COMPOSITIO MATHEMATICA

J. J. MALONE
C. G. LYONS

Finite dihedral groups and D. G. near rings II

Compositio Mathematica, tome 26, nº 3 (1973), p. 249-259
<http://www.numdam.org/item?id=CM_1973__26_3_249_0>

COMPOSITIO MATHEMATICA, Vol. 26, Fasc. 3, 1973, pag. 249–259
Noordhoff International Publishing
Printed in the Netherlands

FINITE DIHEDRAL GROUPS AND D.G. NEAR RINGS II

by

J. J. Malone and C. G. Lyons

In this paper the distributively generated near rings generated, respectively, by the inner automorphisms, automorphisms, and endomorphisms of a dihedral group of order $2n$, n even, are described. For near rings, a theory of successive decompositions generated by idempotents is developed. This theory is used in determing the form of the endomorphism near ring of the dihedral group. The order of the inner automorphism near ring is found to be $n^3/4$ and that of the automorphism near ring to be $n^3/2$. The order of the endomorphism near ring is $n^7/64$ if $4|n$ but $8 \nmid n$. Otherwise its order is $2n^3/(n/gcd(n, 4))^4$. The radicals of these morphism near rings are also given and the near ring modulo its radical is described.

1. Successive decompositions

In this section we extend Theorems 2.1, 2.2, and 2.3 of [6] to cover successive decompositions generated by idempotents. Since the application of this material is to endomorphism near rings, we assume that the near ring R satisfies the condition that $0r = 0 = r0$, for each $r \in R$.

THEOREM 1.1. *Let e and f be idempotents in the near ring R such that $ef = 0$. Then each $r \in R$ has a unique decomposition*

$$r = [(r-er)-f(r-er)]+f(r-er)+er.$$

Thus $R = D+N+M$, *where*

$$D = \{(r-er)-f(r-er)|r \in R\} = \{x \in R|ex = fx = 0\},$$
$$N = \{f(r-er)|r \in R\} = \{y \in R|ey = 0 \text{ and } fy = y\},$$
$$M = \{er|r \in R\} = \{z \in R|ez = z\},$$

and $D \cap N = D \cap M = N \cap M = (D+N) \cap M = D \cap (N+M) = N \cap (D+M) = \{0\}.$

THEOREM 1.2. *D is a right ideal in R. Each of N and M is an R-subgroup (and subnear ring) of R.*

The two theorems just stated are proved in a manner similar to that used in proving Theorems 2.1 and 2.2 of [6]. The following theorem is an extension of Theorem 2.3 of [6].

THEOREM 1.3. *Let R be a near ring such that $(R, +)$ is generated by $\{r_\gamma | \gamma \in \Gamma$, an index set$\}$. Let e and f be idempotents in R such that $ef = 0$. Then M is the subgroup generated by $\{er_\gamma | \gamma \in \Gamma\}$ and $N = fA_e$(A_e is the normal subgroup generated by $\{r_\gamma - er_\gamma | \gamma \in \Gamma\}$, see* [6]). *Also, D is generated by elements of the form $fa_2 + a_1 - fa_1 - fa_2$, with a_1 and a_2 in A_e.*

PROOF. Let $r \in R$ and let r' denote $r - er$ and r'' denote $r' - fr'$. Note that $eg + r' - eg = (eg + r - eg)'$, $g \in R$. Now r can be written as $r = c_1 + c_2 + \cdots + c_k$, with either c_i or $-c_i$ in $\{r_\gamma | \gamma \in \Gamma\}$, $i = 1, \cdots, k$. Since the application of this theorem in the following sections is to finite groups, the proof is presented for the case in which each c_i is in $\{r_\gamma | \gamma \in \Gamma\}$. The proof can be adapted to the other cases by noting that

$$(-r_\gamma) - e(-r_\gamma) = -er_\gamma + (er_\gamma - r_\gamma) + er_\gamma.$$

By Theorem 2.3 of [6], we may write

$$\begin{aligned} r = {} & c'_1 + (ec_1 + c'_2 - ec_1) + \cdots \\ & + (ec_1 + ec_2 + \cdots + ec_{k-1} + c'_k - ec_{k-1} - \cdots - ec_2 - ec_1) \\ & + (ec_1 + ec_2 + \cdots + ec_k). \end{aligned}$$

Then
$$\begin{aligned} r = {} & c'_1 + (ec_1 + c_2 - ec_1)' + \cdots \\ & + (ec_1 + ec_2 + \cdots + ec_{k-1} + c_k - ec_{k-1} - \cdots - ec_2 - ec_1)' \\ & + (ec_1 + ec_2 + \cdots + ec_k). \end{aligned}$$

