J. J. MALONE
C. G. LYONS

Finite dihedral groups and D. G. near rings I

Compositio Mathematica, tome 24, nº 3 (1972), p. 305-312
<http://www.numdam.org/item?id=CM_1972__24_3_305_0>

COMPOSITIO MATHEMATICA, Vol. 24, Fasc. 3, 1972, pag. 305–312
Wolters-Noordhoff Publishing
Printed in the Netherlands

FINITE DIHEDRAL GROUPS AND D. G. NEAR RINGS I

by

J. J. Malone and C. G. Lyons

In this paper two major questions concerning finite dihedral groups of order $2n$, n odd, and distributively generated (d. g.) near rings are investigated. It is shown that the d. g. near rings generated, respectively, by the inner automorphisms, automorphisms, and endomorphisms of such a group are identical, the order being $2n^3$. Results are also obtained about the ideal structure of these near rings. The radical is displayed and it is shown that the endomorphism near ring modulo the radical is isomorphic to the ring $I/(q)$, where q depends on n. The number of non-isomorphic d. g. near rings which can be defined on such a dihedral group is determined. This number is $1+2^r$, where r is the number of distinct primes occurring in the factorization of n. Finally, some results on embeddings are given.

1. Properties 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 odd.

LEMMA 1. 1) *The subgroups of* (a) *are normal in* D_{2n}. *These are the only proper normal subgroups of* D_{2n}.

2) *Let* $k|n$, $k > 1$. *Then* $D_{2n}/(a^k) \cong D_{2k}$. D_{2n} *contains* $n/k = t$ *distinct copies of* D_{2k}.

PROOF. 1) The normality of the subgroups of (a) is clear. If $H \lhd D_{2n}$ and $a^x b \in H$, $x \neq 0$, then $a^2 \in H$ and $H = D_{2n}$.

2) In $D_{2n}/(a^k)$ the class containing a^t serves as the generator of order k and the class containing b serves as the generator of order 2. For any value of x, $(a^t, a^x b) \cong D_{2k}$. For $0 \leqq x \leqq t-1$, these subgroups are distinct.

THEOREM 2. D_{2n} *has* $(n)\phi \cdot n$ *automorphisms*, $2n$ *inner automorphisms, and* n^2+1 *endomorphisms.*

PROOF. Under an automorphism α, a must map to some a^y, with $(n, y) = 1$ and b must map to an element of order 2, say $a^z b$. Thus $(a^x b^s)\alpha = a^{xy+sz} b^s$. It is a routine matter to show that any such α is an automorphism. There are $(n)\phi$ possibilities for y and n possibilities for z. D_{2n} is centerless. Thus distinct elements generate distinct inner automorphisms.

As was noted above, D_{2n} contains $n/k = t$ copies of D_{2k}. The number of ways $D_{2n}/(a^k)$ may be mapped onto any of these is the same as the number of automorphisms of D_{2k}, namely $(k)\phi \cdot k$. Thus the number of endomorphisms with (a^k) as the kernel is $t \cdot (k)\phi \cdot k = n \cdot (k)\phi$. For $k = 1$, $D_{2n}/(a^k) \cong C_2$ which has n copies in D_{2n}. Write $n = n \cdot (1)\phi$. For $k = n$, we have (e) as the kernel and are considering the automorphisms. The only other normal subgroup is D_{2n} itself, which as a kernel, gives the 0 map. Thus the number of endomorphisms of D_{2n} is

$$1 + \sum_{k|n} n \cdot (k)\phi = 1 + n \sum_{k|n} (k)\phi = 1 + n^2.$$

2. Properties of $E(D_{2n})$

$E(D_{2n})$ $(A(D_{2n}), I(D_{2n}))$ designates the d. g. near ring generated additively by the endomorphisms (automorphisms, inner automorphisms) of D_{2n}. (In cases where no confusion would arise, E_n or A_n or I_n will be used.) In this section we use the theory developed in [8] to find the properties of $E(D_{2n})$. For terminology used but not defined in this section, see [8].

Let the inner automorphism generated by $a^x b^s$ be designated by $[a^x b^s]$. In general, let the endomorphism α such that $(a^x b^s)\alpha = a^{xy+sz} b^s$, $0 \leqq y$, $z \leqq n-1$, be denoted by $[a^y, a^z b]$ where the given elements are respectively, the images of a and b. Note that $[a^x] = [a, a^{-2x} b]$ and $[a^x b] = [a^{-1}, a^{2x}]$. The function on D_{2n} which maps each power of a to e and each element of order 2 to some fixed $d \in D_{2n}$ will be given as (e, d). If d has order 2, $(e, d) = [e, d]$.

