Proceedings of the Edinburgh Mathematical Society (1980), 23, 69–86 ©

THE NEAR-RINGS HOSTED BY A CLASS OF GROUPS

by R. R. LAXTON AND R. LOCKHART

(Received 15th September 1975)

1. Introduction

Clay (3), Johnson (5) and Krimmel (6) have each considered the near-rings with identity on dihedral groups. Krimmel actually generalised the class of dihedral groups and investigated the class of finite non-abelian groups with a cyclic normal subgroup of prime index: we shall call this class $\mathcal{K}$. Krimmel considered the near-rings with identity that might be defined on members of $\mathcal{K}$ and he determined the subclass of groups in $\mathcal{K}$ which support near-rings of this kind. He also managed to calculate the number of non-isomorphic near-rings involved for certain cases. His methods were essentially combinatorial, and his results were expressed in terms of various integers which characterised the individual members of $\mathcal{K}$. Certain features of this work led us to investigate the structure of near-rings on members of $\mathcal{K}$ from a more algebraic point of view and thereby to complete and extend Krimmel's programme. Part of the work in this paper formed the basis of the second author's thesis (7). We should like to thank Dr. J. Krimmel for permission to include some of his results, and Dr. J. Meldrum who detected an error in our original formulation of Theorem 7.1.

1. Preliminaries

A (left) *pre-near-ring* (p.n.r.) is an additive group $(H+)$ together with a left-distributive binary operation: $a\cdot(b+c)=a\cdot b+a\cdot c$ for $a,b,c\in H$. A p.n.r. is *zero-symmetric* provided that $0\cdot H=\{0\}$. $\mathcal{P}$ is the class of non-isomorphic pre-near-rings. All our structures will be left-distributive so, to accord with this, if G is a group and $g\in G$ and n is a positive integer, we will write the sum $g+g+g+\cdots+g$ (n times) as gn (rather than the more usual ng).

A (left) *near-ring* is a p.n.r. $(H+\cdot)$ in which $(H\cdot)$ is a semi-group. $\mathcal{N}_1$ is the class of zero-symmetric near-rings with identity, $\mathcal{W}_1$ is the class of non-zero-symmetric near-rings with identity.

Suppose $(H+\cdot)\in\mathcal{P}$. The group $(H+)$ is then said to *host* the p.n.r. $(H+\cdot)$ and we write $(H+)\in Gp\langle\mathcal{P}\rangle$. If $\mathcal{C}$ is a subclass of $\mathcal{P}$, then the cardinality of the subclass of $\mathcal{C}$ consisting of those non-isomorphic p.n.r. hosted by the group $(H+)$ is called the *host number* of H in $\mathcal{C}$ and written $[H:\mathcal{C}]$. Let h be some fixed member of H and $\mathcal{C}$ some class of p.n.r. with identity elements. The cardinality of the class of non-isomorphic p.n.r. $(H+\cdot)$ which are members of $\mathcal{C}$ for which h is the identity element is called the *host number of H in $\mathcal{C}$ with identity h* and written $[H:\mathcal{C};$ with identity $h]$. Clearly $[H:\mathcal{C}]\geqslant[H:\mathcal{C};$ with identity $h]$.

https://doi.org/10.1017/S001309150000362X Published online by Cambridge University Press

Let $(H+\cdot)\in\mathcal{P}$ and suppose that θ is an automorphism of the group $(H+)$. The p.n.r. $(H+*)$ obtained by writing $a*b=(a\theta^{-1}\cdot b\theta^{-1})\theta$ is called the p.n.r. *derived* from $(H+\cdot)$ and θ. $(H+\cdot)$ and $(H+*)$ are isomorphic. They are *distinct* provided that there exist elements a, b such that $a\cdot b\neq a*b$. For any automorphism θ, $[H:\mathcal{C}$; with identity $h]=[H:\mathcal{C}$; with identity $(h)\theta]$.

Our primary interest is in near-rings, so for us pre-near-rings represent simply the first part of the problem of constructing near-rings upon a given group. However, they do arise naturally in, for example, projective geometry (4), and as matrices over near-fields (and, more generally, as matrices over any near-ring hosted by an abelian group). Ideals of p.n.r. are, of course, the kernels of p.n.r. homomorphisms. They have the same structure as ideals of near-rings. When H is zero-symmetric and J is a right ideal, then $J\cdot H\subset J$.

2. Pre-near-ring construction

Throughout this paper we will only consider finitely presented groups H with a presentation of the form

$$H=\langle x_1,\dots,x_r:R_1,R_2,\dots,R_s\rangle, \tag{2.1}$$

where $x_1,\dots,x_r$ are generators and $R_1,\dots,R_s$ are relations. We write the elements of H as words $w=w(x_1,\dots,x_r)$ in the generators $x_1,\dots,x_r$.

Suppose $h_1,\dots,h_r$ are elements of H; then $w(h_1,\dots,h_r)$ denotes the member of H obtained by replacing each occurrence of x_j in w with an occurrence of h_j.

Let $F=\langle\mathfrak{x}_1,\dots,\mathfrak{x}_r\rangle$ be the free group on the symbols $\mathfrak{x}_1,\dots,\mathfrak{x}_r$ and ϕ the epimorphism $F\to H$ defined by $\mathfrak{x}_1\phi=x_i$ for all $i=1,\dots,r$. If we write $\hat{R}_j=R_j(\mathfrak{x}_1,\dots,\mathfrak{x}_r)$ for $1\leq j\leq s$, then the normal closure N of $\langle\hat{R}_1,\dots,\hat{R}_s\rangle$ is the kernel of ϕ and $F/N\cong H$. Let $\psi:F\to H$ be a homomorphism such that $N\psi=\{0\}$. Define a mapping $\theta_1:\{x_1,\dots,x_r\}\to H$ by $(x_j)\theta_1=(\mathfrak{x}_j)\psi$ for all j; then we may extend θ_1 to a well-defined endomorphism θ: $H\to H$ such that $\psi=\phi\theta$. Conversely, all endomorphisms θ: $H\to H$ can be thought of as arising in this manner.

Definition. Let H be a group with presentation (2.1). An r-tuple $(h_1,h_2,\dots,h_r)$ of elements of H is said to satisfy the *p.n.r. construction conditions* for H if $R_j(h_1,h_2,\dots,h_r)=0$ for $1\leq j\leq s$.

The construction conditions depend on the particular presentation of H we choose to work with, and we are at liberty to select the most convenient presentation or even to use two simultaneously. It is easy to find r-tuples which satisfy the construction conditions; $(0,0,0,\dots,0)$, for instance. Our first theorem is a consequence of the simple observations we have made already.

Theorem 2.1. *Suppose that H is a group with presentation* (2.1) *and we associate with each $h\in H$ some r-tuple $(h[x_1],\dots,h[x_r])$ of elements of H which satisfies the p.n.r. construction conditions for the group H. Then the product* $(*)$ *defined on H by putting*

$$h*x_j=h[x_j]\qquad \textit{for}\qquad 1\leq j\leq r$$

https://doi.org/10.1017/S001309150000362X Published online by Cambridge University Press

and

$$h * w = w(h[x_1], \dots, h[x_r])$$

for each $w = w(x_1, \dots, x_r)$ in H, is a well-defined p.n.r. product hosted by H. All p.n.r. hosted by H arise in this manner.

The second part of this definition of product merely extends the product from the generators x_i to the whole of H; we normally omit reference to this obvious extension in applications of Theorem 2.1.

Theorem 2.1 has been found useful in connection with the problem of calculating the p.n.r. hosted by groups of low order. The theorem was used in (7) to determine the p.n.r. with identity hosted by the quaternion group of order eight. On the other hand, in the near-ring host problem, this theorem is used in conjunction with the associativity subgroup to restrict attention to the behaviour of a set of additive generators of the group in question. This usually makes the problem of calculating host numbers much more manageable.

3. The associativity subgroup

Suppose that $(H+\cdot)$ is a pre-near-ring. The subgroup $A(H) = \{h \in H : (a \cdot b) \cdot h = a \cdot (b \cdot h) \text{ for } a, b \in H\}$ is called the *associativity subgroup* of H, it is easy to check that $A(H)$ is a subgroup.

Theorem 3.1. *Suppose H is a group with presentation* (2.1) *and that $(H+\cdot) \in \mathcal{P}$. $(H+\cdot)$ is a near-ring if and only if for all $\omega, h \in H$ and $1 \leq j \leq r$, $(\omega \cdot h) \cdot x_j = \omega \cdot (h \cdot x_j)$.*

The proof of this theorem is straightforward. Notice that $(H\ \cdot)$ is associative if and only if each generator of H is in $A(H)$. Simple though it is, this result is very useful and it will be used in what follows. Of course, if $(H+\cdot)$ has an identity then it will lie inside $A(H)$.

4. The Krimmel class of groups

The class $\mathcal{K}$ consists of those groups H with a finite presentation of the form

$$H = \langle e, \mu : \mu m - ei, en, -\mu + e + \mu - ej \rangle \tag{4.1}$$

where i, j, are positive integers, $1 < j < n$, $0 \leq i < n$ and m is *prime*.