Set
$$d_i = (ec_1 + ec_2 + \cdots + ec_{i-1} + c_i - ec_{i-1} - \cdots - ec_2 - ec_1)',$$
$$i = 2, \cdots, k \text{ and } d_1 = c'_1.$$

Thus
$$\begin{aligned} r &= (d''_1 + fd_1) + (d''_2 + fd_2) + \cdots + (d''_k + fd_k) \\ &\quad + [ec_1 + ec_2 + \cdots + ec_k] \\ &= [d''_1 + (fd_1 + d''_2 - fd_1) + (fd_1 + fd_2 + d''_3 - fd_2 - fd_1) + \cdots \\ &\quad + (fd_1 + fd_2 + \cdots + fd_{k-1} + d''_k - fd_{k-1} - \cdots - fd_2 - fd_1)] \\ &\quad + [fd_1 + fd_2 + \cdots + fd_k] + [ec_1 + ec_2 + \cdots + ec_k]. \end{aligned}$$

Specifically, Theorem 1.3 justifies the following procedure for working successive decompositions. One decomposes the generators of R by e to obtain elements of the form $r_\gamma - er_\gamma$ and of the form er_γ. The elements of the first form are conjugated by the elements of the group generated by the elements of the second form. Then a second idempotent f is selected from the elements which can be generated by the conjugates. Then each element in the set of conjugates (call a typical such conjugate $er+r'y-er$) is decomposed as

$$[(er+r'_y-er)-f(er+r'_y-er)]+[f(er+r'_y-er)].$$

Next the elements of the form given in the first term are conjugated by the elements of the group generated by the forms given in the second term. Then these second conjugates generate D, the $f(er+r'_y-er)$ elements generate N, and then er_y elements generate M. This procedure may be iterated and extended to apply to a decomposition involving any finite number of idempotents. The technique is applied to discover the properties of the endomorphism near ring discussed in Section 4.

2. Endomorphisms of D_{2n}

The finite dihedral group of order $2n$ will be designated by D_{2n} and will be presented as $(a, b|a^n, b^2, abab)$. Elements of D_{2n} will be given in the form $a^x b^s$, $0 \leqq x \leqq n-1$, $0 \leqq s \leqq 1$. For the remainder of this paper it is assumed that n is even.

LEMMA 2.1. *The proper normal subgroups of D_{2n} are the subgroups of* (a), *the normal subgroup S generated by b, and the normal subgroup T generated by ab.*

PROOF. It is immediate that the subgroups of (a) are normal. Since $aba^{-1} = a^2 b \in S$, it follows that $(a^2 b)b = a^2 \in S$ and that

$$S = \{a^{2x}b^s | 0 \leqq s \leqq 1, 0 \leqq x \leqq n/2-1\} \text{ with } |S| = n.$$

It is readily shown that the normal subgroup generated by any element of the form $a^{2x}b$ is S. Since $a(ab)a^{-1} = a^3 b \in T$, it follows that $(a^3 b)(ab) = a^2 \in T$ and that $T = \{a^{2x} | 0 \leqq x \leqq n/2-1\} \cup \{a^k b | k \text{ is odd}\}$ with $|T| = n$.

LEMMA 2.2. *For $n \geqq 4$, D_{2n} has $n \cdot (n)\varphi$ automorphisms and n inner auto-morphisms.*

THEOREM 2.3. *D_{2n} has $(n+2)^2$ endomorphisms.*

PROOF. We allow $n = 2$ so that D_4 is the Klein group. Note that the Klein group has 6 automorphisms. For $n = 2$, the result is well-known (see [2]).

Assume $n \geqq 4$. As was shown in [7], if $k > 1$, $k|n$, then D_{2n} contains $t = n/k$ copies of D_{2k}. The number of ways $D_{2n}/(a^k)$ may be mapped onto any one of these is the same as the number of automorphisms of D_{2k}. For $k > 1$ and $k \neq 2$ this number is $k \cdot (k)\varphi$ and for $k = 2$ the number is 6. So there are exactly $n \cdot (k)\varphi$ endomorphisms with kernel

