Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume 15 **(2013)**. Number 2. pp. 237 – 268

The p–gen nature of $M_0(V)$ (I)

Stuart D. Scott

Communicated by G. Pilz

Abstract. Let V be a finite group (not elementary two) and $p \geq 5$ a prime. The question as to when the nearring $M_0(V)$ of all zero–fixing self-maps on V is generated by a unit of order p is difficult. In this paper we show $M_0(V)$ is so generated if and only if V does not belong to one of three finite disjoint families $\mathcal{D}^{\#}(1,p)$ $(=\mathcal{D}(1,p) \cup \{\{0\}\})$, $\mathcal{D}(2,p)$ and $\mathcal{D}(3,p)$ of groups, where $\mathcal{D}(n,p)$ are those groups G (not elementary two) with $|G| \leq np$ and $\delta(G) > (n-1)p$ (see [1] or §.1 for the definition of $\delta(G)$).

1. Introduction

Throughout this paper nearrings will be taken as zero–symmetric and left distributive. This will mean functions are written on the right. Unless indicated otherwise all nearrings will have an identity. Also groups other than automorphism groups and groups of units will be written additively. This convention is not taken as implying the groups are abelian.

If V is a group then $M_0(V)$ is the nearring of all zero–fixing self–maps of V. These structures are called transformation nearrings. Associated with an element α of $M_0(V)$ is the subnearring $N(\alpha)$ (with or without identity) of $M_0(V)$ generated by α and it is a question of considerable interest as to when α with special properties can generate $M_0(V)$ (ie. is such that $N(\alpha) = M_0(V)$).

Addressing the question as to when any α in $M_0(V)$ generates $M_0(V)$ when V is infinite, is not difficult. Here because $N(\alpha)$ is countable and $M_0(V)$ is not, there are no such elements. So straight away we may assume

2010 MSC: 16Y30.
Key words and phrases: nearring, unit, cycles (p-cycles), fixed–point–free, p–gen.

V is finite (an assumption adopted from now on). However, there are other restrictions that the $N(\alpha) = M_0(V)$ requirement imposes. If for example an element of $M_0(V)$ is not bijective (ie. not a unit of $M_0(V)$), then in no way can it generate $M_0(V)$. This is because if β in $M_0(V)$ is such that $a\beta = b\beta$ (a and b distinct elements of V), then all γ in $M_0(V)$ with $a\gamma = b\gamma$ is a proper subnearring (without identity) containing β.

The requirement that α in $M_0(V)$ is such that $N(\alpha) = M_0(V)$, implies V is finite and α belongs to the group (under composition) $u(M_0(V))$ of all units of $M_0(V)$. So what further sensible restrictions can be placed on α and it still generate $M_0(V)$? In broad terms there is only one property of elements of $u(M_0(V))$ that springs to mind. As $u(M_0(V))$ is the full symmetric group on V^* (the non–zero elements of V) the order (under composition) of an α in $u(M_0(V))$ is surely its dominant feature. Thus for any given integer $n \geq 2$, the question as to when the nearring involved is generated by a unit α of order n is (in the case of $M_0(V)$), at the heart of generation investigations. An $M_0(V)$ so generated will be called n–gen. It is the purpose of this paper to give a complete answer as to when $M_0(V)$ (V not elementary two) is p–gen (p a prime).

In [4] and [5] the problem of when $M_0(V)$ is p–gen was completely solved for $p = 2$ and 3. The main theorem of [4] was that $M_0(V)$ is 2–gen if and only if V is not a C_3 (cyclic group of order three) or an elementary two group, while the main theorem of [5] was that $M_0(V)$ is 3–gen if and only if V is not a C_3, an S_3 (symmetric group of order six) or an elementary two group of order incongruent to 1 *mod* 3 (apart from $\{0\}$ and $C_2 \oplus C_2$). This paper will deal with primes ≥ 5 in the case of V not elementary two. The elementary two case presents special problems, and is dealt with in a separate paper which is called 'The p–gen Nature of $M_0(V)$ (II)'.