To avoid triviality we insist that $j^m \equiv 1 (\operatorname{mod} n)$ and $i(j-1) \equiv 0 (\operatorname{mod} n)$. It will be seen that each group $H \in \mathcal{K}$ has exponent n or mn. In the latter case, we apply the well-known result that the additive order of the multiplicative identity element of a finite near-ring is equal to the group exponent to see that $H \not\in Gp\langle \mathcal{N}_1 \cup \mathcal{W}_1 \rangle$. Thus we may assume that n is the exponent of H throughout the remainder of the paper.

In his thesis (6) Krimmel considered a group H with a presentation of the form (4.1) and calculated $[H : \mathcal{W}_1$; with identity $e]$, and $[H : \mathcal{N}_1$; with identity $e]$ for certain cases only. His methods were combinatorial and he worked with the exact sequence

https://doi.org/10.1017/S001309150000362X Published online by Cambridge University Press

of groups $\langle e\rangle \to H \to H/\langle e\rangle$. We will calculate the host number $[H:\mathcal{N}_1$; with identity $e]$ for all $H \in \mathcal{K}$, thus completing the project. Our methods rely upon an extensive investigation of the structures of members of $\mathcal{N}_1$ hosted by groups H in $\mathcal{K}$ and, in particular, on an exact sequence of near-rings $I \to H \twoheadrightarrow H/I$, whose construction we now describe.

In all that follows, H is a member of $\mathcal{K}$ with presentation (4.1) and exponent n.

Theorem 4.1. *Let $(H+\cdot) \in \mathcal{N}_1$ have identity e.*

(a) *There is a unique prime divisor p of n such that $\langle ep\rangle H = \langle ep\rangle$.*

(b) *The ideal $I = (0:\langle ep\rangle)$, which annihilates $\langle ep\rangle$, has order mp.*

(c) *The order of the commutator subgroup of H is p.*

Proof. (a) Let the prime decomposition of n be $p_1^{a_1}p_2^{a_2}\dots p_v^{a_v}$. If $ep_i \cdot \mu \notin \langle e\rangle$ for all i, $1 \leqslant i \leqslant v$, then by associativity it follows that $ep_1^{a_1}ep_2^{a_2}\dots ep_v^{a_v} \cdot \mu \notin \langle e\rangle$; but

$$ep_1^{a_1}ep_2^{a_2}\dots ep_v^{a_v} \cdot \mu = en \cdot \mu = 0 \in \langle e\rangle.$$

Hence there is some prime divisor p of n for which $ep \cdot \mu \in \langle e\rangle$. This means that $\langle ep\rangle \cdot H = \langle ep\rangle$. The uniqueness of p will follow from (c) proved below.

(b) Since H has order nm and $\langle ep\rangle = ep \cdot H \cong H/I$, it follows that I has order mp.

(c) This isomorphism also shows that $[H, H] \subseteq I$. But the commutator is also in $\langle e\rangle$, since $H/\langle e\rangle$ is of prime order, and so we may write $[H, H] = \langle ed\rangle$ for some d which is a divisor of n. But then $0 = ep \cdot ed = epd$, so that $pd = n$ and consequently $[H, H]$ has order p.

The commutator subgroup is of considerable importance to us in our investigations. The prime p does appear in Krimmel's work, but was not linked by him to the structure of H. Actually, Krimmel calculated $[H:\mathcal{N}_1]$ for those $H \in \mathcal{K}$ for which $m \neq p$; these are the non-nilpotent members of $\mathcal{K}$ which lie in $Gp\langle\mathcal{N}_1\rangle$. In the present paper we attend to the outstanding nilpotent cases (when $m = p$). Our theorem in (7) that if $H \in \mathcal{K}$ then

$$[H:\underline{N}_1 \cup \underline{W}_1] = [H:\underline{N}_1 \cup \underline{W}_1;\ \text{with identity } e]$$

means that our (and Krimmel's) policy of making the element e the identity of the near-ring represents no loss of generality. We shall not give the proof of this theorem here; it is lengthy though not particularly difficult. It is sufficient for our present purposes to prove this result when the group is nilpotent (see Lemma 4.7 below).

Our methods are quite different from Krimmel's. For completeness we give a short summary, an algebraic reformulation, of some of his results of (6).

Theorem 4.2. (Compare Krimmel (6), Theorem 3.1)
Let $H \in \mathcal{K}$. $H \in Gp\langle\mathcal{W}_1\rangle$ with identity e if and only if

(a) *the exact sequence $\langle e\rangle \to H \twoheadrightarrow H/\langle e\rangle$ splits,*

(b) *the commutator subgroup of H has order m,*

(c) *when $m = 2$, 4 divides $n/2$.*

If these three conditions hold, then $[H:\mathcal{W}_1] = 1$.

Theorem 4.3. (Compare Krimmel (6), Theorem 3.2)

Suppose $H \in \mathcal{K}$ is non-nilpotent. Then $H \in Gp\langle \mathcal{N}_1 \rangle$ with identity e if and only if

(a) *the exact sequence $\langle e \rangle \to H \twoheadrightarrow H/\langle e \rangle$ splits,*

(b) *the commutator subgroup has prime order $p \neq m$. If $H \in Gp\langle \mathcal{N}_1 \rangle$, then* $[H : \mathcal{N}_1] = 1$.

The above theorem has as its corollary the result that non-nilpotent dihedral groups D_n lie in $Gp\langle \mathcal{N}_1 \rangle$ if and only if $n = 2p$ where p is a odd prime and then $[D_{2p} : \mathcal{N}_1] = 1$. This theorem was also proved independently by Johnson (5). The only nilpotent dihedral host of members of $\mathcal{N}_1$ is D_4 and Clay (3) used computer methods to prove that $[D_4 : \mathcal{N}_1] = 7$. It is, in fact, possible to prove this result using the methods of this paper. To complete the story for dihedral groups, we proved in (7) that if D is the infinite dihedral group, then $[D : \mathcal{N}_1] = 1$ and $[D : \mathcal{W}_1] = 0$.

Theorem 4.4. (Compare Krimmel (6), Theorem 3.3)

Let $H \in \mathcal{K}$ be nilpotent. $H \in Gp\langle \mathcal{N}_1 \rangle$ with identity e if and only if

(a) *the exact sequence $\langle e \rangle \to H \twoheadrightarrow H/\langle e \rangle$ splits,*

(b) *the commutator subgroup of H has order m.*

The host number $[H : \mathcal{N}_1]$ remains to be calculated when H is nilpotent. We do this in this paper. We do not use any of the last three theorems, though we do find useful the following one.

Theorem 4.5. (Compare Krimmel (6), Theorem 3.4)

Let H be a nilpotent member of $\mathcal{K}$. Suppose that $(H + \cdot) \in \mathcal{N}_1$ with identity e with $n = m^a n'$ where $(m, n') = 1$. Each of $\langle em^a \rangle$ and $\langle \mu, en' \rangle$ are two-sided ideals and $(H + \cdot)$ is a direct sum of them as near-rings.

As the sub-near-ring $\langle em^a \rangle$ mentioned in 4.5 is hosted by a cyclic group, it is isomorphic to the ring of integers modulo n'. The group $\langle \mu, en' \rangle$ is actually a nilpotent member of $\mathcal{K}$ and has order m^{a+1} with $a \geq 2$. Theorem 4.5 says that the Sylow decomposition of the nilpotent group H goes over to near-rings. Thus, we need only study m-groups in $\mathcal{K}$ and do so for the rest of this paper. Such groups have a presentation of the form

$$H = \langle e, \mu : em^a, \mu m, -\mu + e + \mu - e(1 + m^{a-1}) \rangle, \ m \ a \text{ prime}, \ a \geq 2. \tag{4.2}$$

We will assume always that $m + a > 4$, since the case $m + a = 4$ is the dihedral group D_4 already considered by Clay (3). The following is immediate:

Lemma 4.6. *The order of H is m^{a+1} and $\langle em^{a-1} \rangle$ lies in the group centre. The exponent of H is m^a and elements of H can be written uniquely in the form $\mu r + es$ where $0 \leq r < m$ and $0 \leq s < m^a$. For any integer l,*

$$(\mu r + es)l = \mu rl + es\{l + rm^{a-1}l(l-1)/2\}.$$

Next follows the result we mentioned earlier (see above, Theorem 4.2):

https://doi.org/10.1017/S001309150000362X Published online by Cambridge University Press

Lemma 4.7. $[H:\mathcal{N}_1]=[H:\mathcal{N}_1;$ *with identity* $e]$.

Proof. The only candidates for the identity of a near-ring are those elements of H with order equal to the group exponent. We will prove that all such elements are images of e under appropriate automorphisms of H. Consequently it follows that each member of $\mathcal{N}_1$ hosted by H will be derived from some near-ring with e as identity.

Let $h\in H$ have order m^a. We can assume $h\not\in\langle e\rangle$ so we may write $h=\mu r+es$. Now $(\mu r+es)m=es(2+2^{a-1}r)$ for $m=2$ and $(\mu r+es)m=esm$ for $m\neq 2$. So a necessary and sufficient condition that $\mu r+es$ has order m^a is that $(s,m)=1$. Because $1\leqslant r<m$, we have $\mu\not\in\langle\mu r+es\rangle$ and therefore there is an automorphism Φ of H such that $e\Phi=\mu r+es$ and $\mu\Phi=\mu$ when $(s,m)=1$.