(a^k) for $k > 1$ and $k \neq 2$. Also, there are $3n$ endomorphisms with kernel (a^2). For $k = 1$, $D_{2n}/(a^k) \cong C_2$ and it follows that there are $n+1$ endomorphisms with kernel (a). There are also $n+1$ endomorphisms with kernel S, $n+1$ with kernel T, and the 0 map. Write $3n$ as $2n+n \cdot (2)\varphi$ and $n+1$ as $1+n \cdot (1)\varphi$. Then the number of endomorphisms of D_{2n} is

$$n \cdot \sum_{k|n} (k)\varphi + 4n + 4 = n^2 + 4n + 4 = (n+2)^2.$$

3. $I(D_{2n})$ and $A(D_{2n})$

As in [7] and [6], $I(D_{2n})(A(D_{2n}), E(D_{2n}))$ designates the distributively generated near ring generated additively by the inner automorphisms (automorphisms, endomorphisms) of D_{2n}. I or A or E will be used in cases where no confusion would arise. The conventions used in [7] for designating functions are followed here: the inner automorphism generated by $a^x b^s$ is denoted by $[a^x b^s]$; the endomorphism α such that $(a^x b^s)\alpha = a^{xy+sz} b^s$, $0 \leqq y, z \leqq n-1$, is presented in terms of the images of a and b as $[a^y, a^z b]$; and the function on D_{2n} which maps each power of a to e and each element outside (a) to some fixed $d \in D_{2n}$ is given as (e, d).

Because the form of the needed idempotent function varies as n varies, it is more convenient to present I and A as is done below rather than to use the procedure of Section 1.

THEOREM 3.1. $|I(D_{2n})| = n^3/4$.

PROOF. The theorem is true for $n = 2$. Assume $n \geqq 4$. Note that $[a^k] = [a, a^{-2k}b]$ and $[a^k b] = [a^{-1}, s^{2k}b]$. Set $\delta = (ee \cdots e | a^2 a^2 \cdots a^2)$, where the $2n$-tuple is used to indicate, in order, the images of

$$e, a, a^2, \cdots, a^{n-1}, b, ab, a^2 b, \cdots, a^{n-1} b.$$

The bar $|$ is inserted as a matter of convenience between the images of a^{n-1} and b. Since $\delta = -[e]+[a]$, $\delta \in I$. Moreover, $[a^k] = k\delta + [e]$, $k = 0, 1, \cdots, n/2-1$. Now set

$$\alpha = (ee \cdots e | ea^2 a^4 \cdots a^{-2} || ea^2 a^4 \cdots a^{-2}),$$

where the symbol $||$ separates the image of $a^{(n/2)-1}b$ and the image of $a^{n/2}b$. Since $\alpha = [e]+[b]$, $\alpha \in I$. Also,

$$[a^{(n/2)-k}b] = -[a^k]+\alpha, k = 0, 1, \cdots, (n/2)-1.$$

Obviously, $\alpha+\delta = \delta+\alpha$ and $(\alpha) \cap (\delta) = (e, e)$. Also, $-[e]+\delta+[e] = -\delta$ and $-[e]+\alpha+[e] = -\alpha$. In total then, for some choice of integers u, v, and w, an arbitrary element of I can be given in the form $u[e]+v\alpha+w\delta$. Thus $I(D_{2n})$ is the semidirect sum $([e])+[(\alpha) \oplus (\delta)]$, $(\alpha) \oplus (\delta)$ normal in $(I, +)$ and $|I| = n(n/2)(n/2) = n^3/4$.

THEOREM 3.2. $|A(D_{2n})| = n^3/2$, $n \geqq 4$.

PROOF. Let $\beta = (ee \cdots e|aa \cdots a)$. Since $\beta = [a, b] + [a, a^{-1}b]$, $\beta \in A$. Obviously, $\beta \notin I(D_{2n})$. An arbitrary automorphism of D_{2n} has the form $[a^k, a^x b]$, $(k, n) = 1$ (in particular, k is an odd integer). If x is even set $\psi = [a, a^x b] \in I$ and if x is odd set $\psi = \beta + [a, a^{x-1}b]$, where $[a, a^{x-1}b] \in I$. Then $[a^k, a^x b] = ((k-1)/2)\alpha + k\psi$, i.e. all automorphisms are in the group generated by I and β. Since $2\beta = \delta$ we have, in particular, that $\beta + \delta = \delta + \beta$. Also, $\alpha + \delta = \delta + \alpha$ and $-[e] + \beta + [e] = -\beta$. Thus (β) is a normal subgroup of $(A, +)$ and, in fact, $A = (\beta) + I$. Thus $|A(D_{2n})| = (n(n^3/4))/(n/2) = n^3/2$. Note that if $4|n$, we may state that

$$A = ((ee \cdots e|a^{n/2}a^{n/2} \cdots a^{n/2})) \oplus I.$$

Also note that for some choice of integers u, v, and w, an arbitrary element of A can be written in the form $u[e] + v\alpha + w\beta$.

