Cyclic and dihedral constructions of even order

Aleš Drápal

Abstract. Let $G(\circ)$ and $G(*)$ be two groups of finite order n, and suppose that they share a normal subgroup S such that $u \circ v = u * v$ if $u \in S$ or $v \in S$. Cases when G/S is cyclic or dihedral and when $u \circ v \neq u * v$ for exactly $n^2/4$ pairs $(u, v) \in G \times G$ have been shown to be of crucial importance when studying pairs of 2-groups with the latter property. In such cases one can describe two general constructions how to get all possible $G(*)$ from a given $G = G(\circ)$. The constructions, denoted by $G[\alpha, h]$ and $G[\beta, \gamma, h]$, respectively, depend on a coset α (or two cosets β and γ) modulo S, and on an element $h \in S$ (certain additional properties must be satisfied as well). The purpose of the paper is to expose various aspects of these constructions, with a stress on conditions that allow to establish an isomorphism between G and $G[\alpha, h]$ (or $G[\beta, \gamma, h]$).

Keywords: cyclic construction, dihedral construction, quarter distance

Classification: Primary 20D60; Secondary 05B15

For groups $G(\circ)$ and $G(*)$ define $d(\circ, *)$ as the size of the set $\{(u, v) \in G \times G;\ u \circ v \neq u * v\}$. If G is of order n and n is a power of two, then $d(\circ, *) < n^2/4$ implies $G(\circ) \cong G(*)$, by [3]. The cases with $d(\circ, *) = n^2/4$ were studied in [2], [7], [6] and [4]. It has been observed in [4] that a relatively general assumption on the structure of the distance set $\{(u, v) \in G \times G;\ u \circ v \neq u * v\}$ implies the existence of $S \lhd G$ such that $G(\circ)/S \cong G(*)/S$ is cyclic or dihedral. In such cases the relation of $G(*)$ and $G(\circ)$ is so close that one can give a prescription how to construct all $G(*)$ given S and $G = G(\circ)$. These constructions are the subject of this paper.

The mathematics we use remains within elementary group theory. The main concept behind our work is an effort to interpret groups of certain order as a graph with edges corresponding to passages between those groups that exhibit a large amount of similarity, measured by the least possible distance computed over all situations, in which the groups share their underlying sets. At this point it is too early to decide, if this effort will end as a combinatorial curiosity, or will develop into a new effective tool of group theory (other constructions in addition to the cyclic and dihedral ones would probably had to exist in such a case). Nevertheless, experiments on small sets (see below) are encouraging and

Work supported by the institutional grant MSM 113200007 and by Grant Agency of Charles Univ., grant number 269/2001/B-MAT/MFF.

this paper was motivated by these experiments in the sense that the constructions very often yield a group isomorphic to the original group. Some theory explaining why this is happening seemed to be desirable.

The parameters of the cyclic construction are a normal subgroup $S \lhd G$, a generating coset $\alpha \in G/S$ and an element $h \in S \cap Z(G)$. The group $G(*)$ constructed from these parameters is denoted by $G[\alpha, h]$. We shall show that the possible isomorphism types of $G(*)$ do not depend on the choice of the generating coset α, and that $G[\alpha, h_1] \cong G[\alpha, h_2]$ when $h_1 h_2^{-1} = z^{2m}$ for some $z \in S \cap Z(G)$, $|G : S| = 2m$. (In fact, the isomorphism already follows from $h_1 h_2^{-1} = zz^w \dots z^{w^{2m-1}}$, where $w \in \alpha$ and $z \in Z(S)$.)

The parameters of the dihedral construction are a normal subgroup $S \lhd G$, generating cosets $\beta, \gamma \in G/S$ such that $\beta^2 = \gamma^2 = S$, and an element $h \in S$ that satisfies $hxh = x$ for all $x \in \beta \cup \gamma$. The group $G(*)$ is here denoted by $G[\beta, \gamma, h]$. We shall show that the possible isomorphism types of $G(*)$ do not depend on the choice of the generating cosets β and γ, and that $G[\beta, \gamma, h_1] \cong G[\beta, \gamma, h_2]$ when $h_1 h_2^{-1} = z^{2m}$ for some $z \in S$ with $zxz = x$ for all $x \in \beta \cup \gamma$, $|G : S| = 4m$. (The isomorphism already follows from $h_1 h_2^{-1} = zz^w \dots z^{w^{2m-1}}$, where $w \in \beta\gamma$, and where $z = pq$ for some $p, q \in S$ such that $pxp = x$ for all $x \in \beta$ and $qxq = x$ for all $x \in \gamma$.)

The cyclic group of order r will be denoted by C_r, and the dihedral group of order $2r$ will be denoted by D_{2r}. For the purposes of this paper we shall assume $r \geq 2$, thus regarding Klein's 4-group $C_2 \times C_2$ as the smallest dihedral group.

In our main statements we shall always assume $G/S \cong C_{2m}$ or $G/S \cong D_{4m}$, $m \geq 1$. The constructions can be also considered when $G/S \cong C_r$ or $G/S \cong D_{2r}$ for an odd $r \geq 3$, but then they behave somewhat differently. They yield $d(\circ, *) < n^2/4$ and seem to have no bearing on the distances of 2-groups, to which the results of this paper are directed. First steps towards understanding distances of 3-groups were taken in [5], and it is to be expected that the cyclic and dihedral constructions with r odd will receive more attention later.

The basic properties of the cyclic construction are developed in Section 2, and its structural properties mentioned above are proved in Section 3.

Section 4 describes the dihedral construction and discusses the maximum possible difference of the nilpotency degrees of G and $G[\beta, \gamma, h]$ when they are nilpotent (cf. Proposition 4.10). Section 5 gives an abstract characterization of the dihedral construction and Section 6 describes some of its structural properties (including those that were mentioned earlier in this introduction).

In abstract group theory one investigates isomorphism types irrespective of their underlying sets. Hence the situation where two group operations are defined on the same set may seem to be of little relevance. However, this changes when one asks in which cases a group (up to an isomorphism) could have been obtained from another group by one of our constructions. We thus ask for which groups

G_1 and G_2 there exist groups $G \cong G_1$ and $G(*) \cong G_2$ such that $G(*)$ can be expressed as $G[\alpha, h]$ or $G[\beta, \gamma, h]$. The answers are in Theorems 2.10 and 5.3, which give, respectively, the abstract characterizations of the cyclic and the dihedral construction.

The groups G_1 and G_2 are called *C_{2m}-related*, if G_2 can be obtained in the sense above (i.e., up to an isomorphism) from G_1 by the cyclic construction where the common quotient is the cyclic group of order $2m$. Similarly, the groups G_1 and G_2 are said to be *D_{4m}-related* if G_2 can be obtained from G_1 by means of the dihedral construction. We also say that the groups G_1 and G_2 can be *placed at quarter distance* if they are finite of order n and there exist $G(\circ) \cong G_1$ and $G(*) \cong G_2$ with $d(\circ, *) = n^2/4$.

It is known that for $n \leq 32$, n a power of two, one can construct for any two groups G_1 and G_2 a sequence $H_1 = G_1, H_2, \ldots, H_k = G_2$ in such a way that H_i and H_{i+1} can be placed at quarter distance for all i, $1 \leq i < k$. For $n \geq 64$ this seems to remain an open problem. In the case $n = 64$ the cyclic and dihedral constructions yield two blocks. One contains six groups, and the other all remaining ones.

All presently known cases of groups that can be placed at quarter distance correspond either to the cyclic or to the dihedral construction. Moreover, there are reasons to believe that any other construction, if it exists, is an expansion of these constructions (as the dihedral construction is an expansion of the cyclic construction).

When computing the neighbourhood of a group G (say a 2-group) with respect to C_{2m}-relationship and D_{4m}-relationship, one can profit from knowing that certain choices of parameters do not bring anything new. We therefore wish to know when certain parameters yield a group isomorphic to the group obtained from other parameters. For example, when all choices for a given S have been considered, there is no need to consider the cases corresponding to $\varphi(S)$, $\varphi \in \operatorname{Aut} Q$. Suppose now that S is fixed. Then we can consider just one generating coset $\alpha \in G/S$ (see Proposition 3.10 and Corollary 3.11) and just one generating pair $\beta, \gamma \in G/S$ (cf. Theorem 6.10), respectively. We have already mentioned that for some choices of h the group obtained by the cyclic or dihedral construction is isomorphic to the original group. The elements h, for which the isomorphism will be proved, form a subgroup, say T, of the group of all possible choices of h. If two choices h_1 and h_2 are congruent modulo T, then the groups constructed are isomorphic (see Theorems 3.4 and 6.4). This follows from what is called here the *affine behaviour* (see Propositions 3.3 and 6.3) of the cyclic and dihedral constructions. This behaviour also implies that all groups which are C_{2m}-related (or D_{4m}-related) to G, with respect to a fixed subgroup S, are mutually C_{2m}-related (or D_{4m}-related, respectively).

The purpose of this paper therefore rests in a description of tools that can make easier the enumeration of all groups which are C_{2m}-related and D_{4m}-related to a given group. The paper is a generalization of [6], where only the case $m = 1$ was treated. Applications of results of this paper can be found in [1].

Section 1 contains various prerequisites for Sections 2–6.

When $*$ is used for a group operation, the inverse element is denoted by x^*.

1. Group properties

This section is of an auxiliary nature. It is concerned with those group properties which do not require the presence of two group operations, but which will turn to be relevant in such situations.

Lemma 1.1. *Let $A(+,-,0)$ be an abelian group, and suppose that $\alpha \in \mathrm{Aut}(A)$ is an automorphism of order r. If $\beta \in \langle\alpha\rangle$ is of order r as well, then $\alpha^0 + \alpha^1 + \dots + \alpha^{r-1} = \beta^0 + \beta^1 + \dots + \beta^{r-1}$.*

Proof: We have $\beta = \alpha^j$ for some j that is invertible modulo r. The set $\{0, 1, \dots, r-1\}$ coincides, modulo r, with the set $\{0j, 1j, \dots, (r-1)j\}$. $\square$

The additive notation of Lemma 1.1 is replaced from now on by multiplicative notation. This is necessary, since our abelian groups will occur as subgroups of a general group G.