As we have explained earlier, this lemma permits us to restrict our efforts towards defining near-ring products on H which have identity e. Finally we note

Lemma 4.8. *The p.n.r. construction conditions for a p.n.r. hosted by H with e as a right identity are that for all* $h\in H$

(a) $h\cdot e=h$,

(b) $(h\cdot\mu)m=0$,

and

(c) $-(h\cdot\mu)+h+(h\cdot\mu)=h(1+m^{a-1})$.

5. The structure of near-rings hosted by *m*-groups in $\mathcal{K}$

Throughout this section $(H+\cdot)$ is a zero-symmetric near-ring hosted by the group $(H+)$ with presentation (4.2) and identity e. We shall investigate the structure of $(H+\cdot)$.

Lemma 5.1. *The annihilator ideal* $I=(0:\langle em\rangle)$ *is not cyclic if m is odd. We may assume that* $I=\langle\mu+e2^{a-2}\rangle$ *in cyclic cases and* $I=\langle\mu,em^{a-1}\rangle$ *otherwise.*

Proof. I has order m^2 and so is either a cyclic group or a direct product of two cyclic groups. We know that I contains a member of the coset $\{\mu+\langle e\rangle\}$ so when I is not cyclic we can assume that $I=\langle\mu,em^{a-1}\rangle$. If I is cyclic then $em\cdot\mu=e\lambda m^{a-1}$ where $1\leqslant\lambda<m$, so I is generated by $\mu-e\lambda m^{a-2}$. Take $0\leqslant s<m^a$, $0\leqslant r<m$ and put $(\mu r+es)\cdot(\mu-e\lambda m^{a-2})=(\mu-e\lambda m^{a-2})g$ for some $0\leqslant g<m^2$. $(\mu-e\lambda m^{a-2})m=-e\lambda m^{a-1}$, so $(\mu r+es)\cdot(-e\lambda m^{a-1})=-e\lambda m^{a-1}g$ and thus $s\equiv g(\operatorname{mod} m)$.

Also $-(\mu-e\lambda m^{a-2})+e+(\mu-e\lambda m^{a-2})=e(1+m^{a-1})$, therefore $-(\mu-e\lambda m^{a-2})g+\mu r+es+(\mu-e\lambda m^{a-2})g=(\mu r+es)(1+m^{a-1})$, which reduces to the congruence $sg\equiv s$ $(\operatorname{mod} m)$.

The two congruences modulo m express the distributivity in the near-ring (and correspond to the p.n.r. construction conditions). For them to hold simultaneously for arbitrary s in the range given we must have $m=2$. But if $m=2$, then $\lambda=1$ and $(\mu-e\lambda m^{a-2})3=\mu+e2^{a-2}$, which generates I.

We introduce the following notation.

(a) σ,τ are integers and A,B,C members of the annihilator ideal I in H.

(b) We write $\overline{\sigma\tau} \equiv \sigma\tau \pmod{m^{a-1}}$, and $\sigma\tau \equiv \overline{\overline{\sigma\tau}} \pmod{m^{a}}$, where $0 \leqslant \overline{\sigma\tau} < m^{a-1}$ and $0 \leqslant \overline{\overline{\sigma\tau}} < m^{a}$, and put $\mathfrak{M}(\sigma, \tau) = \overline{\overline{\sigma\tau}} - \overline{\sigma\tau}$.

(c) We write (σ, A, B) for $(e\bar{\sigma} + A) \cdot B$.

(d) Finally, the symbol y is μ when $I = \langle \mu, em^{a-1} \rangle$ and $\mu + e2^{a-2}$ when $I = \langle \mu + e2^{a-2} \rangle$.

We begin by deriving various properties of (σ, A, B). The following result expresses the associativity law in the near-ring $(H + \cdot)$.

Lemma 5.2. $(\sigma, A, (\tau, B, C)) = (\sigma\tau, e\mathfrak{M}(\bar{\sigma}, \bar{\tau}) + [e\sigma, -A]\,\tau(\tau - 1)/2 + A\tau + (\sigma, A, B), C)$, *where* $[e\sigma, -A] = -e\bar{\sigma} + A + e\bar{\sigma} - A$.

Proof. It is proved by first establishing

$$(e\bar{\sigma} + A) \cdot (e\bar{\tau} + B) = e\overline{\sigma\tau} + e\mathfrak{M}(\bar{\sigma}, \bar{\tau}) + [e\bar{\sigma}, -A]\bar{\tau}(\bar{\tau} - 1)/2 + A\bar{\tau} + (\bar{\sigma}, A, B) \quad (5.1)$$

and then selecting an integer γ and expanding $(e\bar{\sigma} + A) \cdot (e\bar{\tau} + B) \cdot (e\bar{\gamma} + C)$ in two ways.

Lemma 5.3. *If I is not cyclic and $(\sigma, \mu r + esm^{a-1}, \mu) = \mu l + ek$, then $k \equiv 0 \pmod{m^{a-1}}$ and $\sigma l \equiv \sigma \pmod{m}$.*

Proof. Lemma 4.8(b) implies $k \equiv 0 \pmod{m^{a-1}}$. Since $e\bar{\sigma} + \mu r + esm^{a-1} = \mu r + e\bar{\sigma}(1 + rm^{a-1}) + esm^{a-1}$, we may apply 4.8(c) to obtain

$$-\mu l + \mu r + e\bar{\sigma}(1 + rm^{a-1}) + esm^{a-1} + \mu l = \mu r + e\bar{\sigma}(1 + rm^{a-1}) + esm^{a-1} + e\bar{\sigma}m^{a-1}l.$$

This reduces to the required congruence.

Corollary. *If I is not cyclic and $(\sigma, m) = 1$ then $(\sigma, A, \mu) = \mu + ekm^{a-1}$ for some $0 \leqslant k < m$.*

Lemma 5.4. *If I is cyclic and $(\sigma, A, \mu + e2^{a-2}) = (\mu + e2^{a-2})k$ for some $0 \leqslant k < 4$, then $k \equiv \sigma \pmod{2}$.*

Proof. $(e\bar{\sigma} + A) \cdot (\mu + e2^{a-2})2 = (\mu + e2^{a-2})k2$ reduces to the required congruence.

The following lemma is a simple consequence of our assumptions and definitions.

Lemma 5.5. (a) $(1, 0, A) = A$,
(b) $(sm, 0, A) = (sm, ekm^{a-1}, A) = 0$ *for all integers s and k,*
(c) $(\sigma, A, B + C) = (\sigma, A, B) + (\sigma, A, C)$,
(d) $(\sigma, A, ekm^{a-1}) = e\sigma km^{a-1}$.

Lemma 5.6. (a) $(\sigma, A, (1, ekm^{a-1}, y)) = (\sigma, A + e\sigma km^{a-1}, y)$,
(b) $(\sigma, A, (1, B, y)) = (\sigma, A + (\sigma, A, B), y)$.

Proof. We merely apply Lemmas 5.2 and 5.5.

Lemma 5.7. *If $\sigma \equiv 0 \pmod{m}$, then $(\sigma, A, y) \in \langle em^{a-1} \rangle$.*

https://doi.org/10.1017/S001309150000362X Published online by Cambridge University Press

Proof. 5.4 covers the cyclic case. In the non-cyclic case 5.5(b) permits us to restrict our attention to the situation in which $A \not\in \langle em^{a-1}\rangle$. Thus, put $A = \mu\omega + esm^{a-1}$ with $1 \leqslant \omega < m$. Suppose $(\sigma, A, \mu) = \mu r + ekm^{a-1}$ with $1 \leqslant r < m$. We may choose $1 \leqslant v < m$ such that $rv \equiv -\omega \pmod m$. By the corollary to Lemma 5.3, $(1, \mu v, \mu) = \mu + etm^{a-1}$. Therefore,

$$\begin{aligned}(\sigma, A, \mu) &= (\sigma, A, \mu + etm^{a-1}), \text{ by Lemma 5.5,}\\ &= (\sigma, A, (1, \mu v, \mu)) = (\sigma, A + (\sigma, A, \mu v), \mu), \text{ by Lemma 5.2,}\\ &= (\sigma, \mu(\omega + rv) + e(s + kv)m^{a-1}, \mu) = 0, \text{ by Lemma 5.5.}\end{aligned}$$

Lemma 5.8. *If* $\sigma \equiv 0 \pmod m$, *then for all integers* s $(\sigma, A + esm^{a-1}, y) = (\sigma, A, Y)$.

Proof. We write $(\sigma, A, y) = elm^{a-1}$ and observe from Lemmas 5.3 and 5.4 that $(1, B, y) \not\in \langle em^{a-1}\rangle$. Now, $(\sigma, A, y) = (\sigma, A, (1, B, y)) = (\sigma, A + (\sigma, A, B), y)$.