THEOREM 3.3. *Let $J(R)$ designate the radical of a near ring R. Then $J(I(D_{2n})) = \Phi_n + [(\alpha) \oplus (\delta)]$ and $J(A(D_{2n})) = \Phi_n + [(\alpha) \oplus (\beta)]$, where Φ_n is the subring whose additive group is the Frattini subgroup of the group $([e])$.*

PROOF. Since $(I, +)$ is solvable, it follows from Lemma 2.1 of [1] that each maximal right ideal of I contains the commutator subgroup of $(I, +)$, namely $(2\alpha) \oplus (2\delta)$.

Note that, if u is odd $(u[e] + v\alpha + w\delta)\delta = \delta$ and

$$(u[e] + v\alpha + w\delta)\alpha = -2w\delta + (1-2v)\alpha.$$

Thus, if K is a maximal right ideal which contains $u[e] + v\alpha + w\delta$, then $\delta \in K$ and $\alpha \in K$. It follows that $K = (t[e]) + [(\alpha) \oplus (\delta)]$, where t is an odd integer chosen so that $(t[e])$ is a maximal subgroup of $([e])$. Lemma 2.1 of [1] assures us that a maximal right ideal of I is also a maximal I-subgroup. If L is a right ideal which contains no element for which u is odd, then L is contained in the maximal right ideal $(2[e]) + [(\alpha) \oplus (\beta)]$.

If I is replaced by A and δ is replaced by β in the two paragraphs above, the statements which result are correct. Since, in our case, the radical is the intersection of the maximal right ideals, the theorem follows for both I and A.

By direct observation or by Theorem 2.2 of [1] it can be seen that $J(I)$ and $J(A)$ are nilpotent.

THEOREM 3.4. *$I/J(I) \cong A/J(I) \cong Z/(q)$, where q is the product of the distinct prime factors of n.*

PROOF. Note that Φ_n is generated additively by $q[e]$ (see 8.1 of p. 134 of [4]). From this and the theorems of this section it follows that $|I/J(I)| =$

$|A/J(A)| = q$ and that the additive groups of the quotient near rings are cyclic. Since each of the two quotient near rings has a multiplicative identity, each is isomorphic to the ring of integers modulo q (see the Corollary of p. 147 of [3]).

4. $E(D_{2n})$

In this section the form of $E(D_{2n})$ is displayed. This is done thru the use of the technique of successive decompositions which was developed in the first section. We start by restating the results of Theorem 2.3 in tabular form.

Endomorphisms of D_{2n}

	Form	Kernel	Number	Comment
(1)	$[e, e]$	D_{2n}	1	
(2)	$[a^y, a^x b]$	(e)	$n \cdot (n)\varphi$	$(y, n) = 1,\ 0 \leqq x \leqq n-1$
(3)	$[d, e]$	S	$n+1$	$\|d\| = 2$
(4)	$[d, d]$	T	$n+1$	$\|d\| = 2$
(5)	$[e, d]$	(a)	$n+1$	$\|d\| = 2$
(6)	$[a^{n/2}, a^x b]$	(a^2)	n	$0 \leqq x \leqq n-1$
(7)	$[a^x b, a^{x+n/2} b]$	(a^2)	n	$0 \leqq x \leqq n-1$
(8)	$[a^x b, a^{n/2}]$	(a^2)	n	$0 \leqq x \leqq n-1$
(9)	$[a^{st}, a^x b]$	(a^k)	$\sum_{k\|n} n \cdot (k)\varphi$	$k \neq 1, 2, n;\ t\|n;$ $(s, k) = 1;\ 0 \leqq x \leqq n-1$

Let m be an integer such that $0 \leqq m \leqq n-1$. If $(m, n) = 1$, then $[a^m, a^x b]$ is an automorphism included in form (2). If $(m, n) = t$, then $m = (m/t) \cdot t$ with $(m/t, n/t) = 1$ and $[a^m, a^x b]$ is an endomorphism included in (9). If $m = 0$, then $[a^m, a^x b]$ is a form which includes all endomorphisms of (5) except $[e, a^{n/2}]$. Thus $[a^y, a^x b]$, $0 \leqq y, x \leqq n-1$, gives n^2 endomorphisms and includes all endomorphisms of (2), (5), (6), and (9) with the exception of $[e, a^{n/2}]$. So there are six different forms for the endomorphisms of D_{2n}, i.e. for the generators of E. The idempotent functions of E which will be used to generate the decompositions will be designated by γ's. The generators themselves will be designated by α's. The procedure followed is that given in the last paragraph of Section 1. If γ_1 is chosen to be $[e, b]$, the following table is obtained.