THEOREM 3. *$I(D_{2n}) = A(D_{2n}) = E(D_{2n})$ and $|E_n| = 2n^3$.*

PROOF. We use the technique of Theorem 2.3 of [8] to study I_n. (If R is a near ring such that $(R, +)$ is generated by the elements of S, $S \subset R$, and e is an idempotent of R, then $R = A_e + M_e$ where A_e is the normal subgroup of $(R, +)$ generated by $\{s - es | s \in S\}$ and M_e is the subgroup of $(R, +)$ generated by $\{es | s \in S\}$. In fact, A_e is a right ideal of R and M_e is a subnear ring of R.) First we need an idempotent of I_n which will induce a non-trivial decomposition of I_n. This is furnished by

$$(n+1)[e] + ((n+1)/2)([e] + [b]) + [b] = [e, b].$$

So $[e, b]$ is the 'e' of Theorem 2.3.

Working with the inner automorphisms as the generating set of the d. g. near ring I_n, we see that $[e, b][a^x] = [e, a^{-2x}b]$ and $[e, b][a^x b] = (e, a^{2x})$. Thus $M_e = \{(e, d) | d \in D_{2n}\}$ and $|M_e| = 2n$. Also

$$[a^x] - [e, a^{-2x}b] = (eaa^2 \cdots a^{n-1} | eaa^2 \cdots a^{n-1}) = \beta,$$

where the $2n$-tuple is used to indicate, in order, the images of

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

The bar $|$ is inserted as matter of convenience between the images of a^{n-1} and b. In addition, $[a^x b] - (e, a^{2x}) = (n-1)\beta$. Thus A_e is the normal subgroup generated by β. Consider that

$$((n+1)/2)[-[e, b] + \beta + [e, b] + \beta] = (eaa^2 \cdots a^{-1} | ee \cdots e) = \gamma$$

is in A_e and that

$$(n-1)\gamma + \beta = (ee \cdots e | eaa^2 \cdots a^{-1}) = \delta$$

is in A_e. It follows that $A_e = (\gamma) \oplus (\delta)$ and $|A_e| = n^2$. Thus $|I_n| = 2n^3$.

An arbitrary automorphism $[a^y, a^z b]$, $(y, n) = 1$, is given as $y\gamma + y\delta + [e, a^z b]$. Thus $I_n = A_n$.

Note that all endomorphisms with kernel (a) are in M_e. Consider then an endomorphism Ψ with kernel (a^k), $k|n$, $1 < k < n$. The image of Ψ (see Lemma 1, part 2) is generated by a^t, $t = n/k$, and $a^x b$, x a fixed integer such that $0 \leqq x \leqq t-1$. Thus $a\Psi = a^{yt}$, $(y, k) = 1$, and $b\Psi = a^{x+mt}b$, $0 \leqq m \leqq k-1$. However, $[a^{yt}, a^{x+mt}b] = yt\gamma + yt\delta + [e, a^{x+mt}]$. Thus $I_n = E_n$ and the theorem is proved.

Since a subnear ring of a d. g. near ring need not be d. g. it is of interest to note that Corollary 2.4 of [8] shows that M_e is d. g. Moreover, $M_e^+ \cong D_{2n}$. The near ring (δ) is a zero ring whose group part is C_n. The near ring (γ) is isomorphic to $E(C_n)$, i.e. it is isomorphic to the ring $I/(n)$. Thus A_e is a commutative ring.

3. Ideals in $E(D_{2n})$

Several authors have characterized the radical of a near ring (for instance, [1] and [3]). This radical is the analogue of the Jacobson radical of ring theory and has the usual radical properties.

DEFINITION 4. A subgroup H of the near ring R is an R-subgroup if $HR \subset H$. The radical $J(R)$ is the intersection of the right ideals of R which are maximal R-subgroups.

We now find all maximal right ideals of E_n. The set of all elements of E_n of odd order, namely $(\gamma) + (\delta) + ((e, a))$, is easily seen to be a right (left) ideal of order n^3. Obviously, this is the only maximal right (left) ideal of odd order. Since this ideal is, in particular, a maximal subgroup of E_n, it is a maximal E_n-subgroup.