First suppose $l \not\equiv 0 \pmod m$, Choose $1 \leqslant r < m$ such that $lr \equiv 1 \pmod m$ and on putting $B = yr$ we obtain $(\sigma, A, y) = (\sigma, A + em^{a-1}, y)$.

Now suppose $l \equiv 0 \pmod m$. If, contrary to our claim, $(\sigma, A + esm^{a-1}, y) \neq 0$ for some s, we could put $A' = A + esm^{a-1}$ and apply our first supposition to obtain a contradiction.

Notation. An integer $\bar{\sigma}$ $(0 < \bar{\sigma} < m^{a-1})$ will be written in the form $\bar{\sigma} = m^s q$ where $1 \leqslant q < m^{a-1-s}$ with $(q, m) = 1$ and $0 \leqslant s \leqslant a - 2$.

Lemma 5.9. *Let* $1 \leqslant q < m^{a-1-s}, (q, m) = 1, 1 \leqslant s \leqslant a - 2$. *If* $0 \leqslant r < m$, *then* $(m^s, yr, y) = (m^s q, yrq, y)$.

Proof. We use Lemmas 5.2, 5.3, 5.4 and 5.5 to obtain $(m^s, yr, y) = (m^s, yr, (q, y, y)) = (m^s q, yrq + (m^s, yr, y), y) = (m^s q, yrq, y)$, with this last equality coming from Lemma 5.8.

Lemma 5.10. *If* $(m^s, yr, y) = ekm^{a-1}$, *then* $(m^s q, yr, y) = ekqm^{a-1}$, $s \geqslant 1$.

Proof. $ekqm^{a-1} = (q, y, ekm^{a-1}) = (q, y, (m^s, yr, y)) = (qm^s, (q, y, yr), y)$. Since $(q, y, yr) \in \{yr + \langle em^{a-1}\rangle\}$, it follows that $(qm^s, yr, y) = ekqm^{a-1}$, as required.

Lemma 5.11. *Suppose* $(m^s, y, y) = ekm^{a-1}$ *and* $0 < q < m$. *Then* $(m^s, yq, y) = etm^{a-1}$, *where* $k \equiv qt \pmod m$.

Proof. If $m = 2$, then $q = 1$ and the result is obvious. If $m > 2$, then $(m^s q, \mu q, \mu) = ekm^{a-1}$, by 5.9. Hence Lemma 5.10 implies that $k \equiv qt \pmod m$.

Lemma 5.12. *If* $m \neq 2$, *then* $(0, \mu r, \mu) = 0$ *for all* $0 \leqslant r < m$.

Proof. We write $(0, \mu r, \mu) = ekm^{a-1}$ and fix $0 < q < m$. Then $ekqm^{a-1} =$

$(q, A, (0, \mu r, \mu)) = (0, (q, A, \mu r), \mu) = (0, \mu r, \mu) = ekm^{a-1}$. Thus the congruence $kq \equiv k \pmod{m}$ is valid for all $0 < q < m$, which implies that $k \equiv 0 \pmod{m}$ when $m \neq 2$.

Lemma 5.13. (a) *If* $rk \equiv 1 \pmod{m}$, *then*

$$(r, A, (1, ekm^{a-1}, y)) = (r, A + em^{a-1}, y).$$

(b) *If the ideal* I *is non-cyclic, then*

$$(1, esm^{a-1}, \mu) = (1, em^{a-1}, \mu s) - \mu(s-1) \textit{ for } 0 < s < m.$$

Proof. For (a) observe that $(r, A, (1, ekm^{a-1}, y)) = (r, A + erkm^{a-1}, y)$, whilst for (b) $(1, em^{a-1}, (1, em^{a-1}, \mu)) = (1, em^{a-1} + em^{a-1}, \mu)$. The result then follows by induction.

Lemma 5.14. *If* $m = 2$, *then* $(1, e2^{a-1}, y) = y$.

Proof. By an appeal to Lemmas 5.3 and 5.4 we have only to show that $(1, e2^{a-1}, y) \neq y + e2^{a-1}$.

(1) Suppose that $(1, y, y) = y + e2^{a-1}$ and $(1, e2^{a-1}, y) = y + e2^{a-1}$. Then $(1, e2^{a-1}, y) = (1, e2^{a-1}, (1, y, y) + e2^{a-1}) = (1, e2^{a-1} + (1, e2^{a-1}, y), y) + e2^{a-1} = (1, y, y) + e2^{a-1} = y$.

(2) Now suppose that $(1, y, y) = y$ and $(1, e2^{a-1}, y) = y + e2^{a-1}$. Then $(1, e2^{a-1}, y) = (1, e2^{a-1}, (1, y, y)) = (1, e2^{a-1} + (1, e2^{a-1}, y), y) = (1, y, y) = y$.

Lemma 5.15. *If* $m = 2$, *then* $(\sigma, A + e2^{a-1}, y) = (\sigma, A, y)$.

Proof. 5.8 permits us to assume that $\sigma \equiv 1 \pmod{2}$. But then $(\sigma, A, y) = (\sigma, A, (1, e2^{a-1}, y)) = (\sigma, A + e2^{a-1}, y)$.

From elementary number theory we recall the fact that each of the 2^{a-2} units of the ring of integers modulo 2^{a-1} is of the form $\mp(5^s) \pmod{2^{a-1}}$ for some unique $0 < s \leq 2^{a-3}$.

Lemma 5.16. *Let* $m = 2$. *Suppose* $\sigma \equiv 1 \pmod{2}$, $(5, 0, y) = y + ek2^{a-1}$, *and* $(-5, 0, y) = y + el2^{a-1}$, *where* $0 \leq l, k < 2$. *Then*

(a) $(\sigma, 0, y) = y$ *when* $\sigma \equiv 1 \pmod{8}$.

(b) $(\sigma, 0, y) = y + ek2^{a-1}$ *when* $\sigma \equiv 5 \pmod{8}$.

(c) $(\sigma, 0, y) = y + el2^{a-1}$ *when* $\sigma \equiv 3 \pmod{8}$.

(d) $(\sigma, 0, y) = y + e(l+k)2^{a-1}$ *when* $\sigma \equiv 7 \pmod{8}$.

Proof. When $a = 3$, $\bar{5} = 1$ and the result is obvious. We therefore assume $a \geq 4$. $(5^2, 0, y) = (5, 0, (5, 0, y)) = y$. If s is some positive integer, $(5^{s-1}, 0, (5, 0, y)) = (5^s, 0, y)$ and, using Lemma 5.15, induction on s proves that $(5^s, 0, y) = y$ if $s \equiv 0 \pmod{2}$, but $(5^s, 0, y) = y + ek2^{a-1}$ if $s \equiv 1 \pmod{2}$. This proves (a) and (b). (c) and (d) are proved in a similar way.

https://doi.org/10.1017/S001309150000362X Published online by Cambridge University Press

Lemma 5.17. *Let $m = 2$. Suppose $\sigma \equiv 1 \pmod 2$ and $(1, y, y) = y + et2^{a-1}$. Then $(\sigma, y, y) = (\sigma, 0, y) + et2^{a-1}$.*

Proof. This is immediate, since $(\sigma, y, y) = (\sigma, (\sigma, 0, y), y) = (\sigma, 0, (1, y, y)) = (\sigma, 0, y) + et2^{a-1}$.

In what follows π is to be a primitive root modulo m^2, with $1 < \pi < m$, when m is an odd prime. Thus for all positive integers b, π generates all the units modulo m^s.

Lemma 5.18. *Let m be an odd prime. Suppose r, s are positive integers and $0 \leq s < m$. Then $(r, A + esm^{a-1}, \mu) = (r, A, \mu)$.*

Proof. $r \equiv 0 \pmod m$ is catered for by 5.8, so we can assume that $r \not\equiv 0 \pmod m$. Put $(\pi, 0, \mu) = \mu + ekm^{a-1}$, as we may by the corollary to 5.3; then $(\pi^2, e\mathfrak{M}(\pi, \pi), \mu) = (\pi, 0, (\pi, 0, \mu)) = \mu + ekm^{a-1} + ek\pi m^{a-1}$. $[e\overline{\pi^2}, -e\mathfrak{M}(\pi, \pi)] = 0$, therefore Lemma 5.2 gives $(\pi^3, e\mathfrak{M}(\overline{\pi^2}, \pi) + e\mathfrak{M}(\pi, \pi)\pi, \mu) = (\pi^2, e\mathfrak{M}(\pi, \pi), (\pi, 0, \mu)) = \mu + ekm^{a-1} + ek\pi m^{a-1} + ek\pi^2 m^{a-1}$. By a simple induction, we obtain our basic equality,

$$(\pi^s, e\mathfrak{M}(\overline{\pi^{s-1}}, \pi) + e\mathfrak{M}(\overline{\pi^{s-2}}, \pi)\pi + \cdots + e\mathfrak{M}(\bar{\pi}, \pi)\pi^{s-2}, \mu)$$
$$= \mu + ekm^{a-1}(1 + \pi + \pi^2 + \cdots + \pi^{s-1}).$$

