \langle a^{\frac{n}{2}} \rangle$. For any n such that $2|n$

this gives a semidirect decomposition of type $D_n \rtimes \mathbb{Z}_2$. If $4 \not| n$ then $A_2 \cap B_{n,r} = \{e\}$ which gives a direct decomposition $D_n \times \mathbb{Z}_2$. $\square$

Remark 3. In terms of prime factorization the condition $\mathrm{GCD}(m, \frac{n}{m}) = 1$ is equivalent to the fact that m and $\frac{n}{m}$ are products of full prime powers of the prime factorization of n. Existence of many members of this family also follows from Schur-Zassenhaus theorem. If $m|n$ and $\mathrm{GCD}(m, \frac{n}{m}) = 1$ then $\mathrm{GCD}(|A_m|, |D_{2n}/A_m|) = 1$, $D_{2n}/A_m \simeq D_{\frac{2n}{m}}$ and, hence $D_{2n} \simeq A_m \rtimes D_{\frac{2n}{m}}$.

Remark 4. Note that there are at most 2 external semidirect decompositions when n is a prime power:

1) if $n = p^\alpha$, p an odd prime, then there is only one (classical) external semidirect decomposition: $D_{2p^\alpha} \simeq \mathbb{Z}_{p^\alpha} \rtimes \mathbb{Z}_2$,
2) if $n = 2^\alpha$, $\alpha \geqslant 3$, then there are two external semidirect decompositions: $D_{2\cdot 2^\alpha} \simeq \mathbb{Z}_{2^\alpha} \rtimes \mathbb{Z}_2 \simeq D_{2^\alpha} \rtimes \mathbb{Z}_2$.

Remark 5. The image of the twisting homomorphism in each case of a proper semidirect product is isomorphic to $\mathbb{Z}_2$. If the extending group is not $\mathbb{Z}_2$, then the twisting homomorphism is not injective.

Example 5. External semidirect decompositions of $D_{2\cdot 30}$:

$$\begin{aligned} D_{60} &\simeq \mathbb{Z}_{30} \rtimes \mathbb{Z}_2 \simeq \mathbb{Z}_6 \rtimes D_{10} \simeq \mathbb{Z}_{10} \rtimes D_6 \simeq \mathbb{Z}_{15} \rtimes D_4 \\ &\simeq \mathbb{Z}_3 \rtimes D_{20} \simeq \mathbb{Z}_5 \rtimes D_{12} \simeq D_{30} \rtimes \mathbb{Z}_2 \simeq D_{30} \times \mathbb{Z}_2. \end{aligned}$$

Internal semidirect decompositions of D_{2n}. We now describe all internal semidirect decompositions of D_{2n}.

Proposition 5. *Let $n \in \mathbb{N}$.*

1. *If $m \in \mathbb{N}$, $m|n$, is such that* $\mathrm{GCD}(m, \frac{n}{m}) = 1$, *then*

$$D_{2n} = A_m \rtimes B_{\frac{2n}{m},r},$$

for all $r \in \mathbb{Z}_m$.

2. *If $n = 2^\alpha q$, $\alpha \in \mathbb{N}$, then*

$$D_{2n} = B_{n,0} \rtimes B_{2,r_1} = B_{n,1} \rtimes B_{2,r_0}$$

where $r_i \in \mathbb{Z}_n$, $r_i \equiv i (\mathrm{mod}\ 2)$.

3. *If $2|n$ and $4 \not| n$ then $D_{2n} = B_{n,0} \times A_2$ and $D_{2n} = B_{n,1} \times A_2$.*
4. *There are no other internal semidirect decompositions of D_{2n}.*

Proof. 1. We look for internal semidirect decompositions of D_{2n} in form $A_m \rtimes B_{m',r}$. We must have $m' = \frac{2n}{m}$ and $r \in \mathbb{Z}_m$. $A_m \cap B_{\frac{2n}{m},r} = \{e\}$ iff $\mathrm{GCD}(m, \frac{n}{m}) = 1$. Thus $D_{2n} = A_m \rtimes B_{\frac{2n}{m},r}$ for all m such that $\mathrm{GCD}(m, \frac{n}{m}) = 1$ and all $r \in \mathbb{Z}_m$ are the only possible decompositions of this kind.

2. We look for internal semidirect decompositions of D_{2n} in form $B_{m,r} \rtimes B_{m',r'}$. We must have $B_{m,r} \trianglelefteq D_{2n}$ therefore $2|n$, $m = n$ and $r \in \mathbb{Z}_2$, thus we have two possible decomposition series: $B_{n,0} \rtimes B_{2,r'}$ and $B_{n,1} \rtimes B_{2,r''}$. To ensure trivial intersections of semidirect factors we must have $r' \equiv 1 (\mathrm{mod}\ 2)$ and $r'' \equiv 0 (\mathrm{mod}\ 2)$.