Let $\tau \in E_n$ be an element of order 2 not of the form (e, d) and let $\sigma \in E_n$ be an element of order 2 of the form (e, d). Then the products $\tau \cdot \sigma$ and $\sigma \cdot \tau$ each have the form (e, d) and it follows that the right (left) ideal generated by an element of order 2 must contain an element of the form $(e, a^x b)$. Let $\mu = \delta + (e, b)$. Then the right (left) ideal generated by an element of order 2 must contain

$$-\mu + (e, a^x b) + \mu = (ee \cdots e | a^{-x} b a^{2-x} b \cdots a^{(n-2)-x} b) = v.$$

In E_n the elements of order 2 form a multiplicative semigroup in which μ is an identity. We claim that v is a unit in this semigroup, that $\rho = (\delta + (e, a^x))[a^{(n+1)/2}, b] + [e, b]$ is the inverse of v. Note that

$$\rho = (ee \cdots e | a^{tx} b a^{t(x+1)} b \cdots a^{t(x+n-1)} b)$$

where $t = (n+1)/2$. In particular $(a^y b)\rho = a^{t(x+y)} b$, $0 \leqq y \leqq n-1$. For v we have that $(a^y b)v = a^{2y-x} b$. Thus

$$(a^y b)v\rho = (a^{2y-x} b)\rho = a^{t(x+2y-x)} b = a^{(n+1)y} b = a^y b$$

and

$$(a^y b)\rho v = (a^{t(x+y)} b)v = a^{2t(x+y)-x} b = a^{x+y-x} b = a^y b.$$

So μ and, consequently, each element of order 2 is in the right (left) ideal generated by an element of order 2. It follows that this ideal is $K = (\delta) + M_e$. We summarize this discussion in

THEOREM 5. *$K = (\delta) + M_e$ is the principal right (left) ideal generated by an arbitrary element of order* 2.

Recall that $(\gamma) \cong I/(n)$. Since $E_n = (\gamma) + (\delta) + M_e$ it follows that any subgroup of $(\gamma)^+$ is actually a right (but not left) ideal in E_n. Adjoining any element to K^+ is equivalent to adjoining an element of (γ) to K^+. Thus the number of non-zero even ordered right ideals of E_n is equal to the number of divisors of n. If Y^+ is a maximal subgroup of (γ), then $Y + K$ is a maximal right ideal which, automatically, is maximal as an E_n-subgroup. Each even ordered maximal right ideal of E_n is of this form. Let $n = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$. The m maximal subgroups of (γ) are given by $((ea^p a^{2p} \cdots a^{(n-1)p} | e \cdots e))$ as p ranges over the distinct prime factors of n. The intersection of all these maximal subgroups is

$$\{(ea^k a^{2k} \cdots a^{(n-1)k} | e \cdots e) | p_i | k;\ i = 1, 2, \cdots, m\}.$$

But this says that k is nilpotent in $I/(n)$ and that

$$(ea^k a^{2k} \cdots a^{(n-1)k} | e \cdots e)$$

is nilpotent in E_n. Hence the intersection is

$$((ea^w a^{2w} \cdots a^{(n-1)w}|e \cdots e)) = (\xi),$$

where $w = p_1 p_2 \cdots p_m$, and $|\xi| = n/w$. The intersection of all the maximal right ideals of even order is $K+(\xi)$ which has order $2n^3/w$. It is interesting to note that $K+(\xi)$ consists of all elements of E_n which are either nilpotent or of order 2 (the 'or' is exclusive). Intersecting $K+(\xi)$ with the ideal of order n^3, we find that $J(E_n) = (\xi)+(\delta)+((e, a))$ so that $J(E_n)$ has order n^3/w, consists of all nilpotent elements of E_n, and, as a sum of rings, is a ring.

THEOREM 6. *$E_n/J(E_n) \cong I/(q)$, where $q = 2p_1 p_2 \cdots p_m$.*

PROOF. Let H^+ be the subgroup of order n^3. Then the order of E_n^+/H^+ is prime and H^+ itself is abelian so that E_n^+ is a solvable group. By (2.2) Theorem of [2] $E_n/J(E_n)$ is a ring. But the class containing $[a, b]$ has order q in the quotient structure so that $E_n/J(E_n)$ is a ring with identity whose group part is a cyclic group of order q. Thus, by the corollary of p. 147 of [4], $E_n/J(E_n) \cong I/(q)$.