But $\mathfrak{M}(\overline{\pi^{s-i}}, \pi)\pi^{i-1} = (\overline{\pi^{s-i}} \cdot \pi - \overline{\pi^{s-i+1}})\pi^{i-1}$, so $e\mathfrak{M}(\overline{\pi^{s-1}}, \pi)\pi^{i-1} = e(\overline{\pi^{s-i}} \cdot \pi - \overline{\pi^{s-i+1}})\pi^{i-1}$; hence $e(\Sigma_{i=1}^{s-1} \mathfrak{M}(\overline{\pi^{s-1}}, \pi)\pi^i) = e(\pi^s - \overline{\pi^s})$. Accordingly, we amend the basic equality to obtain

$$(\pi^s, e(\pi^s - \overline{\pi^s}), \mu) = \mu + em^{a-1}k(\pi^s - 1)/(\pi - 1). \tag{5.2}$$

Fix $\phi = \phi(m^{a-1}) = m^{a-2}(m-1)$ and observe that because π is a primitive root modulo m^a, $\pi^\phi \not\equiv 1 \pmod{m^a}$, although $\pi^\phi \equiv 1 \pmod{m^{a-1}}$. Thus $e\,\Sigma_{i=1}^{\phi-1} \mathfrak{M}(\overline{\pi^{\phi-i}}, \pi)\pi^{i-1} = e(\pi^\phi - 1) \neq 0$, so we may write $e(\pi^\phi - 1) = e\psi m^{a-1}$ with $0 < \psi < m$. $\pi^\phi \equiv 1 \pmod m$ thus $em^{a-1}(\pi^\phi - 1)/(\pi - 1) = 0$, and putting $s = \phi$ in 5.2 gives us $(1, e\psi m^{a-1}, \mu) = \mu$.

If we write $(1, em^{a-1}, \mu) = \mu + eum^{a-1}$ for some $0 \leq u < m$, we can use 5.13(b) to obtain $(1, e\psi m^{a-1}, \mu) = \mu + eu\psi m^{a-1}$, which implies $u = 0$. We know now that $(1, etm^{a-1}, \mu) = \mu$ for all $0 \leq t < m$. If $0 < s < m$ we can choose $0 < t < m$ so that $rt \equiv s \pmod m$, then

$$(r, A, \mu) = (r, A, (1, etm^{a-1}, \mu)) = (r, A + ertm^{a-1}, \mu) = (r, A + esm^{a-1}, \mu).$$

This completes the proof.

Lemma 5.19. $(\sigma, A, (\tau, B, C)) = (\sigma\tau, A\tau + (\sigma, A, B), C)$.

This relationship is the basic expression of the near-ring associativity law. It follows from Lemma 5.2 together with 5.15 when $m = 2$ and 5.18 when $m \neq 2$. The following result is immediate.

Lemma 5.20. *Let m be an odd prime. Then $(1, \mu r, \mu) = (1, \mu, \mu r) - \mu(r-1)$. If $\sigma \not\equiv 0 \pmod m$ then $(\sigma, 0, (1, \mu r, \mu)) = (\sigma, \mu r, \mu)$.*

Lemma 5.21. *If $m > 3$, then*
(a) $(\pi, \mu, \mu) = (\pi, 0, \mu)$,
(b) $(1, \mu, \mu) = \mu$,
(c) *when* $\sigma \not\equiv 0 \pmod{m}$, $(\sigma, \mu, \mu) = (\sigma, 0, \mu)$.

Proof. Put $(\pi, 0, \mu) = \mu + ekm^{a-1}$, $(\pi, \mu, \mu) = \mu + e\psi m^{a-1}$, $(1, \mu, \mu) = \mu + etm^{a-1}$, where $0 \leq k, t, \psi < m$. $(\pi, \mu, \mu) = (\pi, 0, (1, \mu, \mu)) = \mu + e(k + \pi t)m^{a-1}$, so $\psi \equiv k + t\pi \pmod{m}$.

Now $(\pi^2, \mu\pi + \mu, \mu) = (\pi, \mu, (\pi, \mu, \mu))$, so induction on s gives $(\pi^s, \mu(\pi^s - 1)/(\pi - 1), \mu) = \mu + e\psi m^{a-1}(\pi^s - 1)/(\pi - 1)$. Yet $(\pi^s - 1)/(\pi - 1) \equiv 0 \pmod{m}$ if and only if $s \equiv 0 \pmod{m-1}$. (5.2) gives $(\pi^s, 0, \mu) = \mu + em^{a-1}k(\pi^s - 1)/(\pi - 1)$. If ω is integral, $(\pi^s, \mu\omega, \mu) = (\pi^s, 0, (1, \mu\omega, \mu)) = (\pi^s, 0, (1, \mu, \mu\omega) - \mu(\omega - 1)) = (\pi^s, 0, \mu + et\omega m^{a-1})$. So the substitution $\omega = (\pi^s - 1)/(\pi - 1)$ gives $\mu + e\psi m^{a-1}(\pi^s - 1)/(\pi - 1) = \mu + em^{a-1}k(\pi^s - 1)/(\pi - 1) + etm^{a-1}\pi^s(\pi^s - 1)/(\pi - 1)$. From which we conclude, $\psi(\pi^s - 1)/(\pi - 1) \equiv (k + t\pi^s)(\pi^s - 1)/(\pi - 1) \pmod{m}$. We substitute the value $s = 2$ and note that $s \not\equiv 0 (\bmod\ m - 1)$ thus, $k + t\pi \equiv \psi \equiv k + t\pi^2 \pmod{m}$. This means that $t = 0$ and $\psi = k$. Lastly, $(\sigma, 0, \mu) = (\sigma, 0, (1, \mu, \mu)) = (\sigma, \mu, \mu)$ and this completes the proof.

Corollary. *If $m = 3$ and k, ψ, t, are as in the proof of* 5.20, *then $\pi = 2$ and* $\psi \equiv k + 2t \pmod{3}$.

Definition. Suppose H is a group with presentation (4.2) and y is a fixed element of H defined by: $y = \mu$ if $m \neq 2$ and $y = \mu$ or $y = \mu + e2^{a-2}$ otherwise. Let I be the subgroup $\langle y, em^{a-1} \rangle$. A mapping $[\,,\,]: Z_{m^{a-1}} \times I \times I \to I$ is a *triple* if for some integers $k, l, t, \omega, v(1), \ldots v(a-2)$ in $[0, m-1]$, the following conditions hold.

(1) If $m = 2$ $[5, 0, y] = y + ek2^{a-1}$ and $k = 0$ if $a = 3$.
(2) If $m \neq 2$ $[\pi, 0, y] = y + ekm^{a-1}$ where π is a primitive root.
(3) If $m = 2$ $[-5, 0, y] = y + el2^{a-1}$.
(4) $[1, y, y] = y + etm^{a-1}$ and $t = 0$ if $m > 3$.
(5) For any integer r in $[1, m-1]$, $[0, yr, y] = e\omega m^{a-1}$ and $\omega = 0$ if $m \neq 2$.
(6) $[\sigma, A, 0] = 0$.
(7) If $\sigma \equiv 0 (\bmod\ m)$ then $[\sigma, 0, A] = 0$.
(8) $[\sigma, A, em^{a-1}] = e\sigma m^{a-1}$.
(9) If $1 \leq s \leq a-2$ then $[m^s, y, y] = ev(s)m^{a-1}$.
(10) For any integer r in $[1, m-1]$, if $\sigma = m^s q$ where $1 \leq q < m^{a-1-s}$, $(m, q) = 1$ and $1 \leq s \leq a-2$ then $[\sigma, yr, y] = ezqm^{a-1}$ where $v(s) \equiv rz \pmod{m}$.
(11) If $m = 2$ and $\sigma \equiv 1 \pmod{2}$ then,
 (a) $[\sigma, 0, y] = y$ when $\sigma \equiv 1 \pmod{8}$,
 (b) $[\sigma, 0, y] = y + ek2^{a-1}$ when $\sigma \equiv 5 \pmod{8}$,
 (c) $[\sigma, 0, y] = y + el2^{a-1}$ when $\sigma \equiv 3 \pmod{8}$,
 (d) $[\sigma, 0, y] = y + e(l + k)2^{a-1}$ when $\sigma \equiv 7 \pmod{8}$.
(12) If $m \neq 2$ and $1 \leq s < m^{a-2}(m-1)$ then $[\pi^s, 0, y] = y + em^{a-1}k(\pi^s - 1)/(\pi - 1)$.
(13) If $\sigma \not\equiv 0 \pmod{m}$ then for all integers r $[\sigma, yr, y] = [\sigma, 0, y] + e\sigma rtm^{a-1}$.
(14) $[\sigma, A + em^{a-1}, B] = [\sigma, A, B]$.
(15) $[\sigma, A, B + C] = [\sigma, A, B] + [\sigma, A, C]$.

https://doi.org/10.1017/S001309150000362X Published online by Cambridge University Press

Theorem 5.22. *Let $(H+)$ be a group with presentation (4.2) and suppose $(H+\cdot)$ is a zero-symmetric near-ring with identity e. Then, the annihilator of $\langle em\rangle$ is an ideal $I=\langle y, em^{a-1}\rangle$, where y may be taken as μ when $m\neq 2$ and either as μ or as $\mu+e2^{a-2}$ when $m=2$. Elements of H may be uniquely written in the form $e\sigma+A$ where $0\leqslant\sigma<m^{a-1}$ and $A\in I$; and the product $(\cdot)$ on H is given by the equation*:

$$(e\sigma+A)\cdot(e\tau+B)=e\sigma\tau+[e\sigma,-A]\tau(\tau-1)/2+A\tau+[\sigma,A,B]$$

where $[\,,\,]$ is a triple.