α	$\alpha-\gamma_1\alpha$	$\gamma_1\alpha$
$[a^y, a^x b]$	$(ea^y a^{2y} a^{3y}\cdots \mid ea^y a^{2y} a^{3y}\cdots)$	$[e, a^x b]$
$[d, e]$	$(eded\cdots \mid eded\cdots)$	$[e, e]$
$[d, d]$	$(eded\cdots \mid eded\cdots)$	$[e, d]$
$[e, a^{n/2}]$	$(eeee\cdots \mid eeee\cdots)$	$[e, a^{n/2}]$
$[a^x b, a^{x+n/2} b]$	$(ea^x bea^x b\cdots \mid ea^x bea^x b\cdots)$	$[e, a^{x+n/2} b]$
$[a^x b, a^{n/2}]$	$(ea^x bea^x b\cdots \mid ea^x bea^x b\cdots)$	$[e, a^{n/2}]$

Now it is seen that $M(\gamma_1) = \{(e, g) \mid g \in D_{2n}\}$ and that as a group $M(\gamma_1)$ is isomorphic to D_{2n}. Among the $\alpha-\gamma_1\alpha$ there are just two forms:

$$(ea^y a^{2y} a^{3y}\cdots \mid ea^y a^{2y} a^{3y}\cdots)$$

and

$$(eded\cdots \mid eded\cdots).$$

Since the case $d = a^{n/2}$ is included in the first of these forms we may assume that the d of the second form can be given as $a^x b$.

Now these two forms must be conjugated by the $\gamma_1\alpha$'s. This conjugation yields the generators of $A(\gamma_1)$:

$(1) = (ea^y a^{2y} a^{3y}\cdots \mid ea^y a^{2y} a^{3y}\cdots)$,
$(2) = (ea^x bea^x b\cdots \mid ea^x bea^x b\cdots)$,
$(3) = (ea^y a^{2y} a^{3y}\cdots \mid ea^{-y} a^{-2y} a^{-3y}\cdots)$,
$(4) = (ea^x bea^x b\cdots \mid ea^{2y-x} bea^{2y-x} b\cdots)$,
$(5) = (ea^x bea^x b\cdots \mid ea^{2y+x} bea^{2y+x} b\cdots)$.

For the second decomposition, set $\gamma_2 = [ab, e] \in A(\gamma_1)$. It follows that:

$\gamma_2(1) = (ea^y ea^y\cdots \mid ea^y ea^y\cdots)$,
$\gamma_2(2) = (ea^x bea^x b\cdots \mid ea^x bea^x b\cdots)$,
$\gamma_2(3) = (ea^{-y} ea^{-y}\cdots \mid ea^{-y} ea^{-y}\cdots)$,
$\gamma_2(4) = (ea^{2y-x} bea^{2y-x} b\cdots \mid ea^{2y-x} bea^{2y-x} b\cdots)$,
$\gamma_2(5) = (ea^{2y+x} bea^{2y+x} b\cdots \mid ea^{2y+x} bea^{2y+x} b\cdots)$.

Thus, $M(\gamma_2) = \{(egeg\cdots \mid egeg\cdots) \mid g \in D_{2n}\}$ and as a group is isomorphic to D_{2n}. In $A(\gamma_2)$ we have:

$(1)-\gamma_2(1) = (eea^{2y} a^{2y}\cdots a^{(n-2)y} \mid eea^{2y} a^{2y}\cdots a^{(n-2)y})$,
$(2)-\gamma_2(2) = (eeee\cdots \mid eeee\cdots)$,
$(3)-\gamma_2(3) = (ea^{2y} a^{2y} a^{4y} a^{4y}\cdots e \mid eea^{-2y} a^{-2y}\cdots a^{-(n-2)y})$,
$(4)-\gamma_2(4) = (ea^{2x-2y} ea^{2x-2y}\cdots \mid eeee\cdots)$,
$(5)-\gamma_2(5) = (ea^{-2y} ea^{-2y}\cdots \mid eeee\cdots)$.