We now move towards the statement of the theorem this paper proves. If V is a group then $\delta(V)$ will be the number of minimal subgroups of V (ie. the number of subgroups of V of prime order). This group invariant was investigated in [1], where its importance for deciding which $M_0(V)$ are p–gen was explained. The fact that we know what groups V have $\delta(V) > \frac{1}{2}|V| - 1$ is significant. It means that given a prime p (≥ 5 say) and group V there is theory available that tells us if $M_0(V)$ is p–gen. To state the theorem this paper proves, we define finite disjoint families $\mathcal{D}(n,p), n = 1, 2, \ldots$ of groups as follows. A group G is in $\mathcal{D}(n,p)$ if, it is not elementary two, $|G| \leq np$ and $\delta(G) > (n-1)p$. With $\mathcal{D}^{\#}(1,p)$ as $\mathcal{D}(1,p) \cup \{\{0\}\}$ we have:-

Theorem 1.1. If V is a group (not elementary two) and $p \geq 5$ a prime, then $M_0(V)$ is p–gen if and only if, V does not belong to any of the three mutually exclusive classes $\mathcal{D}^{\#}(1,p)$, $\mathcal{D}(2,p)$ or $\mathcal{D}(3,p)$.

2. Some group theory

This section develops group notation and theory that will be required later. Because most theory that we cover tends to be quite well known, proofs are nearly always omitted (references are of course supplied). This should make the paper more self contained.

As indicated in the previous section groups being dealt with are finite. A feature of developments is that groups of odd order remain very much in the background. Given this fact, it might be expected that the involutions of a group V (non–zero elements v of V such that $v + v = 0$) play a prominent role. In a real enough sense, this is true. It is mainly the subset $\eta(V)$ of V of all such elements that figures. Indeed we shall often need to look at $|\eta(V)|$ (the order of a subset S of V is denoted by $|S|$). Also the subset $i(V) = \eta(V) \cup \{0\}$ of V will on occasions, also enter. The subset $\tau(V) = V^* \backslash \eta(V)$ (here if S is a subset of V, S^* denotes $S \backslash \{0\}$) consisting of all elements of order > 2, will come into play. One useful fact about the subset $\tau(V)$ of V is that it can be partitioned into two element subsets $\{h, -h\}$ $(h \in \tau(V))$ of V. This has the consequence that:-

Proposition 2.1. For a group V of even order $|\tau(V)|$ is even and $|\eta(V)|$ is odd.

Another more indirect consequence of the above partitioning is that:-

Proposition 2.2. If V is a group and S a subset of $\tau(V)$ of non-zero order $2n$ (or $2n+1$) where $n \geq 0$ is an integer, then S contains a subset K of order n (of order $n+1$) not containing any H^* with H a non–zero subgroup of V.

Proof. Certainly S can be written as a union of disjoint two element subsets and a subset S_1 of elements of S without additive inverses in S. A subset K_1 of S containing one element of each two element subset and S_1 has no element with additive inverse in K_1 and 2.2 readily follows.

Corollary 2.3. The K of 2.2 can be taken to have order $\leq n$ (when $|S| = 2n$ and order $\leq n+1$ (when $|S| = 2n+1$), simply by taking a new K contained in the K of 2.2.

Above information on $\tau(V)$ (V a group) is basic, but there is one result to do with $\eta(V)$ (thus $\tau(V)$ also) which we need and has far more

substance. For our purposes it is of value to know what groups V have $|\eta(V)| > \frac{1}{2}|V| - 1$. There are four families of such groups (type (I) to (IV)) that are now specified. As stated below a theorem due to C.T.C.Wall tells us that a group V with $|\eta(V)| > \frac{1}{2}|V| - 1$ is of type (I) to (IV).

Groups of type (I) are simply the generalised dihedral groups. Such a V is an abelian group A extended semidirectly by an element of order two which, under conjugation additively inverts elements of A. Here V is denoted by $D(A)$ and is only abelian (in fact elementary two) if A is elementary two. These are also the groups V where the characteristic subgroup $\lambda(V)$ of V generated by $\tau(V)$ is $< V$. Indeed it is easy to show that if such a V is not abelian (in fact not elementary two) then $\lambda(V) = A$ (V being a $D(A)$). A special case of a $D(A)$ is where A is a cyclic group C_n of order n. These are the dihedral groups which we denote by D_n. They have order $2n$. A group of the form $\langle a, b\rangle$ with a and b both involutions is one of them.