Our result simply sums up the work of this section. Conditions (1), (2),. . . . . . . (15) in the definition of a triple come from the lemmas we have proved by putting $[\sigma, A, B]=[\sigma, A, B]$ for all σ, A, B.

6. Near-rings

Theorem 6.1. *Let H be a group with presentation $H=\langle e,\mu : em^{a}, \mu m, -\mu+e+\mu-e(1+m^{a-1})\rangle$ where m is prime and $a\geqslant 2$. Define an element y in H by fixing $y=\mu$ if $m\neq 2$ and $y=\mu$ or $y=\mu+e2^{a-2}$ otherwise. Let $I=\langle y, em^{a-1}\rangle$. Elements of H can be uniquely expressed in the form $e\sigma+A$ where $0\leqslant\sigma<m^{a-1}$ and $A\in I$ with $0\leqslant\sigma,\tau<m^{a-1}$ and $A, B\in I$. The product $(\cdot)$ defined on H by*

$(e\sigma+A)\cdot(e\tau+B)=e\sigma\tau+[e\sigma,-A]\tau(\tau-1)/2+A\tau+[\sigma,A,B]$, is a zero-symmetric near-ring product with identity e, provided that $[\,,\,]$ is a triple.

Proof. It is readily apparent from the definition of a triple that our product is zero-symmetric and has identity e. As to verifying that it is indeed a pre-near-ring, we turn to Lemma 4.8. for all cases in which $y=\mu$. Condition (a) is immediate. Condition (b) follows from points (1), (2), (3), (4), (5), (7), (9), (10), (11), (12), (13) of the definition of a triple. Condition (c) requires that for all $0\leqslant\sigma<m^{a-1}$ and $A\in I$ (putting $\tau=0$ and $B=\mu$)

$$-[\sigma,A,\mu]+e\sigma+A+[\sigma,A,\mu]=(e\sigma+A)(1+m^{a-1}).$$

When $\sigma\equiv 0 \pmod m$ the definition of a triple means that $[\sigma, A,\mu]$ is in the centre of $(H+)$ and so

$$-[\sigma,A,\mu]+e\sigma+A+[e\sigma+A]=e\sigma+A=(e\sigma+A)(1+m^{a-1}).$$

When $\sigma\not\equiv 0 \pmod m$, $[\sigma,A,\mu]=\mu+e\psi m^{a-1}$ for some integer ψ in $[0, m-1]$. Condition (c) now is $-\mu+e\sigma+A+\mu=(e\sigma+A)(1+m^{a-1})$ which is seen to be true in the group H (A has order m).

To complete the proof of distributivity we simply note that if, as we may, we write $e\tau+B$ the form $e\gamma+\mu r$ where $0\leqslant\gamma<m^{a}$ and $0\leqslant r<m$, then the definition of our product and points (15) and (8) of the triple definition ensure that

$$(e\sigma+A)\cdot(e\tau+B)=(e\sigma+A)\cdot(e\gamma+\mu r)=(e\sigma+A)\gamma+[\sigma,A,\mu]r.$$

The distributivity of our defined product in the case $y=\mu+e2^{a-2}$ may be

https://doi.org/10.1017/S001309150000362X Published online by Cambridge University Press

established in similar fashion. Thus, we have proved that the product makes $(H+\cdot)$ a pre-near-ring for each triple.

Now we complete the proof of Theorem 6.1 by showing that the product is associative.

We need to consider four distinct cases:

(a) the case $m=2$ and $a=3$, (b) the case $m=2$ and $a>3$, (c) the case $m=3$, (d) the case $m>3$.

We will avoid excessive repetition if we treat cases (b) and (c) only; the proofs for the other two cases are similar and simpler in places.

Case (b) with $m=2$ and $a>3$.

We let $(H+\cdot)$ be one of the p.n.r. products under examination. The associativity subgroup $A(H)$ already contains e so we can achieve our aim by proving $y\in A(H)$. We choose to do this for $y=\mu+e2^{a-2}$; the other, non-cyclic, case is the same.

We need to verify that for $0\leqslant\sigma,\tau<2^{a-1}$ and $A,B\in\langle\mu+e2^{a-2}\rangle$ $((e\sigma+A)\cdot(e\tau+B))\cdot(\mu+e2^{a-2})=(e\sigma+A)\cdot((e\tau+B)\cdot(\mu+e2^{a-2}))$.
By the definition of a triple this becomes

$$[\sigma\tau, A\tau+[\sigma,A,B],\mu+e2^{a-2}]=[\sigma,A,[\tau,B,\mu+e2^{a-2}]]. \tag{6.1}$$

We shall verify this equality by treating different cases.

(i) $\sigma\equiv\tau\equiv 0 \pmod 2$.

$$[\tau,B,\mu+e2^{a-2}]\in\langle e2^{a-1}\rangle \text{ so } [\sigma,A,[\tau,B,\mu+e2^{a-2}]]=0.$$

$\sigma\tau\equiv 0 \pmod 2$ and $A\tau+[\sigma,A,B]\in\langle e2^{a-1}\rangle$ thus

$$[\sigma\tau,A\tau+[\sigma,A,B],\mu+e2^{a-2}]=0 \text{ also.}$$

(ii) $\sigma\equiv 1 \pmod 2$ and $\tau\equiv 0 \pmod 2$.

Assume $\tau\neq 0$ and put $\tau=2^sq$ with $(q,2)=1$, $1\leqslant q<2^{a-1-s}$ and $1\leqslant s\leqslant a-2$. Now $[\tau,B,\mu+e2^{a-2}]=0$ if $B\in\langle e2^{a-1}\rangle$ whilst $[\tau,B,\mu+e2^{a-2}]=ev(s)2^{a-1}$ if $B\notin\langle e2^{a-1}\rangle$. $\sigma\tau\equiv 0 \pmod 2$ and $\overline{\sigma\tau}\neq 0$. Also, $A\tau\in\langle e2^{a-1}\rangle$, consequently $A\tau+[\sigma,A,B]\in\langle e2^{a-1}\rangle$ if and only if $B\in\langle e2^{a-1}\rangle$. Thus if $B\in\langle e2^{a-1}\rangle$, then $[\sigma\tau,A\tau+[\sigma,A,B],\mu+e2^{a-2}]=0$ and (6.1) follows. On the other hand, if $B\notin\langle e2^{a-1}\rangle$, $[\sigma,A,B]\notin\langle e2^{a-1}\rangle$ and $[\sigma\tau,A\tau+[\sigma,A,B],\mu+e2^{a-2}]=[\sigma\tau,\mu+e2^{a-2},\mu+e2^{a-2}]=ev(s)2^{a-1}=[\sigma,A,ev(s)2^{a-1}]=[\sigma,A,[\tau,B,\mu+e2^{a-2}]]$.

Now assume that $\tau=0$. A direct inspection of (6.1) (and in particular conditions (6), (7) and (14) of the definition of a triple permits us to discharge as trivial all cases in which $B\in\langle e2^{a-1}\rangle$. When $B\notin\langle e2^{a-1}\rangle$, we have $[\tau,B,\mu+e2^{a-2}]=e\omega 2^{a-1}$ so that $[\sigma,A,[\tau,B,\mu+e2^{a-2}]]=e\omega 2^{a-1}$. We know $\overline{\sigma\tau}=0$, so $[\sigma\tau,A\tau+[\sigma,A,B],\mu+e2^{a-2}]=[0,[\sigma,A,\mu+e2^{a-2}],\ \mu+e2^{a-2}]=[0,\mu+e2^{a-2},\mu+e2^{a-2}]=e\omega 2^{a-1}$. Hence once again (6.1) is shown to be valid.

(iii) $\sigma\equiv 0 \pmod 2$ and $\tau\equiv 1 \pmod 2$.

$[\tau,B,\mu+e2^{a-2}]\notin e2^{a-1}$, thus $[\sigma,A,[\tau,B,\mu+e2^{a-2}]]=[\sigma,A,\mu+e2^{a-2}]=[\sigma\tau,A,\mu+e2^{a-2}]$ (by condition 10 of the definition of a triple) $=[\sigma\tau,A\tau+[\sigma,A,B],\mu+e2^{a-2}]$.

(iv) $\sigma\tau\equiv 1 \pmod 2$.

This is the hardest case to prove. We split it into four sub-cases which correspond to various values for A and B.

(a) $A, B \in \langle e2^{a-1}\rangle$.