These last five types are of three forms:

$$(1) = (eea^{2y}a^{2y}\cdots a^{(n-2)y} \mid eea^{2y}a^{2y}\cdots a^{(n-2)y}),$$
$$(2) = (ea^{2y}a^{2y}a^{4y}\cdots e \mid eea^{-2y}a^{-2y}\cdots a^{-(n-2)y}),$$
$$(3) = (ea^{2y}ea^{2y}\cdots \mid eeee\cdots).$$

If $n = 4$, then $(1) = (eea^2a^2 \mid eea^2a^2)$, $(2) = (ea^2a^2e \mid eea^2a^2)$, and $(3) = (ea^2ea^2 \mid eeee)$. Since $(3) = (1)+(2)$ and each of (1) and (2) is in the additive center of $E(D_8)$, it follows that $A(\gamma_2) = ((1)) \oplus ((2))$ and that $E(D_8) = A(\gamma_2)+M(\gamma_2)+M(\gamma_1)$ has order 256. Until the statement of Theorem 4.1 it is assumed than $n \neq 4$.

For $n \neq 4$, we conjugate forms (1), (2), and (3) by the elements of $M(\gamma_2)$ and obtain two additional forms:

$$(4) = (eea^{2y}a^{-2y}\cdots a^{-(n-2)y} \mid eea^{2y}a^{-2y}\cdots a^{-(n-2)y}),$$
$$(5) = (ea^{-2y}a^{2y}a^{-4y}\cdots e \mid eea^{-2y}a^{2y}\cdots a^{(n-2)y}).$$

These last five forms furnish the generators for $A(\gamma_2)$.

To begin the third decomposition let γ_3 be the element of form (1) for which $y = 1$. Then:

$$\gamma_3(1) = (eea^{2y}a^{2y}\cdots a^{(n-2)y} \mid eea^{2y}a^{2y}\cdots a^{(n-2)y})$$
$$= \gamma_3(2) = \gamma_3(4) = \gamma_3(5) \text{ and } \gamma_3(3) = [e, e].$$

So $M(\gamma_3)$ is generated additively by γ_3 and is a cyclic group of order $n/2$.

In $A(\gamma_3)$ we have:

$$(1)-\gamma_3(1) = (eeee\cdots \mid eeee\cdots),$$
$$(2)-\gamma_3(2) = (ea^{2y}ea^{2y}\cdots \mid eea^{-4y}a^{-4y}\cdots a^{-2(n-2)y}),$$
$$(3)-\gamma_3(3) = (ea^{2y}ea^{2y}\cdots \mid eeee\cdots),$$
$$(4)-\gamma_3(4) = (eeea^{-4y}ea^{-8y}\cdots a^{-(n-2)y} \mid eeea^{-4y}ea^{-8y}\cdots a^{-2(n-2)y}),$$

and

$$(5)-\gamma_3(5) = (ea^{-2y}ea^{-6y}ea^{-10y}\cdots a^{-(n-2)y} \mid eea^{-4y}ea^{-8y}e\cdots e).$$

The conjugation of these five functions by the elements of $M(\gamma_3)$ produces no new forms so, omitting the identity map, we take the remaining forms as giving the generators of $A(\gamma_3)$. However, the study of $A(\gamma_3)$ is facilitated by introducing a new set of generating forms for $A(\gamma_3)$. These are defined by:

$$\lambda_1 = (3)-\gamma_3(3),$$
$$\lambda_2 = (3)-\gamma_3(3)-((2)-\gamma_3(2))$$
$$= (eeee\cdots \mid eea^{4y}a^{4y}a^{8y}a^{8y}\cdots a^{-4y}),$$

$$\lambda_3 = -((5)-\gamma_3(5))+\lambda_1-\lambda_2-((4)-\gamma_3(4))$$
$$= (ea^{4y}ea^{12y}ea^{20y}\cdots a^{-4y} \mid eeee\cdots),$$
$$\lambda_4 = (4)-\gamma_3(4).$$

Since $(3)-\gamma_3(3) = \lambda_1$, $(2)-\gamma_3(2) = \lambda_1-\lambda_2$, $(4)-\gamma_3(4) = \lambda_4$, and $(5)-\gamma_3(5) = \lambda_1-\lambda_2-\lambda_3-\lambda_4$, the λ's do provide a set of generators for $A(\gamma_3)$. For each i the set of functions of the form λ_i constitute a cyclic subgroup. Henceforth we identify λ_i with the element of that form for which $y = 1$, i.e. λ_i generates that cyclic subgroup. Note that $|\lambda_1| = n/2$ and that $|\lambda_2| = |\lambda_3| = |\lambda_4| = n/gcd(n, 4))$.