The order of $\eta(V)$ (V a $D(A)$) reduces to knowing what $|\eta(A)|$ is.

Proposition 2.4. If V is of the form $D(A)$ (A not elementary two) then $|\eta(V)| = \frac{1}{2}|V| + |\eta(A)|$.

Groups of type (II) are those of the form $D_4 \oplus D_4 \oplus E$, where E is elementary two. Here we have.

Proposition 2.5. A group V of type (II) has $|\eta(V)| = \frac{9}{16}|V| - 1$ (see [4]).

Groups of type (III) are of the form $H(r) \oplus E$ (E elementary two and $r \geq 1$ an integer) where $H(r)$ is the direct sum of r copies of D_4 where the central subgroup consisting of a direct sum of $r - 1$ copies of C_2 that identifies the centers has been factored out so that $Z(H(r))$ is a C_2. If $V = H(r) \oplus E$ where E has order 2^n, then $|V| = 2^{2r+n+1}$ and $|\eta(V)| = |V|/2 + 2^{n+r} - 1$ (see [6] or [1]). The only overlap between (I) and (III) occurs when $r = 1$. Here $|\eta(V)| = \frac{3}{4}|V| - 1$ while for $r = 2$ or ≥ 3 the above value of $|\eta(V)|$ gives.

Proposition 2.6. A group $V = H(r) \oplus E$ of type (III) has $|\eta(V)| = \frac{5}{8}|V| - 1$ when $r = 2$ and $|\eta(V)| \leq \frac{9}{16}|V| - 1$ where $r \geq 3$.

Groups of type (IV) are of the form $S(r) \oplus E$ (E elementary two of order 2^n and $r \geq 1$ an integer) where $S(r)$ is the direct sum of r copies of $C_2 \oplus C_2$ extended semidirectly by a C_2 which is a wreath product (ie. D_4) on each $C_2 \oplus C_2$ component. Again we have the only overlap between (I) and (III) with (IV) is $r = 1$ where $|\eta(V)| = \frac{3}{4}|V| - 1$. In general $|V| = 2^{2r+n+1}$ and $|\eta(V)| = |V|/2 + 2^{n+r} - 1$ (see [6] or [1]) so that as for type (III) we have:-

Proposition 2.7. A group $V = S(r) \oplus E$ of type (IV) has $|\eta(V)| = \frac{5}{8}|V| - 1$ when $r = 2$ and $|\eta(V)| \leq \frac{9}{16}|V| - 1$ where $r \geq 3$.

The theorem of C.T.C.Wall (see [6]) that was mentioned above states.

Theorem 2.8. (Wall) If V is a group with $|\eta(V)| > \frac{1}{2}|V| - 1$, then V is of type (I) to (IV).

Before leaving this section we need some information about fixed–point–free automorphisms. Such an automorphism μ (of a group V) is defined by the property that $v\mu \neq v$ for all non–zero v of V. When μ also has prime order q certain things happen. One is that a subset S of V^* with $S\mu = S$ has order divisible by q. Another is that when $q = 2$, V is necessarily abelian (see [2, Ch.10]). Stated as a proposition:-

Proposition 2.9. If the group V has a fixed–point–free automorphism μ of order two, then V is abelian and $v\mu = -v$ for all v in V.

In the case of q being a larger prime quite a lot can still be said about the structure of V. A fundamental theorem due to Thompson (see [2, Ch.10]) states:-

Theorem 2.10. (Thompson) If the group V has a fixed–point–free automorphism of prime order, then V is nilpotent

3. Elements of $M_0(V)$

In this section we cover notation and elementary theory about elements of $M_0(V)$ that will assist with developments of sections that follow.