Lemma 1.2. *Assume $S \trianglelefteq G$, $z \in Z(S)$, $x \in G$, $\langle S, x\rangle = G$ and $|G/S| = r$. Then $h = zz^x \dots z^{x^{r-1}} \in Z(G)$ and $(zx)^r = (xz)^r = x^r h$.*

Proof: Our first goal is to show that $h = zz^x \dots z^{x^{r-1}}$ commutes with x. We have $h^x = (z^x \dots z^{x^{r-1}}) \cdot z = z \cdot (z^x \dots z^{x^{r-1}}) = h$. To compute $(zx)^r$ and $(xz)^r$ express the i-th occurence of x when counted from the right as $x^i x^{-(i-1)}$ in both terms, $1 \le i \le r$. We obtain $(zx)^r = (zx^r)(z^{x^{r-1}} \dots z^x) = (x^r z)(z^{x^{r-1}} \dots z^x) = x^r h$ and $(xz)^r = x^r z^{x^{r-1}} \dots z^x z = x^r h$. $\square$

Proposition 1.3. *Suppose that G/S is cyclic of order r, $S \trianglelefteq G$. If $x, y \in G$ are such that $\langle S, x\rangle = \langle S, y\rangle = G$, then $zz^x \dots z^{x^{r-1}} = zz^y \dots z^{y^{r-1}}$ for all $z \in Z(S)$. The set of all elements that can be expressed in this way forms a subgroup of $Z(G)$, and this subgroup contains the group $\{z^r;\ z \in Z(G)\}$.*

Proof: The automorphisms $z \mapsto z^x$ and $z \mapsto z^y$ generate the same cyclic subgroup of $\mathrm{Aut}(Z(S))$. By Lemma 1.1 these automorphisms yield the same endomorphism of $Z(S)$, and the elements described in our statement correspond to the image of this endomorphism. They belong to $Z(G)$ by Lemma 1.2. Finally, observe that for $z \in Z(G)$ we have $z^x = z$ and $zz^x \dots z^{x^{r-1}} = z^r$. $\square$

Let G be a group. For $X \subseteq G$ put

$$Q(X) = \{h \in \langle X\rangle \setminus X;\quad hgh = g \ \text{ for all } \ g \in X\}.$$

Furthermore, for $X_1, X_2 \subseteq G$ put

$$Q(X_1, X_2) = Q(X_1 \setminus X_2) \cap Q(X_2 \setminus X_1).$$

These definitions are taken from [6]. In this paper the sets X_1 and X_2 will be always disjoint, and in such a case we have $Q(X_1, X_2) = Q(X_1) \cap Q(X_2)$. The next statement is also based on [6] (cf. Proposition 1.3 and Lemma 1.5), and we state it without a proof (which is not difficult).

Lemma 1.4. *Assume $T < G$ and $|G : T| = 2$. Then $Q(G \setminus T)$ is a subgroup of $Z(T)$, and $h \in Z(T)$ belongs to $Q(G \setminus T)$ if and only if $hgh = g$ for at least one (and thus for all) $g \in G \setminus T$. If $h \in Q(G \setminus T)$ and $g \in G \setminus T$, then $h^g = h^{-1}$ and $[g, h] = h^2$.*

Proposition 1.5. *Assume $S \lhd G$, where G/S is dihedral of order $2r$, $r \geq 2$. Suppose that the cosets β and γ generate G/S and that $\beta^2 = \gamma^2 = S$. Put $\alpha = \beta\gamma$ and denote by G_0 the subgroup of G that is generated by α. Then $S < G_0 < G$, $|G : G_0| = 2$ and*

$$Q(\beta, \gamma) = S \cap Q(G \setminus G_0).$$

Proof: The inclusion $S \cap Q(G \setminus G_0) \subseteq Q(\beta, \gamma)$ follows from $\beta \cup \gamma \subseteq G \setminus G_0$; to prove the converse consider $h \in Q(\beta, \gamma)$. If $u \in \beta$ and $v \in \gamma$, then $huv = huhh^{-1}vh^{-1}h = uvh$, and we see that h centralizes every element of α, and thus $h \in Z(G_0) \cap S$. If $x \in G \setminus G_0$, then $x = uy$ for some $u \in \beta$ and $y \in G_0$, and $hxh = huhh^{-1}yh = uy = x$. □

Lemma 1.6. *Let $S < G_0 < G$ be such that $S \lhd G$, G/S is dihedral of order $2r$ and G_0/S is cyclic of order r. Consider $\beta \in G/S$ and $p \in Q(\beta)$, and suppose that β does not intersect G_0. Suppose also that wS, where $w \in G_0$, generates G_0/S. Then $h = pp^w \dots p^{w^{r-1}}$ belongs to $Q(G \setminus G_0)$, and $pp^x \dots p^{x^{r-1}} = h$ for all $x \in G_0$ such that xS generates G/G_0.*

Proof: We have $p \in Z(S)$, by Lemma 1.4, and hence the definition of h does not depend on the choice of $w \in G_0$, $G_0 = \langle w, S \rangle$, by Proposition 1.3. We can assume $w = uv$, where $u \in \beta$. Put $\gamma = vS$ and note that β and γ satisfy the assumptions of Proposition 1.5. We have $h \in Z(S)$, since $p^x \in Z(S)$ for all $x \in G$, and hence we only need to show $h \in Q(\beta, \gamma)$. This is equivalent to proving $h^u = h^{-1}$ and $h^v = h^{-1}$.

We have $p^u = p^{-1}$, by Lemma 1.4, and $h = pp^{uv} \dots p^{(uv)^{r-1}}$. Hence $h^u = p^{-1}(p^{-1})^{vu} \dots (p^{-1})^{(vu)^{r-1}} = (pp^{vu} \dots p^{(vu)^{r-1}})^{-1}$, and this is equal to h^{-1}, since vuS generates G_0/S as well.

Now, v^2 and $(vu)^r$ belong to S, and hence $p^v = (p^v)^{(vu)^r} = ((p^{v^2})^u)^{(vu)^{r-1}} = (p^{-1})^{(vu)^{r-1}}$. We can express h^v as $p^v((p^u) \dots (p^u)^{(vu)^{r-2}})^{v^2}$, and this is equal to $(p^{-1})^{(vu)^{r-1}} \cdot (p^{-1} \dots (p^{-1})^{(vu)^{r-2}}) = ((p \dots p^{(vu)^{r-2}}) \cdot p^{(vu)^{r-1}})^{-1} = h^{-1}$. □

Proposition 1.7. *Suppose that G/S is dihedral of order $2r$, $S \lhd G$, and let $G_0 < G$ be such that $S < G_0$ and G_0/S is cyclic and of order $r \geq 2$. Let $\beta_1, \dots, \beta_r$ be all the cosets modulo S outside G_0, and put $Z = Q(\beta_1) \dots Q(\beta_r)$. Then $Z \leq Z(S)$, and if $\langle S, x\rangle = \langle S, y\rangle = G_0$, then $zz^x \dots z^{x^{r-1}} = zz^y \dots z^{y^{r-1}}$ for all $z \in Z$ and $x, y \in G_0$. The set of all such elements forms a subgroup of $S \cap Q(G \setminus G_0)$, and this subgroup contains the group $\{z^r;\, z \in S \cap Q(G \setminus G_0)\}$.*

Proof: We have $Q(\beta_i) \leq Z(S)$, $1 \leq i \leq r$, by Lemma 1.4, and hence $Z \leq Z(S)$. Consider $z = p_1 \dots p_r \in Z$, where $p_i \in Q(\beta_i)$, and put $h_i = p_i p_i^x \dots p_i^{x^{r-1}}$, $1 \leq i \leq r$, where xS generates G_0/S. From Lemma 1.6 we see that h_i does not depend on the choice of x and that h_i belongs to $Q(G \setminus G_0)$. Thus $zz^x \dots z^{x^{r-1}} = h_1 \dots h_r \in Q(G \setminus G_0)$ does not depend on the choice of x either. We are considering the image of Z by the endomorphism $z \mapsto zz^x \dots z^{x^{r-1}}$ of $Z(S)$, and we have observed that this image is a subgroup of $Q(G \setminus G_0)$. Finally, if $z \in S \cap Q(G \setminus G_0) = \bigcap(Q(\beta_i);\, 1 \leq i \leq r) \leq Z$, then $z \in Z(G_0)$, by Lemma 1.4, and hence $zz^x \dots z^{x^{r-1}} = z^r$ for every $x \in G_0$. $\square$

The subgroup of all $zz^x \dots z^{x^{r-1}}$ described in Proposition 1.7 can be perceived as an image of $Z \leq Z(S)$ by an endomorphism $z \mapsto zz^x \dots z^{x^{r-1}}$. The purpose of the next proposition is to show that this image does not change when the elements z are chosen from $Q(\beta_1)Q(\beta_2)$, where $\beta_2 = \beta_1 x$. The proposition assumes that r is even. It will be clear from its proof that in the case of odd order r one can choose z just from $Q(\beta_1)$.

Proposition 1.8. *Suppose that G/S is dihedral of order $4m$, $m \geq 1$, $S \lhd G$, and let $G_0 < G$ be such that $S < G_0$ and G_0/S is cyclic and of order $2m$. Let α generate G_0/S, choose $w \in \alpha$, and consider $\beta \in G/S$ that does not intersect G_0. Put $Z = Q(\beta)Q(\beta\alpha) \dots Q(\beta\alpha^{2m-1})$ and $T = \{zz^w \dots z^{w^{2m-1}};\, z \in Z\}$. Then $T = \{zz^w \dots z^{w^{2m-1}};\, z \in Q(\beta)Q(\beta\alpha)\}$.*

Proof: Consider $z = p_0 \dots p_{2m-1}$, where $p_i \in Q(\beta\alpha^i)$, $0 \leq i < 2m$. If $i = 2j$ is even, then $p_i = a_j^{w^j}$ for some $a_j \in Q(\beta)$, and if $i = 2j+1$ is odd, then $p_i = b_j^{w^j}$ for some $b_j \in Q(\beta\alpha)$. Put $z_1 = a_0 a_1^w \dots a_{m-1}^{w^{m-1}}$, $c_1 = a_0 a_1 \dots a_{m-1}$, $z_2 = b_0 b_1^w \dots b_{m-1}^{w^{m-1}}$, and $c_2 = b_0 b_1 \dots b_{m-1}$. Then $z = z_1 z_2$, $c_1 \in Q(\beta)$, $c_2 \in Q(\beta\alpha)$, and it suffices to prove $z_r z_r^w \dots z_r^{w^{2m-1}} = c_r c_r^w \dots c_r^{w^{2m-1}}$, for both values of $r \in \{1, 2\}$. We shall consider just the case $r = 1$, the other case is similar.