4. D. g. near rings on D_{2n}

In this section we display all non-isomorphic d. g. near rings which can be defined on the group D_{2n}. Since two binary operations on D_{2n} will be studied, the group D_{2n} will be written in additive notation in this section and the second operation will be referred to as the multiplication. One near ring of the type we seek is the zero near ring on D_{2n}, i.e. each product is 0. Unless otherwise stated, in what follows it is presumed that the near rings dealt with are not zero near rings.

Let $(D_{2n}, +, \cdot)$ be a near ring. In what follows the properties of multiplication in such a near ring are studied. Each endomorphic image of D_{2n} other than the subgroup $\{0\}$ must contain an element of order 2. Hence, in order for $d \in D_{2n}$ to be right distributive and not be a right annihilating element in the near ring $D = (D_{2n}, +, \cdot)$, $\{xd | x \in D\}$ must contain an element of order 2. But, since the near ring obeys the left distributive law, each row in the multiplication table represents an endomorphism of D^+. Since no element of order 2 can be an endomorphic image of an element of $(a)^+$, no element of $(a)^+$ can be right distributive without being a right annihilator. Thus the generating (in the d. g. near ring sense) set must contain at least one element of order 2. Let $d \in D$ be a right distributive element of order 2. Each element $xd, x \in D$, looked at from the viewpoint of the rows of the multiplication table is an endomorphic image of d and so xd is either 0 or is an element of order two. In particular, we have $ad = 0$. Since not every generating element is a right annihilator, we have for at least one d that the kernel of the endomorphism of D^+ determined by right multiplication by d is precisely $(a)^+$. Thus this endomorphism is onto a subgroup of order 2. Another way of saying this is that $fd = gd$ for any f and g of order 2 in D. In fact this condition holds for any d in the generating set, not just for d of order 2. If $d \in (a)$, $fd = 0 = gd$. Thus we see that the multiplication table row of any element of (a) consists of 0 entries and that the rows of any two elements of order 2 are identical. This row common to the elements of order 2 will be called the 2-row. Because of the additive arithmetic of D^+ and because no element of order 2 can be in the kernel of the 2-row endomorphism, it follows that the product of two elements of order 2 is an element of order 2 and that each element of order two is right distributive. Thus, without loss of generality, we may identify the generating set with the set of elements of order 2.

We proceed to determine the form of the 2-row. Let $(xa+b)(xa+b) = za+b$. Then it is also true that $(za+b)(xa+b) = za+b$. But $za+b = (za+b)(xa+b) = (za+b)(xa+b)(xa+b) = (za+b)(za+b)$ shows that an element of order 2 in the range of the 2-row endomorphism is idempotent. Now let $(xa)^2 = ya$ and let d be an idempotent element of order 2. Then $ya = d(xa) = dd(xa) = d(ya)$ and ya is fixed by the 2-row endomorphism. Since any element occurring in the 2-row is a fixed point for the endomorphism, the 2-row endomorphism is an idempotent endomorphism of D^+ and, in particular, the restriction to $(a)^+$ is an idempotent endomorphism of a cyclic group of order n.

But these last maps are determined by mapping a to ka, where k is an idempotent in $I/(n)$. As is well known, $I/(n)$ has 2^r idempotents where r is the number of distinct prime factors in the factorization of n. (An outline of the proof of this fact is given later in this section.) To finish the determination of a 2-row endomorphism, we must find the product db, d any element of order 2. Let $da = ka$ and $db = ya+b$. Then $ya+b = (ya+b)^2 = (ya+b)ya+(ya+b)b = kya+ya+b$. Thus $n|ky$. Let y be selected to satisfy this condition. Then the 2-row endomorphism has the form $[ka, ya+b]$ and $(xa+sb)[ka, ya+b] = (xk+sy)a+sb$. Moreover,

$$((xk+sy)a+sb)[ka,\ ya+b] = (k(xk+sy)+sy)a+sb = (xk+sy)a+sb,$$

so that each endomorphism satisfying the conditions on k and y has each element in its range as a fixed point.

The multiplication being defined is certainly left distributive. Consider associativity. Let $d, f, g \in D$. If $d \in (a)$ or if d has order 2 and $f \in (a)$, then $d(fg) = 0 = (df)g$. Let d and f be of order 2. Then fg is an element in the range of the 2-row endomorphism and $d(fg) = fg$. On the other hand, df is an element of order 2 as is f, so that $(df)g = fg$. So, indeed, the systems we have constructed are d. g. near rings.