If V is a group and α an element of $M_0(V)$, then an element v of V^* is said to be moved by α if $v\alpha \neq v$, otherwise v in V^* is said to be fixed by α. The set of all v in V^* moved (fixed) by α is denoted by $M(\alpha)$ (by $F(\alpha)$). Two elements α_1 and α_2 of $M_0(V)$ are said to be disjoint if $M(\alpha_1) \cap M(\alpha_2) = \emptyset$.

There are certain elements of $u(M_0(V))$ that will play a prominent role in what follows. These are the cycles. If $n \geq 2$ is an integer and $a_1, \ldots, a_n$, n elements of V^* then $[a_1, \ldots, a_n]$ will denote the element of $u(M_0(V))$ that fixes elements of $V^* \backslash \{a_1, \ldots, a_n\}$ (of course 0 goes to 0), takes a_i to a_{i+1} for $i = 1, \ldots, n-1$, and takes a_n to a_1. It is called a cycle (more descriptively an n–cycle on V). As a unit of $M_0(V)$ it has order n (ie. $[a_1, \ldots, a_n]^n = 1$ and n is the smallest integer with this property). It is clear that if $\alpha = [a_1, \ldots, a_n]$ then $M(\alpha) = \{a_1, \ldots, a_n\}$ and $F(\alpha) = V^* \backslash \{a_1, \ldots, a_n\}$. Disjoint cycles will be important. Here $\alpha_1 = [b_1, \ldots, b_r]$ and $\alpha_2 = [c_1, \ldots, c_s]$ are disjoint (see above) if $\{b_1, \ldots, b_r\} \cap \{c_1, \ldots, c_s\}$

is empty. Also k cycles $\beta_1, \ldots, \beta_k$, of $u(M_0(V))$ are mutually disjoint if every two element subset of the set $\{\beta_1, \ldots, \beta_k\}$ is disjoint. The product $\beta_1\beta_2 \ldots \beta_k$ of mutually disjoint β_i may be rearranged in any way as β_i and β_j (i and j in $\{1, \ldots, k\}$) commute. Also the order of this element of $u(M_0(V))$ is the l.c.m of the orders of the $\beta_i,\ i = 1, \ldots, k$.

The notion of disjoint cycles is important when dealing with a unit α of $M_0(V)$ of order p (p a prime). This is because α can be expressed uniquely (apart from rearrangement) as a product $\alpha_1\alpha_2 \ldots \alpha_k$ of mutually disjoint p–cycles $\alpha_i,\ i = 1, \ldots, k$, on V. In this regard, there is a feature that subgroups of V may have relative to α when slightly more information on the α_i is given. How things go here is now covered. We call a subgroup H of V with $H\alpha \subseteq H,\ \alpha$–invariant. In the situation where V has no non–zero proper α–invariant subgroups we say α confuses proper subgroups of V. The useful feature that certain α in $u(M_0(V))$ of order p have is as follows:-

Lemma 3.1. Suppose V is a group, p a prime and $n \geq 2$ an integer. If $|V| > np$ and $g_1, \ldots, g_{np}$ are np elements of V^*, then

$$\alpha = [g_1, \ldots, g_p][g_{p+1}, \ldots, g_{2p}] \ldots [g_{(n-1)p+1}, \ldots, g_{np}]$$

is a unit of $M_0(V)$ of order p, and if $g_{sp} = -g_{sp+1}$, for $s = 1, \ldots, n-1$, then any α–invariant subgroup H of V such that $H \cap \{g_1, \ldots, g_{np}\} \neq \emptyset$ necessarily contains $\{g_1, \ldots, g_{np}\}$.