Put $h_j = a_j a_j^w \dots a_j^{w^{2m-1}}$, $0 \leq j < m$. Then $z_1 z_1^w \dots z_1^{w^{2m-1}}$ can be expressed as $h_0 h_1^w \dots h_{m-1}^{w^{2m-1}}$. However, $h_j \in Q(G \setminus G_0)$, by Lemma 1.6, and thus $h_j \in Z(G_0)$, by Lemma 1.4, for all j, $0 \leq j < m$. Therefore $z_1 z_1^w \dots z_1^{w^{2m-1}} = h_0 h_1 \dots h_{m-1} = c_1 c_1^w \dots c_1^{w^{2m-1}}$. $\square$

2. The cyclic construction

We shall now investigate the properties of a construction that appears in Theorem 6.8 of [4]. This construction will be called *cyclic*. From Section 4 on we shall also be investigating another construction from [4], and that will be called *dihedral*. The goal of [4] was to prove that both these constructions are obtained naturally from certain general assumptions on the relationship of n-element groups $G(\circ)$ and $G(*)$ with $d(\circ, *) = n^2/4$. However, that motivation is of no importance for our investigation here, and hence Theorem 6.8 mentioned above is the only result of [4] relevant to the cyclic construction that is needed in this paper. We start by restating it.

Theorem 2.1. *Assume $S \lhd G$, with G/S cyclic of an even order $2m$. Suppose that $\alpha \in G/S$ is a generator and that $h \in S \cap Z(G)$. Define an operation $*$ on G by*

$$x * y = \begin{cases} xyh, & \text{if } x \in \alpha^i \text{ and } y \in \alpha^j, \\ & \text{where } 1 \le i, j \le m \text{ and } i + j > m; \\ xyh^{-1}, & \text{if } x \in \alpha^{-i} \text{ and } y \in \alpha^{-j}, \\ & \text{where } 1 \le i, j < m \text{ and } i + j \ge m; \\ xy, & \text{in the other cases.} \end{cases}$$

Then $G(*)$ is a group.

The group $G(*)$ of Theorem 2.1 will be denoted by $G[\alpha, h]$. The case $|G : S| = 2$ was investigated already in [6], and in that paper the group $G[G \backslash S, h]$ was denoted by $G[S, h]$. If $m > 1$, then a choice of a generating coset of G/S is necessary to determine $G(*)$ completely, and hence some change in notation could not have been avoided.

Note that for every pair of integers (i, j) there exists $\varepsilon \in \{-1, 0, 1\}$ such that $x * y = xyh^\varepsilon$ for all $(x, y) \in (\alpha^i, \alpha^j)$. The operation $*$ is defined so that for all $i, j \in M = \{-m+1, \ldots, -1, 0, 1, \ldots, m\}$ the value of ε is equal to $\sigma(i+j)$, where $\sigma(k) = 0$ if $k \in M$, $\sigma(k) = 1$ if $k > m$ and $\sigma(k) = -1$ if $k \le -m$. We can thus write

$$x * y = xyh^{\sigma(i+j)}, \quad \text{where} \quad x \in \alpha^i, \ y \in \alpha^j \quad \text{and} \quad i, j \in M.$$

By writing $G(*) = G[\alpha, h]$ we implicitly assume that α is a coset of $S \lhd G$ that generates a cyclic group G/S of an even order. Unless otherwise stated, this order is assumed to be equal to $2m$, and we shall also use M and $\sigma : M \to \mathbb{Z}$ with the meaning defined above. Furthermore, with respect to h the notation $G(*) = G[\alpha, h]$ carries the assumption that h is an element of $Z(G) \cap S$.

To envisage the value of ε, where $h^\varepsilon = (xy)^{-1} \cdot (x * y)$, use a table with the bottom row and the rightmost column labelled by α, and with the remaining rows and columns labelled by α^i, $2 \le i \le 2m$, working from right to left and bottom to top. The top row and the leftmost column thus correspond to the neutral element $S = \alpha^{2m}$, and their neighbours correspond to α^{-1}. In this way we obtain a $2m \times 2m$ square table, and we shall consider its natural division into four $m \times m$ subsquares. The value $\varepsilon = 1$ corresponds to those cells in the bottom right subsquare that are on and over its right-left (i.e., northeast-southwest) diagonal, while $\varepsilon = -1$ corresponds to the cells under the right-left diagonal of the upper left subsquare. The other cells have $\varepsilon = 0$. Figure 1 depicts the table for $m = 4$ (with $+$ standing for 1 and $-$ for -1).

	S	α^7	α^6	α^5	α^4	α^3	α^2	α
S	0	0	0	0	0	0	0	0
α^7	0	0	0	$-$	0	0	0	0
α^6	0	0	$-$	$-$	0	0	0	0
α^5	0	$-$	$-$	$-$	0	0	0	0
α^4	0	0	0	0	$+$	$+$	$+$	$+$
α^3	0	0	0	0	$+$	$+$	$+$	0
α^2	0	0	0	0	$+$	$+$	0	0
α	0	0	0	0	$+$	0	0	0

Figure 1: Distribution of the powers of h in the cyclic construction

The operation $*$ determines both α and h uniquely. To see this observe that α^m is the only row with m occurences of $\varepsilon \neq 0$, and that α is the only row, for which the only occurence of $\varepsilon \neq 0$ takes place in the column indexed by α^m.

The table conveys the definition of $*$ in a clear way. It also seems to suggest that an exchange of α and α^{-1} might be useful, since rows and columns would become labelled in a natural order, and not in the reverse order induced by our choice of α. However, such an exchange would require the differentiation of the cases $m = 1$ and $m > 1$ in some formulas. For example, in $G(*)$ the $2m$-th power of $x \in \alpha$ always equals $x^{2m}h$, while for $x \in \alpha^{-1}$ it equals $x^{2m}h^{-1}$ if $m > 1$, and x^2h if $m = 1$.

Lemma 2.2. *Assume $G(*) = G[\alpha, h]$ and $xy \in S$, for some $x, y \in G$. If $x \notin \alpha^m$, then $x * y = xy$. If $x \in \alpha^m$, then $x * y = xyh$.*

Proof: Define $i, j \in M$ by $x \in \alpha^i$ and $y \in \alpha^j$. If $i \neq m$, then $j = -i$, and $i + j = 0 \in M$ implies $x * y = xy$. If $x, y \in \alpha^m$, then $x * y = xyh$, by the definition of $G(*)$. □

Corollary 2.3. *Assume $G(*) = G[\alpha, h]$ and consider $x \in G$. If $x \notin \alpha^m$, then $x^* = x^{-1}$. If $x \in \alpha^m$, then $x^* = x^{-1}h^{-1}$.*

The next statement expresses one of the main properties of $G[\alpha, h]$.

Theorem 2.4. *Assume $G(*) = G[\alpha, h]$. Then $x * y * x^* = xyx^{-1}$ and $x^* * y * x = x^{-1}yx$ for all $x, y \in G$.*

Proof: Let $x \in \alpha^i$ and $y \in \alpha^j$, where $i, j \in M$. Suppose first $i \neq m$. Then $x^* = x^{-1}$, by Corollary 2.3, and $-i \in M$. By definition, $x * y * x^{-1} = (xyh^{\sigma(i+j)}) * x^{-1} = xyx^{-1}h^{\sigma(i+j)+\sigma((i\oplus j)-i)}$, where $\oplus$ refers to addition in M modulo $2m$. We shall show $\sigma(i+j) + \sigma((i \oplus j) - i) = 0$. If $i + j = i \oplus j$, then both $i + j$ and $(i \oplus j) - j = i$ belong to M, and hence their σ values equal 0. If $i + j > m$, then $\sigma(i+j) = 1$, and $\sigma((i \oplus j) - i) = -1$ follows from $(i \oplus j) - i = ((i+j) - 2m) - i = j - 2m \leq m - 2m = -m$. Similarly, $i + j \leq -m$ induces opposite σ values, since $(i \oplus j) - i = (i + j) + 2m - i = j + 2m > -m + 2m = m$. Hence $x * y * x^* = xyx^{-1}$ for $x \notin \alpha^m$, and from $x^* = x^{-1}$ and $x = (x^{-1})^*$ we also get $x^* * y * x = x^{-1}yx$.

Suppose now $x \in \alpha^m$. Then $x^* = x^{-1}h^{-1}$, and we have to show $x * y * x^{-1} = xyx^{-1}h$ and $x^{-1} * y * x = x^{-1}yxh$, for all $y \in \alpha^j$, $j \in M$. It suffices to prove the former equality, as x^{-1} also falls into α^m. If $j \geq 1$, then $-m < j - m \leq 0$ and $(x * y) * x^{-1} = (xyh) * x^{-1} = xyhx^{-1}$, and if $j \leq 0$, then $1 \leq j + m \leq m$ and $(x * y) * x^{-1} = (xy) * x^{-1} = xyx^{-1}h$. □

Corollary 2.5. *Assume $G(*) = G[\alpha, h]$. Then $x * y * x^* * y^* = xyx^{-1}y^{-1}$ and $x^{-1}y^{-1}xy = x^* * y^* * x * y$, for all $x, y \in G$.*

Proof: If $y \notin \alpha^m$, then $y^* = y^{-1}$, by Corollary 2.3, and $x * y * x^* * y^* = (xyx^{-1}) * y^{-1}$, by Theorem 2.4. This is equal to $xyx^{-1}y^{-1}$ by Lemma 2.2. For $y \in \alpha^m$ we get $y^* = y^{-1}h^{-1}$ and $x * y * x^* * y^* = (xyx^{-1}) * (y^{-1}h^{-1}) = xyx^{-1}y^{-1}h^{-1}h = xyx^{-1}y^{-1}$. The computation of $x^* * y^* * x * y$ is done similarly. □

Proposition 2.6. *Assume $G(*) = G[\alpha, h]$. A (normal) subgroup H of $G(\cdot)$ is a (normal) subgroup of $G(*)$ if and only if $H \leq S$ or $h \in H$.*

Proof: From the definition of $G(*)$ we see that if $h \in H$ or $H \subseteq S$, then $H \subseteq G$ is a subgroup of $G(\cdot)$ if and only if it is a subgroup of $G(*)$. From Theorem 2.4 we see that this correspondence retains normality. If $H < G(\cdot)$ is a subgroup of $G(*)$ that is not contained in S, then HS/S is a nontrivial subgroup of G/S. Hence it is generated by some α^k, where k divides $2m$ and is less than $2m$. Thus $k \leq m$, and we can consider the greatest $r \geq 1$ such that $kr \leq m$. Choose $x \in H \cap \alpha^{rk}$ and $y \in H \cap \alpha^k$, and observe that $(k + 1)r > m$ implies $x * y = xyh$. However, that means $h \in H$, since both $x * y$ and xy are assumed to belong to H. □

If $G(*) = G[\alpha, h]$, then from the preceding two statements one easily derives the coincidence of the members of the lower and the upper central series.

Proposition 2.7. *Assume $G(*) = G[\alpha, h]$. Then $\gamma_i(G) = \gamma_i(G(*))$, for every $i \geq 1$, and $\vartheta_j(G) = \vartheta_j(G(*))$, for every $j \geq 0$.*

Proof: We shall use induction. We have $\gamma_1(G(*)) = G = \gamma_1(G(\cdot))$. If $\gamma_i(G) = \gamma_i(G(*))$, then the next member is generated in both operations by the same set of commutators, by Corollary 2.5. This set is included in S, since G/S is abelian, and hence in both operations it generates the same subgroup of S.