Obviously, $(\lambda_1) \cap (\lambda_2) = [e, e]$ so that the sum of (λ_1) and (λ_2) is direct. Consider $((\lambda_1) \oplus (\lambda_2)) \cap (\lambda_3)$. This intersection is the same as $(\lambda_1) \cap (\lambda_3)$. If $x\lambda_1 = y\lambda_3$, then in particular $n|2x-4y$ and $n|2x-12y$ so that $n|8y$. Thus an element in the intersection is the identity map or has order 2. In the latter case a^{2x} must be $a^{n/2}$. If $4\nmid n$, this is impossible and the intersection is trivial so that the sum $(\lambda_1)+(\lambda_2)+(\lambda_3)$ is direct and has order $(n/2)^3 = (n/gcd(n, 4))^3$. If $4|n$ but $8\nmid n$, the intersection is trivial since $n\nmid(4y-(n/2))$, i.e. $y\lambda_3$ cannot be of order 2. Thus the sum is direct and has order $n^3/32$. If $8|n$, the intersection has order 2 and the sum is a subgroup of order $((n/2)\cdot(n/4)^2)/2 = (n/gcd(n, 4))^3$. Since $(\lambda_2) \cap (\lambda_4) = [e, e]$, it follows that $((\lambda_1)+(\lambda_2)+(\lambda_3)) \cap (\lambda_4) = [e, e]$. Hence $A(\gamma_3) = ((\lambda_1)+(\lambda_2)+(\lambda_3)) \oplus (\lambda_4)$ has order $(n/gcd(n, 4))^4$ unless $4|n$ but $8\nmid n$. In that case, $|A(\gamma_3)| = n^4/128$.

Since $E = [[[A(\gamma_3)]+M(\gamma_3)]+M(\gamma_2)]+M(\gamma_1)$ and $|E| = |A(\gamma_3)|\cdot(n/2)\cdot(2n)^2$ we have the following theorem. Note that the case $n = 4$ is included in the statement of the theorem.

THEOREM 4.1. *If $4|n$ but $8\nmid n$, the order of $E(D_{2n})$ is $n^7/64$. Otherwise the order of $E(D_{2n})$ is $2n^3(n/gcd(n, 4))^4$.*

5. The Radical of $E(D_{2n})$

LEMMA 5.1. *Let $\sigma \in J(E)$. Then $(D_{2n})\sigma \leqq (a^2)$.*

PROOF. If, for $c \in D_{2n}$, $c\sigma \notin (a^2)$, then there is a function π of $M(\gamma_2)$ or $M(\gamma_1)$ for which $g = c$ so that $c\sigma\pi = c$. But then $\sigma\pi \in J(E)$ and $\sigma\pi$ fixes c. This is a contradiction since $J(E)$ must be nilpotent (see Theorem 2.2 of [1]).

Note that (a^2) is a fully invariant abelian subgroup of D_{2n} and that each element of E when restricted to (a^2) is an endomorphism of (a^2). Thus the restriction is completely determined by its action on a^2.

LEMMA 5.2. *Let $\sigma \in J(E)$. Then $a^2\sigma = a^{2r}$, where r is divisible by each* *prime factor of n if* $4|n$ *and is divisible by each odd prime factor of n if* $4\nmid n$.

PROOF. If $a^2\sigma = a^{2r}$, then $a^2\sigma^2 = a^{2r\cdot r}$, etc. In order for σ to be nilpotent, there must exist a k such that $n|2r^k$. Thus the condition on x which was stated in the Lemma is a necessary and sufficient condition for σ to be nilpotent.

THEOREM 5.3. $J(E) = \{\sigma \in E|(D_{2n})\sigma \subseteq (a^2)$ *and* $a^2\sigma = a^{2r}$, r *as in Lemma* 5.2$\}$.

PROOF. By the previous two lemmas, the given conditions on σ are necessary for σ to be in $J(E)$. Conversely, it is easily seen that the set of elements which obey the given conditions is closed under addition. Let $\pi \in E$. Recall that (a^2) is fully invariant so that there exists a k such that $a^2\pi = a^{2k}$. But then, $c\sigma\pi \subseteq (a^2)$ for any $c \in D_{2n}$ and $a^2\sigma\pi = a^{2rk}$, where rk satisfies the conditions on r given in Lemma 5.2. Thus the given set is an E-subgroup. By Theorem 2.7 of [5] this E-subgroup is nilpotent (the nilpotence may also be noted by inspection) and by Theorem 2.5 of [5] the set is contained in $J(E)$.