From (6.1) and condition (14) of a triple we have to verify

$$[\sigma\tau, 0, \mu + e2^{a-2}] = [\sigma, 0, [\tau, 0, \mu + e2^{a-2}]].$$

We may write $[\sigma, 0, \mu + e2^{a-2}] = \mu + e2^{a-2} + e\chi 2^{a-1}$ and $[\tau, 0, \mu + e2^{a-2}] = \mu + e2^{a-2} + e\psi 2^{a-1}$, with χ and ψ depending on the congruence classes of σ and τ modulo 8. $[\sigma, 0, [\tau, 0, \mu + e2^{a-2}]] = \mu + e2^{a-2} + e(\chi + \psi)2^{a-1}$ so we must show that this is the value of $[\sigma\tau, 0, \mu + e2^{a-2}]$. Now its value depends only on the congruence class of $\sigma\tau$ modulo 8. When $\sigma \equiv 1 \pmod 8$ $\chi = 0$ and $\sigma\tau \equiv \tau \pmod 8$, which means that $[\sigma\tau, 0, \mu + e2^{a-2}] = [\tau, 0, \mu + e2^{a-2}] = \mu + e2^{a-2} + e\psi 2^{a-1}$. The same is true when $\tau \equiv 1 \pmod 8$ (when $\psi = 0$).

The multiplicative group of units in the ring of integers modulo 8 is isomorphic to the Klein group. Thus, whenever $\sigma \equiv \tau \pmod 8$, $\sigma\tau \equiv 1 \pmod 8$ and $\chi = \psi$, so $[\sigma\tau, 0, \mu + e2^{a-2}] = \mu + e2^{a-2} = \mu + e2^{a-2} + e(\chi + \psi)2^{a-1}$. If σ and τ are distinct modulo 8 and neither is congruent to 1, $\sigma\tau$ is distinct from each of them and from 1. We appeal to point (11) of the condition for triples to see that wherever P, Q, R are pairwise distinct members of $\{3, 5, 7\}$

$$[P, 0, \mu + e2^{a-2}] + [Q, 0, \mu + e2^{a-2}] = [R, 0, \mu + e2^{a-2}] + \mu + e2^{a-2}.$$

In consequence of this $[\sigma, 0, \mu + e2^{a-2}] + [\tau, 0, \mu + e2^{a-2}] = [\sigma\tau, 0, \mu + e2^{a-2}] + \mu + e2^{a-2}$ and $[\sigma, 0, [\tau, 0, \mu + e2^{a-2}]] = [\sigma, 0, \mu + e2^{a-2}] + [\tau, 0, \mu + e2^{a-2}] + (\mu + e2^{a-2}) + e2^{a-1} = [\sigma\tau, 0, \mu + e2^{a-2}]$.

(b) $A \in \langle e2^{a-1}\rangle$ but $B \notin \langle e2^{a-1}\rangle$.

The form of (6.1) to be checked is now

$$[\sigma\tau, \mu + e2^{a-2}, \mu + e2^{a-2}] = [\sigma, 0, [\tau, \mu + e2^{a-2}, \mu + e2^{a-2}]].$$

Applying condition (13), $[\sigma\tau, \mu + e2^{a-2}, \mu + e2^{a-2}] = [\sigma\tau, 0, \mu + e2^{a-2}] + et2^{a-1} = [\sigma, 0, [\tau, 0, \mu + e2^{a-2}] + et2^{a-1}] = [\sigma, 0, [\tau, \mu + e2^{a-2}, \mu + e2^{a-2}]]$, as required.

(c) $A \notin \langle e2^{a-1}\rangle$ but $B \in \langle e2^{a-1}\rangle$.

This time we must show that

$$[\sigma\tau, \mu + e2^{a-2}, \mu + e2^{a-2}] = [\sigma, \mu + e2^{a-2}, [\tau, 0, \mu + e2^{a-2}]].$$

But $[\sigma\tau, \mu + e2^{a-2}, \mu + e2^{a-2}] = [\sigma\tau, 0, \mu + e2^{a-2}] + et2^{a-1} = [\sigma, 0, [\tau, 0, \mu + e2^{a-2}]] + et2^{a-1} = [\sigma, \mu + e2^{a-2}, [\tau, 0, \mu + e2^{a-2}]]$, again as required.

(d) $A \notin \langle e2^{a-1}\rangle$ and $B \notin \langle e2^{a-1}\rangle$.

The relation to be verified here is

$$[\sigma\tau, 0, \mu + e2^{a-2}] = [\sigma, \mu + e2^{a-2}, [\tau, \mu + e2^{a-2}, \mu + e2^{a-2}]].$$

But $[\sigma, \mu + e2^{a-2}, [\tau, \mu + e2^{a-2}, \mu + e2^{a-2}]] = [\sigma, \mu + e2^{a-2}, [\tau, 0, \mu + e2^{a-2}]] + e\sigma t2^{a-1} = [\sigma, 0, [\tau, 0, \mu + e2^{a-2}]] + e2t \cdot 2^{a-1} = [\sigma, 0, [\tau, 0, \mu + e2^{a-2}]]$.

This completes the proof for $m = 2, a > 3$. A slight variant of this proves the non-cyclic case also.

https://doi.org/10.1017/S001309150000362X Published online by Cambridge University Press

Case (c) with $m = 3$.

Let $(H+\cdot)$ represent one of the 3^a distinct p.n.r. which can be formed using the conditions for a triple. Once again $e \in A(H)$, but this time we show that $\mu \in A(H)$ that is

$$((e\sigma + A)\cdot(e\tau + B))\cdot\mu = (e\sigma + A)\cdot((e\tau + B)\cdot\mu)$$

This reduces to the relation

$$[\sigma\tau, A\tau + [\sigma, A, B], \mu] = [\sigma, A, [\tau, B, \mu]]. \tag{6.2}$$

Again we must consider cases

(i) $\sigma \equiv 0 \equiv \tau \pmod 3$.

Now $\sigma\tau \equiv 0 \pmod 3$, so $[\sigma\tau, A\tau + [\sigma, A, B], \mu] = [\sigma\tau, 0, \mu] = 0$. $[\tau, B, \mu] \in \langle e3^{a-1}\rangle$ whence $[\sigma, A, [\tau, B, \mu]] = 0$.

(ii) $\sigma \equiv 0 \pmod 3$ and $\tau \not\equiv 0 \pmod 3$.

Since $[\sigma, A, B] \in \langle e3^{a-1}\rangle$ we need only prove that

$$[\sigma\tau, A\tau, \mu] = [\sigma, A, [\tau, B, \mu]].$$

Condition (7) for a triple proves this for $A \in \langle e3^{a-1}\rangle$, and when $\sigma = 0$ we may invoke condition (5). Thus we put $A = \mu r + e\chi 3^{a-1}$ with $0 < r < 3$, $0 \leqslant \chi < 3$, and $\sigma = 3^s q$ with $1 \leqslant s \leqslant a-2$, $(3, q) = 1$, $1 \leqslant q < 3^{a-1-s}$. We do know that $[\sigma, A, [\tau, B, \mu]] = [\sigma, A, \mu] = e\omega q 3^{a-1}$ where $v(s) \equiv \omega r$ (mod 3]. $\overline{\sigma\tau} = 3^s g$ for some $1 \leqslant g < 3^{a-1-s}$ with $(3, g) = 1$; whence: $[\sigma\tau, A\tau, \mu] = [3^s g, \mu r\tau, \mu] = ezg3^{a-1}$, where $v(s) \equiv zr\tau \pmod 3$, so $\omega \equiv z\tau \pmod 3$. But then $[\sigma\tau, A\tau, \mu] = ezg3^{a-1} = ezg3^{a-1-s}3^s g = ez3^{a-1-s}\overline{\sigma\tau} = ez3^{a-1}\tau q = e\omega q 3^{a-1} = [\sigma, A, [\tau, B, \mu]]$.

(iii) $\sigma \not\equiv 0 \pmod 3$ and $\tau \equiv 0 \pmod 3$.

We need to establish the following form:

$$[\sigma\tau, [\sigma, A, B], \mu] = [\sigma, A, [\tau, B, \mu]],$$

of (6.2). The relation clearly is true when $B \in \langle e3^{a-1}\rangle$. Accordingly, put $B = \mu r + e\chi 3^{a-1}$ with $0 < r < 3$. Triviality is avoided by assuming $\tau = 3^s q$ where $1 \leqslant q < 3^{a-1-s}$, $(3, q) = 1$, $1 \leqslant s \leqslant a-2$. $[\tau, B, \mu] = e\omega q 3^{a-1}$ and $v(s) \equiv \omega r \pmod 3$. $[\sigma, A, [\tau, B, \mu]] = e\sigma\omega q 3^{a-1}$, At the same time, $[\sigma\tau, [\sigma, A, B], \mu] = [\sigma\tau, \mu r, \mu] = e\sigma q z 3^{a-1}$, where $v(s) \equiv zr$. This means that $z \equiv \omega \pmod 3$ and the equality is established.

(iv) $\sigma\tau \not\equiv 0 \pmod 3$.

Again it is the last case which gives us the biggest problem, forcing us to consider sub-cases. We shall write $\sigma \equiv \pi^s \pmod{3^{a-1}}$, $\tau \equiv \pi^u \pmod{3^{a-1}}$, with $1 \leqslant s, u \leqslant 2 \cdot 3^{a-2}$. Of course $\pi = 2$, since $m = 3$.

(a) $A, B \in \langle e3^{a-1}\rangle$.