The operations $\cdot$ and $*$ share the unit element, and hence $\vartheta_0(G) = \vartheta_0(G(*))$. Assume $\vartheta_j(G) = \vartheta_j(G(*))$. The next member of the series can be defined just by means of the commutators, and hence in both operations we get the same subgroup. $\square$

Proposition 2.8. *For $r \in \{1,2\}$ assume $G_r = \langle S, u_r\rangle$, where $S < G_r$ is normal and of index $2m$, $m \geq 1$. Put $h = u_2^{2m}u_1^{-2m}$. If $s^{u_1} = s^{u_2}$ for all $s \in S$, then h is central in both G_1 and G_2, and $G_1(*) = G_1[u_1S, h]$ is isomorphic to G_2.*

Proof: The computation of $s^{u_2^{2m}}$ in G_2, $s \in S$, can be perceived as a result of $2m$ iterations of the automorphism $s \mapsto s^{u_2}$. Since u_1 gives the same automorphism of S, we get $s^{u_2^{2m}} = s^{u_1^{2m}}$, for all $s \in S$. The element h is defined as the product of $u_2^{2m} \in S$ and $u_1^{-2m} \in S$, and so $s^h = s$ for all $s \in S$. Since u_2^{2m} commutes with u_1, by $(u_2^{2m})^{u_1} = (u_2^{2m})^{u_2} = u_2^{2m}$, we also get $h^{u_1} = h$, and hence $h \in Z(G_1)$. Symmetry yields $h^{-1} \in Z(G_2)$. We have proved that h is central in both G_1 and G_2.

Define $\varphi : G_2 \to G_1$ by $\varphi(u_2^i s) = u_1^i s$ for all $s \in S$ and all $i \in M = \{-m+1, \dots, -1, 0, 1, \dots, m\}$. If $i \in M$ and $s \in S$, then $\varphi(su_2^i) = \varphi(u_2^i u_2^{-i} s u_2^i) = u_1^i \cdot (u_2^{-i} s u_2^i) = u_1^i \cdot (u_1^{-i} s u_1^i) = su_1^i$.

Define the group $G_1(*)$ by $x * y = \varphi(\varphi^{-1}(x)\varphi^{-1}(y))$. Clearly $G_1(*) \cong G_2$. Our goal is to verify that our definition of $*$ coincides with that of $G_1[u_1S, h]$. If $i, j \in M$ and $s, t \in S$, then our definition gives $(u_1^i s) * (tu_1^j) = \varphi(u_2^i st u_2^j) = \varphi(u_2^i st u_2^{-i} u_2^{j+i}) = u_1^i st u_1^{-i} \varphi(u_2^{j+i})$. Set $k = j+i$. We need to prove that $\varphi(u_2^k) = u_1^k h^{\sigma(k)}$, for every k, $-2m+2 \leq k \leq 2m$.

If $k \in M$, then $\sigma(k) = 0$ and $\varphi(u_2^k) = u_1^k$, by the definition of φ. If $k > m$, then $\sigma(k) = 1$, and $\varphi(u_2^k) = \varphi(u_2^{2m}u_2^{k-2m}) = u_2^{2m}u_1^{k-2m} = hu_1^{2m}u_1^{k-2m} = u_1^k h$. Similarly, if $k \leq -m$, then $\sigma(k) = -1$ and $\varphi(u_2^k) = \varphi(u_2^{k+2m}u_2^{-2m}) = u_1^{k+2m}u_2^{-2m} = u_1^{k+2m}u_1^{-2m}h^{-1} = u_1^k h^{-1}$. $\square$

Corollary 2.9. *For $r \in \{1,2\}$ assume $G_r = \langle S, u_r\rangle$, where $S < G_r$ is normal and of index $2m$, $m \geq 1$. Assume also $u_1^{2m} = u_2^{2m}$, and $s^{u_1} = s^{u_2}$, for all $s \in S$. Then there exists an isomorphism $\varphi : G_2 \cong G_1$ such that $\varphi(u_2^i s) = u_1^i s$ and $\varphi(su_2^i) = su_1^i$ for all $s \in S$ and $i \in \mathbb{Z}$.*

Proof: Consider $G_1(*)$ and φ from the proof of Proposition 2.8. We assume $h = 1$, and hence $G_1(*)$ does not differ from $G_1(\cdot)$. The assumption $u_2^{2m} = u_1^{2m}$ makes it possible to extend the formulas for φ from $i \in M$ to all $i \in \mathbb{Z}$. $\square$

Recall that the groups G_1 and G_2 are *C_{2m}-related*, $m \geq 1$, if there exist a group $G = G(\cdot)$, its subgroup $S \lhd G$, an element $h \in S \cap Z(G)$, and a coset $\alpha \in G/S$, such that $|G : S| = 2m$, α generates G/S, $G_1 \cong G(\cdot)$ and $G_2 \cong G(*) = G[\alpha, h]$.

Theorem 2.10. *The groups G_1 and G_2 are C_{2m}-related, $m \geq 1$, if and only if there exist groups $H_r \cong G_r$, their common subgroup $S \lhd H_i$, $|H_r : S| = 2m$, and elements $u_r \in H_i$, such that $u_r S$ generates H_r/S, $r \in \{1, 2\}$, and $s^{u_1} = s^{u_2}$ for all $s \in S$.*

Proof: If groups H_r and elements u_r satisfying the above conditions exist, then G_1 and G_2 are C_{2m}-related by Proposition 2.8. If $G_1 \cong G(\cdot)$ and $G_2 \cong G(*)$, where $G(*) = G[\alpha, h]$ and $|G : S| = 2m$, then we can put $H_1 = G(\cdot)$, $H_2 = G(*)$, and consider any $u_1 = u_2 \in \alpha$. The inner automorphisms coincide on S by Theorem 2.4. □

Proposition 2.11. *Assume $G(*) = G[\alpha, h]$. Then $G(\cdot)/\langle h\rangle \cong G(*)/\langle h\rangle$.*

Proof: The group $\langle h\rangle$ is a central subgroup (and thus a normal subgroup) of both $G(\cdot)$ and $G(*)$. The statement hence follows directly from the definition of $*$. □

Proposition 2.11 shows that the groups $G(\cdot)$ and $G(*)$ could be handled as central extensions of the same group by the same quotient. Each of these extensions can be represented by a factor system, and many of our results could be obtained alternatively by considering the difference of these two factor systems.

3. Isomorphisms of cyclic constructions

Lemma 3.1. *Assume $G(*) = G[\alpha, h]$, and consider $x \in \alpha$. Denote by x_i the i-th power $x * \cdots * x$, $i \geq 0$. If $0 \leq i \leq m$, then $x_i = x^i$. If $m < i \leq 2m$, then $x_i = x^i h$.*

Proof: We have $x_i \in \alpha^i$, and hence $x_i * x = x_i x$ whenever $0 \leq i \leq 2m$ and $i \neq m$. We also have $x_m * x = x_m x h$, and the rest is clear. □

The next statement describes the principal case, in which we can establish an isomorphism $G[\alpha, h] \cong G$ without resorting to a specific structural investigation of G.

Proposition 3.2. *Assume $G = \langle S, x\rangle$, where $S \lhd G$ and $|G : S| = 2m$. Consider $z \in Z(S)$, and put $h = z^{x^{2m-1}} \ldots z^x z$. Then there exists an isomorphism $\varphi :$ $G[xS, h] \cong G$ such that $\varphi(sx^i) = s(zx)^i$ for all $s \in S$ and $i \in \mathbb{Z}$.*

Proof: The element h belongs to $Z(G)$ by Lemma 1.2, and the inner automorphisms of $u_2 = x$ and $u_1 = zx$ coincide on S with respect to both group operations, by Theorem 2.4. Hence to apply Corollary 2.9 it suffices to show that $(zx)^{2m}$ equals $x^{2m}h$, since the latter element is equal to the $2m$-th power of x in $G(*)$, by Lemma 3.1. However, $(zx)^{2m} = x^{2m}h$ follows from Lemma 1.2. □

We shall now point to a property that can be described as the *affine behaviour* (of the cyclic construction). This behaviour will allow us to derive from Proposition 3.2 an isomorphism $G[\alpha, h_1] \cong G[\alpha, h_2]$ for all $h_1, h_2 \in S \cap Z(G)$ that are equivalent modulo $T = \{z^{x^{2m-1}} \ldots z^x z;\ z \in Z(S)\}$.

Proposition 3.3. *Assume $G_1 = G[\alpha, h_1]$ and $G_2 = G[\alpha, h_1h_2]$, where $h_1, h_2 \in S \cap Z(G)$. Then $G_2 = G_1[\alpha, h_2]$.*

Proof: Consider $x \in \alpha^i$ and $y \in \alpha^j$, where $i, j \in M$. The product of x and y in $G[\alpha, h_1h_2]$ is equal to $xy(h_1h_2)^{\sigma(i+j)} = xyh_1^{\sigma(i+j)}h_2^{\sigma(i+j)}$, while the product of x and y in $G_1[S, h_2]$ equals $x * y * h_2^{\sigma(i+j)} = (x * y)h_2^{\sigma(i+j)}$, where $*$ denotes the group operation of $G_1 = G[\alpha, h_1]$. We have $x * y = xyh_1^{\sigma(i+j)}$, and thus the products considered give the same result. □

Theorem 3.4. *Assume $S \lhd G$, $|G : S| = 2m$, and suppose that G/S is cyclic. For $x \in S$, $\langle S, x\rangle = G$, put $T = \{z^{x^{2m-1}} \dots z^x z;\ z \in Z(S)\}$. Then T is a subgroup of $S \cap Z(G)$. It does not depend on the choice of $x \in G$, $\langle S, x\rangle = G$, and contains $\{z^{2m};\ z \in S \cap Z(G)\}$. If α generates G/S, then $G[\alpha, h_1] \cong G[\alpha, h_2]$ whenever $h_1, h_2 \in S \cap Z(G)$ are equivalent modulo T. In particular, $G[\alpha, h] \cong G$ for every $h \in T$.*

Proof: The above properties of T are taken from Proposition 1.3. If $h_1 \equiv h_2 \bmod T$, then $G[\alpha, h_2] = G_1[\alpha, h]$, where $G_1 = G[\alpha, h_1]$ and $h = h_1^{-1}h_2 \in T$, by Proposition 3.3. From Theorem 2.4 we see that by defining T with respect to G_1 and G we get the same subgroup of S, and hence $G[\alpha, h_2] \cong G_1$ follows from Proposition 3.2. □

Corollary 3.5. *Assume $G(*) = G[\alpha, h]$. Then there exists $h' \in S \cap Z(G)$ such that every prime divisor of its order divides $2m$, and $G(*) \cong G[\alpha, h']$.*

Proof: Express h as a product of its powers, $h = h'h''$, in such a way that the order of h'' is coprime to $2m$. Then $h'' = z^{2m}$ for certain $z \in \langle h''\rangle \leq S \cap Z(G)$. □

The following two statements can be easily directly verified, and their proof is thus omitted. They are included here in order to make the list of available isomorphisms as large as possible.