We now use Theorem 5.3 to determine the size of $J(E)$ and the nature of the ring $E/J(E)$. Theorem 2.2 of [1] assures us that the quotient near ring is actually a ring. First we determine $J(E)$ for D_8. From Theorem 5.3 we have that

$$J(E(D_8)) = ((ea^2ea^2 \mid eeee))+((ea^2ea^2 \mid ea^2ea^2)) \\ +((eeee \mid a^2a^2a^2a^2)).$$

It is interesting to note that $|J(E(D_8))| = 8$, $|J(A(D_8))| = 16$, and $|J(I(D_8))| = 8$. In this case, $E/J(E)$ has order 32 and additively is the direct sum of groups of order 2. In the discussion of J which follows it is assumed that $n \geqq 6$.

Let $K = \{\sigma \in J(E)|a^2\sigma = e$, i.e. $r = n/2\}$. The set K is easily seen to be a nilpotent E-subgroup and, in fact, $K = A(\gamma_3) \oplus M' \oplus M''$, where

$$M' = \{\sigma \in M(\gamma_1)|g \in (a^2)\} \text{ and } M'' = \{\sigma \in M(\gamma_2)|g \in (a^2)\}.$$

Thus $K \subseteq J(E)$. Also, $|M'| = |M''| = n/2$. Note that K has the null multiplication.

Now consider those elements of J for which $a^2\sigma \neq e$. If such an element is presented in the form for the decomposition of E given in Section 4, then the summand from $M(\gamma_3)$ cannot be $[e, e]$. This summand from $M(\gamma_3)$ can have any element of K added to it. Of course, the summand from $M(\gamma_3)$ must be nilpotent and so we define $M''' = \{\sigma \in M(\gamma_3)|a^2\sigma = a^{2r}$, r as in Lemma 5.2$\}$. Note that M''' is analagous to the Φ_n which appears in the decomposition of $J(I)$ or $J(A)$ and that $|M'''| = n/2p_2 \cdots p_m$ if $4 \nmid n$ and $|M'''| = n/4p_2 \cdots p_m$ if $4|n$, the p_i being the distinct prime factors on n. All told,

$$J(E) = A(\gamma_3) \oplus M' \oplus M'' \oplus M'''.$$

Let $q = 2p_2 \cdots p_m$.

The following table sums up the information on the order of $J(E)$.

	$\lvert A(\gamma_3)\rvert$	$\lvert M'\rvert$	$\lvert M''\rvert$	$\lvert M'''\rvert$	$\lvert J(E)\rvert$	$\lvert E/J(E)\rvert$
$2\mid n,\ 4\nmid n$	$n^4/16$	$n/2$	$n/2$	n/q	$n^7/2^6q$	$8q$
$4\mid n,\ 8\nmid n$	$n^4/128$	$n/2$	$n/2$	$n/2q$	$n^7/2^{10}q$	$16q$
$8\mid n$	$n^4/256$	$n/2$	$n/2$	$n/2q$	$n^7/2^{11}q$	$16q$

In the quotient structure $E/J(E)$, $M(\gamma_1)$ and $M(\gamma_2)$ become rings of order 4 and characteristic 2 and $A(\gamma_3)$ is reduced to order 1. $M(\gamma_3)$ is reduced to a ring defined on a cyclic group of order $q/2$ if $4 \nmid n$ and to a ring defined on a cyclic group of order q if $4|n$. Overall, $E/J(E)$ is a ring with identity with order as given in the table above.

REFERENCES

J. C. BEIDLEMAN

[1] Distributively generated near-rings with descending chain condition, Math. Z. 91 (1966), 65–69.

J. R. CLAY

[2] The near rings on groups of low order, Math. Z. 104 (1968), 364–371.

J. R. CLAY and J. J. MALONE

[3] The near-rings with identities on certain finite groups, Math. Scand. 19 (1966), 146–150.

J. D. DIXON

[4] Problems in group theory, Blaisdell, Waltham, 1967.

R. R. LAXTON

[5] A radical and its theory for distributively generated near rings, J. London Math. Soc. 38 (1963), 40–49.

J. J. MALONE and C. G. LYONS

[6] Endomorphism near rings, Proc. Edinburgh Math. Soc. 17 (1970), 71–78.

J. J. MALONE and C. G. LYONS

[7] Finite dihedral groups and d.g. near rings I, Compositio Mathematica 24 (1972), 305-312.

(Oblatum 16–III–1972)

J. J. Malone
Department of Mathematics
Worcester Polytechnic Institute
Worcester, Massachusetts 01609

C. G. Lyons
Department of Mathematics
Madison College
Harrisonburg, Virginia 22801