By condition (14) for a triple (6.2) now reduces to

$$[\sigma, 0, [\tau, 0, \mu]] = [\sigma\tau, 0, \mu].$$

Now $[\sigma, 0, \mu] = \mu + ek(2^s - 1)3^{a-1}$ from Condition (12). $[\sigma, 0, [\tau, 0, \mu]] = \mu + ek(2^s - 1)3^{a-1} + e\sigma k 3^{a-1}(2^u - 1) = \mu + ek(2^s - 1)3^{a-1} + ek2^s(2^u - 1)3^{a-1} = \mu + ek3^{a-1}(2^{s+u} - 1)$. $\sigma\tau \equiv 2^{s+u} \pmod{3^{a-1}}$ and so $[\sigma\tau, 0, \mu] = \mu + ek(2^{s+u} - 1)3^{a-1}$. (Note the possibility that $s + u > e^{a-2}2$.)

https://doi.org/10.1017/S001309150000362X Published online by Cambridge University Press

(b) $A \in \langle e3^{a-1} \rangle$ and $B \not\in \langle e3^{a-1} \rangle$.

Then $B = \mu r + e\chi 3^{a-1}$ for some $0 < r < 3$. The form of (6.2) we need to verify is:

$$[\sigma\tau, \mu r, \mu] = [\sigma, 0, [\tau, \mu r, \mu]].$$

Now $[\tau, \mu r, \mu] = [\pi^u, \mu r, \mu] = \mu + ek3^{a-1}(2^u - 1) + e2^u rt3^{a-1}$ and so $[\sigma, 0, [\tau, \mu r, \mu]] = \mu + ek3^{a-1}(2^{s+u} - 1) + e2^{u+s}3^{a-1}rt$. But also $[\sigma\tau, \mu r, \mu] = [2^{s+u}, \mu r, \mu] = \mu + ek3^{a-1}(2^{s+u} - 1) + ert3^{a-1}2^{s+u}$.

(c) $A \not\in \langle e3^{a-1} \rangle$ and $B \in \langle e3^{a-1} \rangle$.

Now we write $A = \mu r + e\chi 3^{a-1}$ with $0 < r < 3$ and prove the equivalent

$$[\sigma\tau, \mu r\tau, \mu] = [\sigma, \mu r, [\tau, 0, \mu]].$$

Now $[\sigma, \mu r, [\tau, 0, \mu]] = \mu + e2^s rt3^{a-1} - ek3^{a-1} + ek3^{a-1}2^{s+u}$. $[\sigma\tau, \mu r\tau, \mu] \equiv [2^{s+u}, \mu r2^u, \mu] = \mu + ek3^{a-1}2^{s+u} - ek3^{a-1} + ert2^{s+u}3^{a-1}2^u = \mu + ek3^{a-1}2^{s+u} - ek3^{a-1} + ert2^s3^{a-1}$.
$ert\, 2^{s+u}3^{a-1}2^u = \mu + ek3^{a-1}2^{s+u} - ek3^{a-1} + ert2^s3^{a-1}$.

(d) $A \not\in \langle e3^{a-1} \rangle$ and $B \not\in \langle e3^{a-1} \rangle$.

Put $A = \mu r + e\chi 3^{a-1}$, $B = \mu g + ez3^{a-1}$ with $0 < r, g < 3$. It is enough for us to prove that

$$[\sigma, \mu r, [\tau, \mu g, \mu]] = [\sigma\tau, \mu r\tau + [\sigma, \mu r, \mu g], \mu],$$

and this is verified by direct substitution.

This completes the proof of the theorem.

It is straightforward to show that the subgroup $I = \langle y, em^{a-1} \rangle$ defined in the statement of the theorem is, in fact, the annihilating ideal of $\langle em \rangle$.

7. Host numbers

In this section we complete the project started by John Krimmel in (6). Throughout H is a group in $\mathscr{K}$ with the presentation (4.2) and (a), (b), (c), (d) refer to the four subcases considered in the proof of Theorem 6.1.

Theorem 7.1.
(i) *Case* (a). *If* $m = 2$ *and* $a = 3$, *then* $[H : \mathcal{N}_1] = 32$.
(ii) *Case* (b). *If* $m = 2$ *and* $a > 3$, *then* $[H : \mathcal{N}_1] = 2^{a+3}$.
(iii) *Case* (c). *If* $m = 3$, *then* $[H : \mathcal{N}_1] = 3^{a-1}$.
(iv) *Case* (d). *If* $m > 3$, *then* $[H : \mathcal{N}_1] = m^{a-2}$.

Proof. In consequence of 6.1, each allocation of values to the unknowns appearing in the conditions of the definition of a triple results in a zero-symmetric near-ring product with identity e hosted by H. Of course, by Theorem 4.7 there are no members of $\mathcal{N}_1$ hosted by H which do not arise in this way (up to isomorphism). In (a), when $m = 2$ and $a = 3$, there are 16 distinct near-rings which arise in this fashion in each of the cyclic and non-cyclic cases. Our theorem is completed by utilising our knowledge of the automorphisms of H which fix e to show that no two of the 32 distinct near-rings arising can be isomorphic (see a similar argument below). Similar arguments apply in case (b), where there are 2^{a+3} near-rings to be considered (that is: 2^{a+2} ways of assigning value to each of: $k, l, t, \omega, v(1), \ldots, v(a-2)$ in each of the cyclic and non-cyclic cases).

We will now consider (c) and (d) in more detail. Values must be affixed to $k, t, v(1), \ldots, v(a-2)$ in such a manner that these are non-negative integers less than m, and $t=0$ when $m \neq 3$. There are 3^a ways of doing this if $m=3$, and m^{a-1} ways otherwise. Automorphisms Φ of H which fix e satisfy the following: $-(\mu\Phi)+e+\mu\Phi = e(1+m^{a-1})$, $(\mu\Phi)m = 0$. Thus $\mu\Phi = \mu + egm^{a-1}$ and to avoid triviality, restrict g to the range $1 \leq g < m$.

Suppose that $(H+\cdot)$ and $(H+*)$ are distinct near-rings (see Section 1 for the definition of distinct near-rings). We may write: $e\pi \cdot \mu = \mu + ek_1m^{a-1}$, $(e+\mu)\cdot\mu = \mu + et_1m^{a-1}$, $(em^s+\mu)\cdot\mu = ev_1(s)m^{a-1}$ for $1 \leq s \leq a-2$; $e\pi*\mu = \mu + ek_2m^{a-1}$, $(e+\mu)*\mu = \mu + et_2m^{a-1}$, $(em^s+\mu)*\mu = ev_2(s)m^{a-1}$ for $1 \leq s \leq a-2$. If $(H+*)$ is derived from $(H+\cdot)$ and Φ, then for all $x, y \in H$, $(x\Phi)*(y\Phi) = (x\cdot y)\Phi$. In this way, we obtain the congruences

$$k_1 \equiv k_2 + g(\pi - 1) \pmod{m},$$
$$t_2 \equiv t_1 \pmod{m}$$

and

$$v_2(s) \equiv v_1(s) \pmod{m} \ (1 \leq s \leq a-2),$$

where π is a primitive root (mod m) as defined after Lemma 5.17.

Thus $(H+\cdot)$ and $(H+*)$ will be isomorphic if and only if $t_2 = t_1$ and $v_2(s) = v_1(s)$ for $1 \leq s \leq a-2$. When $m=3$ it follows that there are 3^{a-1} non-isomorphic members of $\mathcal{N}_1$ hosted by H; these correspond to the distinct possible choices for: $t, v(1), v(2), \ldots, v(a-2)$. When $m>3$ there are m^{a-2} distinct choices for $v(1), \ldots, v(a-2)$, so that $[H:\mathcal{N}_1] = m^{a-2}$.

8. Generalisations

Various particular generalisations of the presentation (4.1) can be made, and it seems that the work in this paper is still at least partially applicable to these generalisations. In (7) we considered groups similar to those defined in (4.1) except that m is allowed to be a square-free integer, rather than prime. Also we considered Abelian groups with cyclic subgroups of prime index. Neither generalisation was completed in (7), although some progress was made.

REFERENCES

(1) G. Betsch, Primitive Near-Rings, *Math. Z.* **130** (1973), 351–361.

(2) J. R. Clay, The Near-Rings on Groups of Low Order, *Math. Z.* **104** (1968), 364–371.

(3) J. R. Clay, Research into Near-Ring Theory using a digital computer, *B.I.T.* **104** 10 (1970), 249–265.

(4) M. Hall, *The Theory of Groups* (Macmillan, 1973).

(5) M. JOHNSON, Near-Rings with identities on Dihedral Groups, *Proc. Edinburgh Math. Soc.* (2) **18** (1973), 219–228.

(6) *Conditions on Near-Rings with identity and the near-ring with identity on some metacyclic groups* (Doctoral dissertation, Univ. of Arizona, Tucson, 1972).

(7) R. LOCKHART, *Near-Rings on a class of Groups* (Doctoral dissertation, Univ. of Nottingham, 1977).

UNIVERSITY OF NOTTINGHAM

https://doi.org/10.1017/S001309150000362X Published online by Cambridge University Press