Proposition 3.6. *Assume $G_2 = G_1[\alpha, h]$. Then $G_1 = G_2[\alpha, h^{-1}]$.*

Proposition 3.7. *Suppose $\varphi : G_1 \cong G_2$ and $G_1(*) = G_1[\alpha, h]$. Then φ also yields an isomorphism $G_1(*) \cong G_2(*)$, where $G_2(*) = G_2[\varphi(\alpha), \varphi(h)]$.*

We shall now show that the possible isomorphism types of $G[\alpha, h]$ depend only on the subgroup S, and not on the choice of the generating coset $\alpha \in G/S$. To this purpose we first record two easy lemmas.

Lemma 3.8. *Assume $G(*) = G[\alpha, h]$, and consider $x \in \alpha$ and $j \in M$. Then the j-th powers of x in $G(*)$ and in $G(\cdot)$ are the same.*

Proof: The equality follows from Lemma 3.1 immediately if $0 \leq j \leq m$. Assume $-1 \geq j \geq -m+1$, and denote by x_i the i-th power of x in $G(*)$. From Corollary 2.3 we get $(x_j)^* = x_{-j} = x^{-j} = (x^j)^{-1} = (x^j)^*$, and hence $x_j = x^j$. □

Lemma 3.9. *Assume $G(*) = G[\alpha, h]$, and consider $j \in M$ and $y \in \alpha^j$. Then the $2m$-th power of y in $G(*)$ is equal to $y^{2m}h^j$.*

Proof: Let us again use lower indices to denote the powers induced by $*$. If $y, y' \in \alpha^j$, then there exist $\varepsilon, \varepsilon' \in \mathbb{Z}$ such that $y_{2m} = y^{2m}h^{\varepsilon}$ and $y'_{2m} = (y')^{2m}h^{\varepsilon'}$. The indices ε and ε' have to coincide, as the powers of h in the definition of $*$ depend only on the incidence to the cosets of S. Hence we can assume $y = x^j$, for some $x \in \alpha$. Lemma 3.8 gives $x_j = x^j$, and from Lemma 3.1 we thus get $y_{2m} = x_{2mj} = (x_{2m})^j = (x^{2m}h)^j = (x^j)^{2m}h^j = y^{2m}h^j$. □

Proposition 3.10. *Assume $G(*) = G[\alpha^j, h]$, where α generates G/S, $|G : S| = 2m$, and $j \in M$ is coprime to $2m$. Consider $k \in M$ with $jk \equiv 1 \bmod 2m$. Then $G(*) \cong G[\alpha, h^k]$.*

Proof: We shall use Corollary 2.9 with respect to $G_2 = G(*)$, $G_1 = G[\alpha, h^k]$ and $u_2 = x = u_1$, where x is an element of α. The automorphisms of S that are induced by x are the same, by Theorem 2.4. From Lemma 3.1 we see that the $2m$-th power of x in G_1 equals $x^{2m}h^k$. Let us consider the $2m$-th power of x in G_2. We have $\alpha = (\alpha^j)^k$, and hence Lemma 3.9 implies that this power is also equal to $x^{2m}h^k$. □

Corollary 3.11. *Suppose that α generates G/S, $|G : S| = 2m$. If $H \cong G[\alpha', h]$, where α' is another generator of G/S, then there exists $h' \in S \cap Z(G)$ such that $H \cong G[\alpha, h']$.*

4. The dihedral construction

The dihedral construction refers to the situation when there exists $S \lhd G$ such that $G/S \cong D_{4m}$ is a dihedral group of order $4m$, $m \geq 1$.

Theorem 4.1. *Assume $S \lhd G$, with G/S dihedral of order $4m$, $m \geq 1$. Suppose that $G/S = \langle \beta, \gamma \rangle$, where β and γ are involutions in G/S, and let $h \in S$ be such that $hxh = x$ for all $x \in \beta \cup \gamma$. Put $\alpha = \beta\gamma$, and for each $(x, y) \in G \times G$ find $i, j \in \{-m+1, \dots, -1, 0, 1, \dots, m\}$ and $\varepsilon, \eta \in \{0, 1\}$ such that $x \in \beta^{\varepsilon}\alpha^i$ and $y \in \alpha^j\gamma^{\eta}$. Put $\xi = (-1)^{\eta}$, and define an operation $*$ on G by*

$$x * y = \begin{cases} xyh^{\xi}, & \text{if } 1 \leq i, j \leq m \text{ and } i + j > m; \\ xyh^{-\xi}, & \text{if } -m < i, j \leq -1 \text{ and } i + j \leq -m; \\ xy, & \text{in the other cases.} \end{cases}$$

Then $G(*)$ is a group.

The proof is not necessary, since the construction is the same as that of [4, Theorem 7.8]. However, some observations should be made since the wording of the two theorems is not exactly the same.

Firstly, in [4] one does not use the notational shortcut involving ξ, but gives an explicit formula for all cases $(\varepsilon,\eta) \in \{0,1\} \times \{0,1\}$. Secondly, the condition $\langle\beta,\gamma\rangle = G/S$ is clearly equivalent to the requirement of [4] that $\alpha = \beta\gamma$ is of order $2m$. Put $G_0 = \langle\alpha\rangle$ and note that $Q(\beta,\gamma) = S \cap Q(G \setminus G_0)$, by Proposition 1.5. Hence, thirdly, the choice of $h \in Q(\beta,\gamma)$ in Theorem 4.1 is the same as the choice of $h \in S \cap Q(G \setminus G_0)$ in [4].

The group $G(*)$ will be denoted by $G[\beta,\gamma,h]$, and whenever we write $G(*) = G[\beta,\gamma,h]$ we implicitly assume that G/S, where $S = \beta^2 = \gamma^2$, is a dihedral group of order $4m$, that $G/S = \langle\beta,\gamma\rangle$ and that $h \in S$ satisfies $hxh = x$ for all $x \in \beta \cup \gamma$. Furthermore, the meaning of m, S, G_0 and α will be regarded as generically fixed. The set $\{-m+1,\dots,-1,0,1,\dots,m\}$ will be denoted by M as in the preceding sections, and we shall also use the mapping σ in the same sense.

The notation $G[U,V,h]$ that was used in [7] and [6] means in our present notation $G[\beta,\gamma,h^{-1}]$, where $m=1$, $U = S\cup\beta$ and $V = S \cup \gamma$.

Note that the operation $*$ can be expressed by

$$x * y = xyh^{(-1)^\eta\sigma(i+j)},\ \text{where } x \in \beta^\varepsilon\alpha^i,\ y \in \alpha^j\gamma^\eta,\ i,j \in M \text{ and } \varepsilon,\eta \in \{0,1\}.$$

The following facts are therefore clear.

Lemma 4.2. *Assume $G(*) = G[\beta,\gamma,h]$. Then $S \cup \beta = \{x \in G;\, x * y = xy$ for all $y \in G\}$ and $S \cup \gamma = \{x \in G;\, y * x = yx$ for all $y \in G\}$. Furthermore, G_0 is also a subgroup of $G(*)$, and $G_0(*) = G_0[\alpha,h]$.*

The formula $x * y = xyh^{(-1)^\eta\sigma(i+j)}$ is not fully satisfactory, as the description of the cosets is different for x and y. Now, $\beta\alpha^j = \alpha^{1-j}\gamma$ and $\alpha^j\gamma = \beta\alpha^{1-j}$ for all $j \in \mathbb{Z}$, and the mapping $\mu : j \mapsto 1-j$ yields an involutory permutation of M. We obtain

$$x * y = xyh^{(-1)^\eta\sigma(i+\mu^\eta(j))},\ \text{where } x \in \beta^\varepsilon\alpha^i,\ y \in \beta^\eta\alpha^j,\ i,j \in M \text{ and } \varepsilon,\eta \in \{0,1\}.$$

The pictorial representation of $G(*) = G[\beta,\gamma,h]$ is discussed in [4], following Theorem 7.8. It consists of four subsquares, where the left upper subsquare corresponds to the pictorial representation of $G_0[\alpha,h]$ that is discussed in Section 2. The other three subsquares are obtained by propagating its pattern first down and then to the right. Rows of $G \setminus G_0$ are labelled $\beta = \beta\alpha^{2m}$, $\beta\alpha^{2m-1}$, $\dots$, $\beta\alpha$, and the motion down is just a shift. There are two ways of representing the subsquares on the right, depending on our choice of column labels. If the columns are denoted by $\gamma = \alpha^{2m}\gamma$, $\alpha^{2m-1}\gamma$, $\dots$, $\alpha\gamma$, then the pattern is obtained by shifting, and if they are denoted by $\beta = \beta\alpha^{2m}$, $\beta\alpha^{2m-1}$, $\dots$, $\beta\alpha$, one has to use mirroring. However, in both cases the value of ε, where $h^\varepsilon = (x*y)(xy)^{-1}$, changes to $-\varepsilon$. Figure 2 gives the table for the case $m=2$ (with $+$ standing for 1 and $-$ for -1).