3. If $2|n$ and $4 \nmid n$ then $B_{n,0} \cap A_2 = B_{n,1} \cap A_2 = \{e\}$ where all subgroups are normal.

4. It follows from the previous arguments. □

Permutation representations of dihedral groups. Finally we find minimal degrees of faithful permutation representations of D_{2n}. If n is not a prime power then these numbers are smaller than degrees of classical permutation representations of dihedral groups. This is a consequence of Proposition 4 and Karpilovsky bounds for finite abelian groups [4].

Let $\mu(G)$ be the minimal faithful permutation representation degree of G, i.e. the minimal $n \in \mathbb{N}$ such that there is an injective group homomorphism $G \to \Sigma_n$. It is known that for finite groups G, H and a group homomorphism $\varphi : H \to \mathrm{Aut}(G)$ we have that $\mu(G \rtimes_\varphi H) \leqslant |G| + \mu(H)$. If, additionally, φ is injective, then $\mu(G \rtimes_\varphi H) \leqslant |G|$.

Proposition 6. *Let $n = \prod_i p_i^{\alpha_i}$ be the prime factorization of $n \in \mathbb{N}$. Then $\mu(D_{2n}) = \sum_i p_i^{\alpha_i}$.*

Proof. First we prove that

$$\mu(D_{2n}) \leqslant \sum_i p_i^{\alpha_i}. \qquad (*)$$

By statement 1 of Proposition 4 we have that $D_{2n} \simeq \mathbb{Z}_{p_1^{\alpha_1}} \rtimes D_{2n_1}$, where $n_1 = \frac{n}{p_1^{\alpha_1}}$. Thus $\mu(D_{2n}) \leqslant p_1^{\alpha_1} + \mu(D_{2n_1})$. $(*)$ follows by induction in i using injectivity of the twisting homomorphism at the last step.

To prove the opposite inequality and the statement, we remind that $\mathbb{Z}_n \leqslant D_{2n}$. It implies $\mu(\mathbb{Z}_n) \leqslant \mu(D_{2n})$, therefore $\sum_i p_i^{\alpha_i} \leqslant \mu(D_{2n})$ by the Karpilovsky theorem for abelian groups [4]. □

Example 6. $\min_{n\in\mathbb{N}}\{n : \mu(D_{2n}) < n\} = 6$: $\mu(D_{2\cdot 6}) = 5$, $D_{2\cdot 6}$ can be generated by $(1,2,3)$, $(1,2)$, $(4,5)$. If, additionally, D_{2n} is directly indecomposable, then the minimum is 12: $\mu(D_{2\cdot 12}) = 7$, $D_{2\cdot 12}$ can be generated by $(1, 2, 3, 4)$, $(5, 6, 7)$, $(1, 3)(5, 6)$.

4. Conclusion

We have obtained results showing possibility of various semidirect decompositions of a given semidirect product in two cases: 1) if the original twisting homomorphism is diagonal and the base group is directly decomposable and 2) if the extending group is directly decomposable. These results may stimulate further interest in looking for analogues of Krull-Remak-Schmidt theorem type results for semidirect and Zappa-Szep products.

We have presented semidirect decompositions of generalized dihedral groups and classical dihedral groups as an application. Apart from semidirect decompositions guarranteed by the general proposition 4, for D_{2n} there are additional decompositions of external type $D_n \rtimes \mathbb{Z}_2$ if $2|n$.

Semidirect decompositions of dihedral groups give the exact value of $\mu(D_{2n})$.

Computations were performed using the computational algebra system MAGMA, see Bosma et al. [1].

References

[1] Bosma W, Cannon J, and Playoust C (1997), The Magma algebra system. I. The user language, J. Symbolic Comput., 24, pp. 235-265.

[2] Conrad K (2015) Dihedral groups II http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/dihedral2.pdf.

[3] Hillar C, Rhea D (2007) Automorphisms of finite abelian groups American Mathematical Monthly, 114, no.10, pp. 917-923.

[4] Karpilovsky G.I. (1970) The least degree of a faithful representation of abelian groups Vestnik Khar'kov Gos. Univ., 53:107-115.

[5] Robinson D (1996) A course in the theory of groups. Springer-Verlag, New York.

[6] Rotman J (1995) An introduction to the theory of groups. Springer-Verlag, New York.

Contact information

P. Daugulis Institute of Life Sciences and Technologies,
Daugavpils University,
Daugavpils, LV-5400, Latvia
E-Mail(s): peteris.daugulis@du.lv

Received by the editors: 08.05.2016
and in final form 16.08.2016.