Recall that the idempotents of $I/(n)$ are found two at a time by considering integers m_1, m_2 such that $m_1 m_2 = n$ and $(m_1, m_2) = 1$. For m_1 and m_2 there exist integers c_1 and c_2 such that $c_1 m_1 + c_2 m_2 = 1$. Then $c_1 m_1$ and $c_2 m_2$ are idempotents of $I/(n)$. Since $(c_1, m_2) = (c_2, m_1) = 1$, $|c_1 m_1| = m_2$ and $|c_2 m_2| = m_1$ in $I/(n)$. If, for a given m_1 and m_2, there exist c_1' and c_2' such that $c_1' m_1 + c_2' m_2 = 1$, then $c_1 m_1 \equiv c_1' m_1$ and $c_2 m_2 \equiv c_2' m_2 \pmod{n}$. Thus two 2-row endomorphisms having different values of k lead to non-isomorphic near rings since the two k's have different orders. We now show that the near rings corresponding to $[ka, y_1 a+b]$ and $[ka, y_2 a+b]$ are isomorphic. Thus, for a fixed k, we may as well use $[ka, b]$ as the 2-row endomorphism and we may say that the non-isomorphic d. g. near rings are the zero near ring and those determined by the $[ka, b]$ as k ranges over the 2^r idempotents of $I/(n)$.

Let ${}_iD = (D_{2n}, +, \cdot_i)$ be determined by $[ka, y_i a+b]$; $i = 1, 2$. To show ${}_1D \cong {}_2D$, define a map Ψ on ${}_1D$ to ${}_2D$ such that $a\Psi = a$. We also want $(y_1 a+b)\Psi = y_2 a+b$. But, having fixed a, it is seen that this is equivalent to having $b\Psi = (y_2 - y_1)a+b$. As Ψ then, take the group automorphism $[a, (y_2-y_1)a+b]$. If $d, f \in {}_1D$ and $d \in (a)$, then $(df)\Psi = 0 = (d\Psi)(f\Psi)$. If $|d| = 2$ and $f = xa$, then $(df)\Psi = kxa = (d\Psi)(f\Psi)$. If $|d| = 2$ and $f = xa+b$, then $(df)\Psi = (y_2+xk)a+b = (d\Psi)(f\Psi)$. We summarize with

THEOREM 7. *The number of non-isomorphic d. g. near rings definable on D_{2n} is $1+2^r$, where r is the number of distinct primes occurring in the factorization of n.*

5. Comments on embeddings

The theorem given in [7] has as a corollary the statement that any finite d. g. near ring can be embedded in some $E(G)$. However, certain of the d. g. near rings of the last section can be embedded in $E(G_1)$ where $|G_1|$ is much smaller than $|G|$, with G is as given in [7].

Note that $D_{2n} \oplus C_2 \cong D_{4n}$. Then Proposition 2 of [5] says that the zero near ring on D_{2n} embeds in $E(D_{4n})$. The d. g. near ring with 2-row endomorphism $[a, b]$ can be embedded in $E(D_{2n})$ by the technique of 'right multiplications' that is used in embedding a ring R with identity in $E(R^+)$. The embedding given in [6] shows, essentially, how to embed the near ring with 2-row endomorphism $[0, b]$ in $E(D_{4n})$. One wonders if each of the d. g. near rings of Section 4 can be embedded in $E(D_{4n})$.

REFERENCES

J. C. Beidleman

[1] A radical for near-ring modules, Michigan Math. J. 12 (1965), 377–383.

J. C. Beidleman

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

G. Betsch

[3] Ein Radikal für Fastringe, Math. Z. 78 (1962), 86–90.

J. R. Clay and J. J. Malone

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

H. E. Heatherly and J. J. Malone

[5] Some near-ring embeddings II, Quart. J. Math. Oxford Ser. (2) 21 (1970), 445–448.

J. D. McCracken

[6] Some results on embeddings of near rings, Master's Thesis, Texas A & M University, 1970.

J. J. Malone

[7] A near ring analogue of a ring embedding theorem, J. Algebra 16 (1970), 237–238.

J. J. Malone and C. G. Lyons

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

Oblatum 15–VI–1970

Department of Mathematics
Worcester Polytechnic Institute
Worcester, Mass., U.S.A.