	1	α^3	α^2	α	β	$\beta\alpha^3$	$\beta\alpha^2$	$\beta\alpha$
1	0	0	0	0	0	0	0	0
α^3	0	$-$	0	0	0	0	$+$	0
α^2	0	0	$+$	$+$	$-$	$-$	0	0
α	0	0	$+$	0	0	$-$	0	0
β	0	0	0	0	0	0	0	0
$\beta\alpha^3$	0	$-$	0	0	0	0	$+$	0
$\beta\alpha^2$	0	0	$+$	$+$	$-$	$-$	0	0
$\beta\alpha$	0	0	$+$	0	0	$-$	0	0

Distribution of the powers of h in the dihedral construction

Lemma 4.3. *Assume $G(*) = G[\beta,\gamma,h]$ and $xy \in S$, for some $x, y \in G$. If $x \notin \alpha^m$, then $x * y = xy$. If $x \in \alpha^m$, then $x * y = xyh$.*

Proof: We have $x \in G_0$ if and only if $y \in G_0$. One can use Lemma 2.2, when $x \in G_0$, and so we can assume $x \in G \setminus G_0$. Then $xS = yS$, and for $x \in \beta\alpha^i$, $i \in M$, we obtain $x * y = xyh^{-\sigma(i+1-i)} = xy$, as $\sigma(1) = 0$. □

Lemma 4.4. *Assume $G(*) = G[\beta,\gamma,h]$, and consider $u \in G \setminus G_0$. Then $H = S \cup Su$ is a common subgroup of both $G(\cdot)$ and $G(*)$, and $x * y = xy$ for all $x, y \in H$.*

Proof: To observe that H is a subgroup, it is sufficient to note that Su is an involution in G/S. Assume $x, y \in H \setminus S$. Then $x * y = xy$, by Lemma 4.3. □

Corollary 2.3 can be thus extended to

Corollary 4.5. *Assume $G(*) = G[\beta,\gamma,h]$ and consider $x \in G$. If $x \notin \alpha^m$, then $x^* = x^{-1}$. If $x \in \alpha^m$, then $x^* = x^{-1}h^{-1}$.*

In the dihedral construction there always exist cases with $x * y * x^* \neq xyx^{-1}$:

Lemma 4.6. *Assume $G(*) = G[\beta,\gamma,h]$. If $s \in S$, then $x * s * x^* = xsx^{-1}$, $x^* * s * x = x^{-1}sx$ and $s^* * x^* * s * x = s^{-1}x^{-1}sx$, for all $x \in G$. If $u \in \alpha^m$, then $u * x * u^* = uxu^{-1}h^{-1}$ and $x * u * x^* * u^* = xux^{-1}u^{-1}h^{-1}$ for all $x \in G \setminus G_0$.*

Proof: The equalities with $s \in S$ follow from Theorem 2.4, Corollary 2.5 and Lemma 4.4. Assume $u \in \alpha^m$ and $x \in \beta\alpha^i$, $i \in M$. Express x as $e * y = ey$, where $e \in \beta$ and $y \in \alpha^i$, $i \in M$, and note that α^m is in the centre of G/S. We obtain $u * x * x^* = (u * e * u^*) * (u * y * u^*) = (u * (eu^{-1}h^{-1}))(uyu^{-1}) = (ueu^{-1}h^{-1}h^{-\sigma(m+1-m)})(uyu^{-1}) = ueyu^{-1}h^{-1} = uxu^{-1}h^{-1}$, using Theorem 2.4, Lemma 4.2, Lemma 2.2 and the definition of $*$. The last equality now easily follows from Lemma 4.4 and Corollary 4.5. □

Proposition 4.7. *Assume $G(*) = G[\beta, \gamma, h]$. A subgroup H of $G(\cdot)$ is a subgroup of $G(*)$ if and only if $h \in H$ or $H \le S \cup Sx$, for some $x \in G \setminus G_0$. If H is a common subgroup of $G(\cdot)$ and $G(*)$, and H is normal in $G(\cdot)$, then H is normal in $G(*)$ if and only if $h \in H$ or $H \le S$.*

Proof: A subset $H \subseteq G$ with $h \in H$ is clearly a (normal) subgroup of $G(\cdot)$ if and only if it is a (normal) subgroup of $G(*)$. For subgroups of $S \cup Sx$, $x \in G \setminus G_0$, use Lemma 4.4. If $H \le S$, then the normality is retained by Lemma 4.6. The same lemma implies $h \in H$ when H is normal in both $G(\cdot)$ and $G(*)$, and satisfies $H \le S \cup Sx$ and $H \cap Sx \ne \emptyset$, for some $x \in G \setminus G_0$. If $H \le G(\cdot)$ is contained in no $S \cup Sx$, $x \in G \setminus G_0$, then $G_0 \cap H$ is not contained in S. If in such a case H is to be a subgroup of $G(*)$, then $G_0 \cap H$ is a subgroup of both $G_0(\cdot)$ and $G_0(*)$. Since it is not contained in S, it has to contain h, by Proposition 2.6. □

If $G(*) = G[\beta, \gamma, h]$, then $h \in Q(G \setminus G_0)$, and $h^g = h^{\pm 1}$, by Lemma 1.4. From Lemma 4.6 we see that $\langle h \rangle$ is a normal subgroup of both $G(\cdot)$ and $G(*)$. The following statement is therefore an immediate consequence of the definition of $*$.

Proposition 4.8. *Assume $G(*) = G[\beta, \gamma, h]$. Then $\langle h \rangle$ is a cyclic normal subgroup of both $G(\cdot)$ and $G(*)$, and the quotient groups $G(\cdot)/\langle h \rangle$ and $G(*)/\langle h \rangle$ coincide.*

It is clear that the operation $\cdot$ can be recovered from $*$ by a converse procedure, and hence we can state without a proof the following proposition, which is analogous to Proposition 3.6.

Proposition 4.9. *If $G(*) = G[\beta, \gamma, h]$, then $G(\cdot) = G(*)[\beta, \gamma, h^{-1}]$.*

The dihedral group D_{4m} is nilpotent if and only if $m = 2^k$ for some $k \ge 0$, and in such a case its nilpotency degree is equal to $k + 1$. These are the only cases when it makes sense to consider the nilpotency of $G[\beta, \gamma, h]$.

Proposition 4.10. *Assume $G(*) = G[\beta, \gamma, h]$ and suppose that $G/S \cong D_{4m}$, $m = 2^k$. The group $G(*)$ is nilpotent if and only if $G(\cdot)$ is nilpotent, and their nilpotency differs at most by $k + 1$.*

Proof: The relationship of $G(\cdot)$ and $G(*)$ is symmetric, by Proposition 4.9. We can thus assume that $G(\cdot)$ is nilpotent. Let $1 \le G_t \lhd G_{t-1} \lhd \dots G_1 \lhd G_0 = G$ be the upper central series of $G(\cdot)$, and let $S = H_k \lhd \dots \lhd H_0 = G$ be such that $H_k/S \lhd \dots \lhd H_0/S$ is the lower central series of $G/S \cong D_{2^{k+2}}$. The series

$$1 = G_t \cap S \trianglelefteq G_{t-1} \cap S \trianglelefteq \dots \trianglelefteq G_1 \cap S \trianglelefteq S \lhd H_{k-1} \lhd \dots \lhd H_0 = G$$

is a central series in $G(*)$, by Proposition 4.7 and Lemma 4.6, since the commutators in $G(*)$ and $G(\cdot)$ coincide when one of their arguments lies in S.

□

Surprisingly, the estimate of Proposition 4.10 is the best possible. Indeed, consider the group

$$G = \langle x, y, z;\ x^{2^k} = y^2 = z^{2^k} = 1,\ xz = zx,\ x^y = x^{-1},\ z^y = z^{-1}\rangle,$$

where $k \geq 1$. This group is a semidirect product of $C_{2^k} \times C_{2^k}$ with C_2, and is of order 2^{2k+1}. It is nilpotent of degree k, and we shall show that for $S = \langle x \rangle$ and $h = x$ we can get $G(*)$ that is isomorphic to $D_{2^{2k+1}}$. This will be the example we need, since $G/S \cong D_{2^{k+1}}$.

Put $\beta = yS$ and $\gamma = yzS$. The crucial point is to show that the $2m$-th power of z in $G(*)$ is an element of S that is of order $2m$ (we have $2m = 2^k$). However, by Lemma 3.1 it is equal to $z^{2^k}h = x$, and so the order of z in $G(*)$ is 2^{2k}. Furthermore, $y * y = y^2 = 1$ and $y * z = yz$, by Lemma 4.2, and for $m \geq 2$ we have $y * z * y = (yz) * y = yzyh^{-\sigma(1+1)} = yzy = z^{-1} = z^*$, by Lemma 4.5, while for $m = 1$ we obtain $y * z * y = (yz) * y = yzyh^{-1} = zh^{-1} = z^*$.

Further information about the groups that can be derived from D_{2^k} by means of cyclic and dihedral constructions can be found in [1]. For the case $m = 1$ see also [7].

5. Characterization of the dihedral construction

Proposition 5.1. *For $i \in \{1,2\}$ assume $G_i = \langle S, u_i, v_i\rangle$, where S is normal in G_i, G_i/S is dihedral of order $4m$, $G_i/S = \langle u_iS, v_iS\rangle$, $u_1^2 = u_2^2 \in S$ and $v_1^2 = v_2^2 \in S$. Put $h = (u_2v_2)^{2m}(u_1v_1)^{-2m}$. If $s^{u_1} = s^{u_2}$ and $s^{v_1} = s^{v_2}$ for all $s \in S$, then $h \in Q(u_iS, v_iS)$ for both $i \in \{1,2\}$, and $G_1(*) = G_1[u_1S, v_1S, h]$ is isomorphic to G_2.*

Proof: We start by proving $(u_1v_1)^j(v_1u_1)^j = (u_2v_2)^j(v_2u_2)^j \in S$, for all $j \geq 0$. The case $j = 0$ is clear. Assume $j \geq 0$ and put $s = (u_1v_1)^j(v_1u_1)^j$. The induction step follows from $(u_1v_1)^{j+1}(v_1u_1)^{j+1} = u_1v_1sv_1u_1 = u_1(v_1^2s^{v_1})u_1 = u_1^2(v_2^2s^{v_2})^{u_1} = u_2^2(v_2sv_2)^{u_2} = u_2v_2sv_2u_2 = (u_2v_2)^{j+1}(v_2u_2)^{j+1}$. The role of u_i and v_i, $i \in \{1,2\}$, is at this stage symmetric, and hence also $(v_1u_1)^j(u_1v_1)^j = (v_2u_2)^j(u_2v_2)^j$, for all $j \geq 0$. Both equalities can be inverted, and therefore they hold for all integers j.

The index of S in $\langle S, u_iv_i\rangle$, $i \in \{1,2\}$, is equal to $2m$, and the respective quotient is cyclic. We have $s^{u_1v_1} = s^{u_2v_2}$ for all $s \in S$, and hence h lies in the centre of $\langle S, u_iv_i\rangle$, by Proposition 2.8. From $h(u_1v_1)^{2m} = (u_1v_1)^{2m}h$ we obtain $(u_2v_2)^{2m}(u_1v_1)^{2m} = (u_1v_1)^{2m}(u_2v_2)^{2m}$, and this gives

$$\begin{aligned}(u_2v_2)^{2m}(u_1v_1)^{-2m}(v_2u_2)^{2m}(v_1u_1)^{-2m} &= \\ (u_1v_1)^{-2m}(u_2v_2)^{2m}(v_2u_2)^{2m}(v_1u_1)^{-2m} &= \\ (u_1v_1)^{-2m}(u_1v_1)^{2m}(v_1u_1)^{2m}(v_1u_1)^{-2m} &= 1.\end{aligned}$$

This means $h^{-1} = (v_2u_2)^{2m}(v_1u_1)^{-2m}$. Now, $h^{u_i} = ((u_2v_2)^{2m})^{u_i}((u_1v_1)^{-2m})^{u_i}$ $= ((u_2v_2)^{2m})^{u_2}((u_1v_1)^{-2m})^{u_1} = (v_2u_2)^{2m}(v_1u_1)^{-2m} = h^{-1}$, for both $i \in \{1,2\}$. We have proved $h \in Q(u_iS)$, by Lemma 1.4. Symmetrically we also get $h^{-1} \in Q(v_iS)$, and so $h \in Q(u_iS, v_iS)$, $i \in \{1,2\}$.

Define now $\varphi : G_2 \to G_1$ by $\varphi(u_2^\varepsilon(u_2v_2)^js) = u_1^\varepsilon(u_1v_1)^js$, for all $s \in S$, $\varepsilon \in \{0,1\}$ and $j \in M = \{-m+1, \dots, -1, 0, 1, \dots, m\}$. If s' is another element of S, then $\varphi(u_2^\varepsilon s'(u_2v_2)^js) = \varphi_2(u_2^\varepsilon(u_2v_2)^j(s')^{(u_1v_1)^j}s) = u_1^\varepsilon s'(u_1v_1)^js$. Similarly, for $s_1, s_2, s_3 \in S$ we get $\varphi(s_1u_2^\varepsilon s_2(u_2v_2)^js_3) = \varphi(u_2^\varepsilon s_1^{u_2^\varepsilon}s_2(u_2v_2)^js_3) = u_1^\varepsilon s_1^{u_1^\varepsilon}s_2(u_1v_1)^js_3 = s_1u_1^\varepsilon s_2(u_1v_1)^js_3$.

For $s_1, s_2, s_3 \in S$, $\varepsilon \in \{0,1\}$ and $j \in M$ we also obtain

$$\varphi(s_1u_2^\varepsilon s_2(v_2u_2)^{-j}s_3) = \varphi(s_1u_2^\varepsilon s_2(v_2u_2)^{-j}(u_2v_2)^{-j}(u_2v_2)^js_3) = \\ s_1u_1^\varepsilon s_2(v_1u_1)^{-j}(u_1v_1)^{-j}(u_1v_1)^js_3 = s_1u_1^\varepsilon s_2(v_1u_1)^{-j}s_3.$$

If $j \in M$, then $-(j-1) \in M$ as well, and $(u_2v_2)^jv_2$ is equal to

$$u_2(v_2u_2)^{j-1}v_2^2(v_2u_2)^{-(j-1)}(v_2u_2)^{j-1} = u_2(v_1u_1)^{j-1}v_1^2(v_1u_1)^{-(j-1)}(v_2u_2)^{j-1}.$$

Hence $\varphi(s_1u_2^\varepsilon s_2(u_2v_2)^js_3v_2)$ is equal to

$$\varphi(s_1u_2^\varepsilon s_2u_2(v_1u_1)^{j-1}v_1^2(v_1u_1)^{-(j-1)}(v_2u_2)^{j-1}s_3^{v_1}).$$

For $\varepsilon = 0$ this gives $s_1s_2(u_1v_1)^js_3v_1$, while for $\varepsilon = 1$ we obtain

$$s_1u_1^2s_2^{u_1}(v_1u_1)^{j-1}v_1^2(v_1u_1)^{-(j-1)}(v_1u_1)^{j-1}s_3^{v_1} = s_1u_1s_2(u_1v_1)^js_3v_1.$$

We have proved that

$$\varphi(s_1u_2^\varepsilon s_2(u_2v_2)^js_3v_2^\eta) = s_1u_1^\varepsilon s_2(u_1v_1)^js_3v_1^\eta$$

for all $s_1, s_2, s_3 \in S$, $j \in M$ and $\varepsilon, \eta \in \{0,1\}$.

Assume $i, j \in M$, $\varepsilon, \eta \in \{0,1\}$ and $s, t \in S$. When $x = u_1^\varepsilon(u_1v_1)^is$ and $y = t(u_1v_1)^jv_1^\eta$ are multiplied in $G_1[u_1S, v_1S, h]$, then one gets $xyh^{(-1)^\eta\sigma(i+j)}$. Define $*$ on G_1 by $x*y = \varphi(\varphi^{-1}(x)\varphi^{-1}(y))$. Then $\varphi : G_1(*) \cong G_2$, and it remains to show that $x*y = xyh^{(-1)^\eta\sigma(i+j)}$. We have $x*y = \varphi(u_2^\varepsilon(u_2v_2)^ist(u_2v_2)^jv_2^\eta) = \varphi(u_2^\varepsilon(st)^{(u_2v_2)^{-i}}(u_2v_2)^{i+j}v_2^\eta)$, and from the above formula for φ we see that $x*y$ is equal to $u_1^\varepsilon(st)^{(u_1v_1)^{-i}}wv_2^\eta$, where $w = \varphi((u_2v_2)^k)$ and $k = i+j$. If $\varphi((u_2v_2)^k) = (u_1v_1)^kh^{\sigma(k)}$, then $x*y = u_1^\varepsilon(u_1v_1)^ist(u_1v_1)^jh^{\sigma(i+j)}v_2^\eta$, and from $hv_2 = v_2h^{-1}$ one really gets the required formula $x*y = xyh^{(-1)^\eta\sigma(i+j)}$. Hence we need to prove $\varphi((u_2v_2)^k) = (u_1v_1)^kh^{\sigma(k)}$ for every k, $-2m \le k \le 2m$. This can be done by repeating the last paragraph of the proof of Proposition 2.8 (where u_i is replaced by u_iv_i, $i \in \{1,2\}$). $\square$

Corollary 5.2. *For $i \in \{1,2\}$ assume $G_i = \langle S, u_i, v_i\rangle$, where $S < G_i$ is a normal subgroup of index $4m$, and G_i/S is generated by involutions u_iS and v_iS. Assume also $u_1^2 = u_2^2$, $v_1^2 = v_2^2$, $(u_1v_1)^{2m} = (u_2v_2)^{2m}$, and suppose $s^{u_1} = s^{u_2}$ and $s^{v_1} = s^{v_2}$ for all $s \in S$. Then there exists an isomorphism $\varphi : G_2 \cong G_1$ such that $\varphi(u_2^\varepsilon s(u_2v_2)^j tv_2^\eta) = u_1^\varepsilon s(u_1v_1)^j tv_1^\eta$ for all $s,t \in S$ and all $\varepsilon, \eta, j \in \mathbb{Z}$.*

Proof: Consider $G_1(*)$ and φ from the proof of Proposition Diso. We assume $h = 1$, and hence $G_1(*)$ does not differ from $G_1(\cdot)$. The isomorphism φ maps u_2 to u_1, v_2 to v_1, u_2v_2 to u_1v_1, and fixes each $s \in S$. Hence the formula for φ can be extended to all integers ε, η and j. $\square$

Recall that the groups G_1 and G_2 are D_{4m}-related, $m \geq 1$, if there exist a group $G = G(\cdot)$, a subgroup $S \lhd G$, involutory cosets $\beta, \gamma \in G/S$ and an element $h \in Q(\beta,\gamma)$ such that $|G : S| = 4m$, $G/S = \langle\beta,\gamma\rangle$, $G_1 \cong G(\cdot)$ and $G_2 \cong G(*) = G[\beta,\gamma,h]$.

Theorem 5.3. *The groups G_1 and G_2 are D_{4m}-related, $m \geq 1$, if and only if there exist groups $H_i \cong G_i$, $i \in \{1,2\}$, a common subgroup $S \lhd H_i$, and elements $u_i, v_i \in H_i \setminus S$ such that $H_i/S = \langle u_iS, v_iS\rangle$, $|H_i : S| = 4m$, $i \in \{1,2\}$, and $u_1^2 = u_2^2 \in S$, $v_1^2 = v_2^2 \in S$, $s^{u_1} = s^{u_2}$ and $s^{v_1} = s^{v_2}$, for all $s \in S$.*

Proof: If groups H_i and elements u_i and v_i exist, then H_i/S is dihedral, and the groups G_1 and G_2 are D_{4m}-related by Proposition 5.1. If $G_1 \cong G(\cdot)$ and $G_2 \cong G(*)$, where $G(*) = G[\beta,\gamma,h]$ and $|G : S| = 4m$, then we can put $H_1 = G(\cdot)$, $H_2 = G(*)$, and consider any $u_1 = u_2 \in \beta$ and $v_1 = v_2 \in \gamma$. The rest follows from Lemmas 4.4 and 4.6. $\square$

6. Isomorphisms of dihedral constructions

Proposition 6.1. *Assume $G = \langle S, u, v\rangle$, where $S \lhd G$, $u^2 \in S$, $v^2 \in S$ and G/S is dihedral of order $4m$, $m \geq 1$. Suppose that $h = (pq)^{(uv)^{2m-1}} \dots (pq)^{(uv)}(pq)$, where $p \in Q(uS)$ and $q \in Q(vS)$. Then $h \in Q(uS, vS)$, and there exists an isomorphism $\varphi : G[uS, vS, h] \cong G$ such that $\varphi(u^\varepsilon s(uv)^j tv^\eta) = (pu)^\varepsilon s(puvq)^j t(vq)^\eta$ for all $j, \varepsilon, \eta \in \mathbb{Z}$.*

Proof: Put $w = uv$ and $z = pq$. We have $z \in Z = Q(uw^0S)\dots Q(uw^{2m-1}S)$, and hence $h \in S \cap Q(G \setminus G_0) = Q(uS, vS)$, by Propositions 1.7 and 1.5. The existence of φ will be proved by means of Corollary 5.2, setting $G_2 = G[uS, vS, h]$, $G_1 = G$, $u_2 = u$, $v_2 = v$, $u_1 = pu$ and $v_1 = uq$. The groups $S \cup Su_1 = S \cup Su_2$ and $S \cup Sv_1 = S \cup Sv_2$ are the same in both G_1 and G_2, by Lemma 4.4, and hence to verify that $u_1^2 = u_2^2$, $s^{u_1} = s^{u_2}$, $v_1^2 = v_2^2$ and $s^{v_1} = s^{v_2}$, $s \in S$, we can compute both sides of each of these equations in G. Conjugation by u_i and v_i, $i \in \{1,2\}$, coincides on S, since $p, q \in Z(S)$, by Lemma 1.4. Furthermore, $u_1^2 = (pup)u = u^2 = u_2^2$ and $v_1^2 = v(qvq) = v^2 = v_2^2$.

The product of u_2 and v_2 in G_2 is equal to $u_2v_2 = w$, by Lemma 4.2, and the $2m$-th power of w in G_2 is equal to $w^{2m}h$, by Lemma 3.1. To fulfil the assumptions of Corollary 5.2 it remains to verify $w^{2m}h = (pwq)^{2m}$, since $pwq = u_1v_1$.

The elements p, q belong to $Z(S)$ and $\langle S, w\rangle = G_0$. A double application of Lemma 1.2 therefore gives

$$(pwq)^{2m} = (wq)^{2m}pp^w \dots p^{w^{2m-1}} = w^{2m}qq^w \dots q^{w^{2m-1}}pp^w \dots p^{w^{2m-1}} = w^{2m}h.$$

□

Corollary 6.2. *Assume $G(*) = G[\beta, \gamma, h]$, $\alpha = \beta\gamma$, and put*

$$Z = Q(\beta)Q(\beta\alpha)\dots Q(\beta\alpha^{2m-1}).$$

If there exists $z \in Z$ and $w \in \alpha$ with $h = z^{w^{2m-1}} \dots z^w z$, then $G(*) \cong G$.

Proof: This is a direct consequence of Propositions 1.8 and 6.1. □

The subgroup $Z = Q(\beta)Q(\beta\alpha)\dots Q(\beta\alpha^{2m-1})$ has for the dihedral construction a similar role to that of $Z(S)$ for the cyclic construction. By setting $T = \{zz^w \dots z^{w^{2m-1}};\ z \in Z\}$ we get a subgroup of $Q(\beta, \gamma)$ such that $G[\beta, \gamma, h_1] \cong G[\beta, \gamma, h_2]$ whenever $h_1, h_2 \in Q(\beta, \gamma)$ are congruent modulo T. This is proved below, but first we have to observe that the dihedral construction exhibits an *affine behaviour* similar to that of the cyclic case.

Proposition 6.3. *Assume $G_1 = G[\beta, \gamma, h_1]$ and $G_2 = G[\beta, \gamma, h_1h_2]$, where h_1 and h_2 are elements of $Q(\beta, \gamma)$. Then $G_2 = G_1[\beta, \gamma, h_2]$.*

Proof: Consider $x \in \beta^\varepsilon\alpha^i$ and $y \in \alpha^j\gamma^\eta$, where $i, j \in M$ and $\varepsilon, \eta \in \{0, 1\}$. The product of x and y in $G_2 = G[\beta, \gamma, h_1h_2]$ is equal to $xy(h_1h_2)^a = xyh_1^ah_2^a$, where $a = (-1)^\eta\sigma(i + j)$. Denote by $*$ the operation of $G_1 = G[\beta, \gamma, h_1]$. The product of x and y in $G_1[\beta, \gamma, h_2]$ is equal to $x * y * h_2^a = (x * y)h_2^a = xyh_1^ah_2^a$. We see that both products give the same result. □

Theorem 6.4. *Assume $S \lhd G$, $G/S \cong D_{4m}$, $m \geq 1$, and suppose that G/S is generated by the cosets β and γ, $\beta^2 = \gamma^2 = S$. Put $\alpha = \beta\gamma$, $G_0 = \langle\alpha, S\rangle$, and $Z = Q(\beta)Q(\beta\alpha)\dots Q(\beta\alpha^{2m-1})$. If $\langle w, S\rangle = G_0$, then $T = \{zz^w \dots z^{w^{2m-1}};\ z \in Z\}$ is a subgroup of $Q(\beta, \gamma) = S \cap Q(G \setminus G_0)$. It contains $\{z^{2m};\ z \in Q(\beta, \gamma)\}$ and does not depend on the choice of $w \in G$, $\langle w, S\rangle = G_0$. If $h_1, h_2 \in Q(\beta, \gamma)$ are such that $h_1h_2^{-1} \in T$, then $G[\beta, \gamma, h_1] \cong G[\beta, \gamma, h_2]$.*

Proof: All of the above mentioned properties of the subgroup T are proved in Proposition 1.7. If $h_1 \equiv h_2 \bmod T$, then $G[\beta, \gamma, h_2] = G_1[\beta, \gamma, h]$, where $G_1 = G[\beta, \gamma, h_1]$ and $h = h_1^{-1}h_2 \in T$, by Proposition 6.3. Inner automorphisms act on S in the same way in G and G_1, by Lemma 4.6. Hence the group $Q(\beta\alpha^j)$, $0 \leq j < 2m$, does not change when defined with respect to G_1. The groups Z and T do not change as well, and so $G[\beta, \gamma, h_2] \cong G_1$ follows from Corollary 6.2.

□

Corollary 6.5. *Assume $G(*) = G[\beta,\gamma,h]$. Then there exists $h' \in Q(\beta,\gamma)$ such that every prime divisor of its order divides $2m$, and $G(*) = G[\beta,\gamma,h']$.*

PROOF: Express h as a product of its powers, $h = h'h''$, in such a way that the order of h'' is coprime to $2m$. Then $h'' = z^{2m}$ for certain $z \in \langle h''\rangle \le Q(\beta,\gamma)$. □

Proposition 6.6. *Assume $G(*) = G[\gamma,\beta,h^{-1}]$. Then there exists an isomorphism $\varphi : G(*) \cong G[\beta,\gamma,h]$ that fixes all elements of $\beta\cup\gamma\cup S$.*

PROOF: Fix $u \in \beta$ and $v \in \gamma$. The product of u and v in $G[\beta,\gamma,h]$ is equal to uv, and the $2m$-th power of uv in $G[\beta,\gamma,h]$ is equal to $(uv)^{2m}h$, by Lemma 3.1. We shall construct the required isomorphism by means of Corollary 5.2 (with $u_1 = u_2 = u$ and $v_1 = v_2 = v$), and we see that the only fact to verify is the equality of the $2m$-th power of $u * v$ in $G(*)$ to $(uv)^{2m}h$.

Suppose first $m = 1$. Then $x * y = xyh^{-1}$ for $(x,y) \in (\alpha\cup\beta)\times\alpha$, $x * y = xyh$ for $(x,y) \in (\alpha\cup\beta)\times\gamma$, and $x * y = xy$ in other cases. Hence $(u*v)*(u*v) = (uvh)*(uvh) = uvhuvhh^{-1} = (uv)^2h$, as required.

Let us now have $m > 1$. Then $u * v = uv$, as $u \in v(vu)S$, $v \in (vu)uS$ and $1+1 = 2 \le m$. We have $uv \in (vu)^{-1}S$ and $-1 \in M$, which implies that the $2m$-th power of uv in $G(*)$ equals $(uv)^{2m}(h^{-1})^{-1} = (uv)^{2m}h$, by Lemma 3.9. □

The next proposition resembles Proposition 3.7, and it is clear that it can be stated without proof.

Proposition 6.7. *Suppose $\varphi : G_1 \cong G_2$ and $G_1(*) \cong G_1[\beta,\gamma,h]$. Then φ also yields an isomorphism $G_1(*) \cong G_2(*)$, where $G_2(*) = G_2[\varphi(\beta),\varphi(\gamma),\varphi(h)]$.*

Proposition 6.8. *Assume $G(*) = G[\beta,\gamma,h]$ and let β' be a coset of G/S that does not intersect G_0. Then there exist $\gamma' \in G/S$ and $h' \in Q(\beta,\gamma) = Q(\beta',\gamma')$ such that $G(*) \cong G[\beta',\gamma',h']$.*

PROOF: We have $G(*) \cong G[\gamma,\beta,h^{-1}]$, by Proposition 6.6, and β' is a conjugate of either β, or $\gamma = \beta\alpha$. The rest can be derived from Proposition 6.7, with φ an appropriate inner automorphism of $G = G(\cdot)$. □

Proposition 6.9. *Assume $G(*) = G[\beta,\gamma\alpha^j,h]$, where β and γ generate G/S, $\alpha = \beta\gamma$ and $j \in M$ is coprime to $2m$. Consider $k \in M$ with $jk \equiv 1 \bmod 2m$. Then $G(*) \cong G[\beta,\gamma,h^k]$.*

PROOF: Put $G_2 = G(*)$ and $G_1 = G[\beta,\gamma,h^k]$, choose $u \in \beta$ and $v \in \gamma$, and set $u_2 = u_1 = u$ and $v_2 = v_1 = v$. Note that the product of u and v is equal to uv in both G_1 and G_2, by Lemma 4.2. We shall again construct the required isomorphism by means of Corollary 5.2. From Lemma 4.4 we see that we need only to verify that the $2m$-th powers of $w = uv$ are the same. In G_1 this power equals $w^{2m}h^k$, by Lemma 3.1. To compute it in G_2, first observe that $\alpha = (\alpha^j)^k$. From Lemma 3.9 we now obtain that it equals $w^{2m}h^k$ as well. □

Theorem 6.10. *Let $S \lhd G$ and $\beta_i, \gamma_i \in G/S$ be such that $G/S \cong D_{4m}$ is generated by β_i and γ_i, $\beta_i^2 = \gamma_i^2 = S$, $i \in \{1,2\}$. For $m = 1$ also assume $\beta_1\gamma_1 = \beta_2\gamma_2$. Then $Q(\beta_1, \gamma_1) = Q(\beta_2, \gamma_2)$ and for every h_1 from this set there exists an element h_2 of the same set such that $G[\beta_1, \gamma_1, h_1] \cong G[\beta_2, \gamma_2, h_2]$.*

Proof: By Proposition 1.5 we have $Q(\beta_i, \gamma_i) = S \cap Q(G \setminus G_0)$. For $m \geq 2$ the subgroup G_0 is determined uniquely. However, for $m = 1$ there are three possibilities, and hence the assumption $\beta_1\gamma_1 = \beta_2\gamma_2$ is needed to guarantee that we are dealing with the same group G_0 for both $i \in \{1,2\}$. Proposition 6.8 reduces the statement to the case $\beta_1 = \beta_2$, and this case is solved in Proposition 6.9. □

References

[1] Bálek M., Drápal A., Zhukavets N., *The neighbourhood of dihedral 2-groups*, submitted.

[2] Donovan D., Oates-Williams S., Praeger C.E., *On the distance of distinct Latin squares*, J. Combin. Des. **5** (1997), 235–248.

[3] Drápal A., *Non-isomorphic 2-groups coincide at most in three quarters of their multiplication tables*, European J. Combin. **21** (2000), 301–321.

[4] Drápal A., *On groups that differ in one of four squares*, European J. Combin. **23** (2002), 899–918.

[5] Drápal A., *On distances of 2-groups and 3-groups*, Proceedings of Groups St. Andrews 2001 in Oxford, to appear.

[6] Drápal A., Zhukavets N., *On multiplication tables of groups that agree on half of columns and half of rows*, Glasgow Math. J. **45** (2003), 293–308.

[7] Zhukavets N., *On small distances of small 2-groups*, Comment. Math. Univ. Carolinae **42** (2001), 247–257.

Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic

E-mail: drapal@karlin.mff.cuni.cz

(*Received* March 20, 2003, *revised* September 12, 2003)