Proof. The cycles used to define α are disjoint. Since $M(\alpha)$ in non–empty (ie. $\alpha \neq 1$) it follows from above that α has order p. If some g_i is in H, then g_i is in $\{g_{rp+1}, \ldots, g_{(r+1)p}\}$, where r is one of $\{0, \ldots, n-1\}$. Now, $H[g_{rp+1}, \ldots, g_{(r+1)p}]^k$ ($k \geq 1$ an integer) is contained in H. Thus all of $\{g_{rp+1}, \ldots, g_{(r+1)p}\}$ is contained in H, and if $r \geq 1$, then $-g_{rp+1}$ (ie. g_{rp}) is in H. This in turn means, $\{g_{(r-1)p+1}, \ldots, g_{rp}\}$ must be contained in H. Continuing in this way we see $\{g_{kp+1}, \ldots, g_{(k+1)p}\} \subseteq H$ where $0 \leq k \leq r$. A reasonably similar argument shows $\{g_{kp+1}, \ldots, g_{(k+1)p}\} \subseteq H$ whenever $r \leq k \leq n-1$ so that 3.1 holds.

For a group V with $\alpha = \alpha_1\alpha_2 \ldots \alpha_k$ ($k \geq 1$ an integer) an element of $u(M_0(V))$ of order p, where the α_i, $i = 1, \ldots, k$, are mutually disjoint p-cycles, we seek information on an automorphism μ of V such that $\alpha\mu = \mu\alpha$. One thing to note here is that $F(\alpha)\mu = F(\alpha)$. This is because $g\mu\alpha = g\alpha\mu = g\mu$ for all g in $F(\alpha)$. The other thing to note is that $\alpha_i\mu = \alpha_j$ (i and j in $\{1, \ldots, k\}$). This is not hard to prove. For example if $\alpha_1 = [g_1, \ldots, g_p]$ we see $g_1\mu\alpha = g_1\alpha_1\mu = g_2\mu$ etc., so that $[g_1\mu, \ldots, g_p\mu]$ is a p–cycle under α and must be an α_r with r in $\{1, \ldots, k\}$. Thus we

certainly have, if i is in $\{1,\ldots,k\}$, then $M(\alpha_i)\mu = M(\alpha_j)$ for some j in $\{1,\ldots,k\}$.

Automorphisms having the feature just displayed will, in a sense, be quite important. Ensuring there are no such fixed–point–free automorphisms of prime order, allows under certain circumstances the conclusion that $N(\alpha) = M_0(V)$. Indeed, when α confuses proper subgroups of V this is the case.

Theorem 3.2. Let V be a group and α a unit of $M_0(V)$ of order p (p a prime) which confuses proper subgroups of V. If there does not exist a fixed–point–free automorphism μ of V with prime order such that $\mu\alpha = \alpha\mu$, then $N(\alpha) = M_0(V)$ and $M_0(V)$ is a p–gen nearring.

Proof. Set $N = N(\alpha)$. If it is shown that $N = M_0(V)$, then the theorem will follow. It should first be noted that, V is a minimal N–group (ie. of type two). Here because α is a unit of finite order, V is readily seen to be unitary. Also, if $v \neq 0$ is an element of V, then vN is a non–zero subgroup of V with the property that $vN\alpha \subseteq vN$. Because α confuses proper subgroups of V, $vN = V$ and V is minimal. The next step is to show N is a non–ring. To obtain a contradiction assume N is a ring. Since $\alpha \neq 0$ and $V \neq \{0\}$ there exists $v \neq 0$ in V such that $vN = V$. This implies that, the N–group V is a ring module, and α is in $Aut(V)$. Thus the subset of elements of V fixed by α (0 included), is a subgroup H of V. Since $H\alpha \subseteq H$ and, because α confuses proper subgroups of V, we see $H = V$ or $H = \{0\}$. If $H = V$, then $\alpha = 1$, contrary to α having order p. This means α is a fixed–point–free automorphism of V of prime order which commutes with α. This situation has been excluded and N is necessarily a non–ring.

If $Aut_N(V)$ (the group of N–automorphisms of V) is distinct from $\{1\}$ then, by [3, 4.52], $Aut_N(V)$ contains a fixed–point–free automorphism (μ say) of V of prime order. Because $\mu\alpha = \alpha\mu$, we have a contradiction. Thus $Aut_N(V) = \{1\}$ and, by [3, 4.52], N must coincide with $M_0(V)$.

4. Groups with few involutions

We now start deriving results telling us about the p–gen nature of $M_0(V)$ (V a group). To begin with it would be too much to take on arbitrary V. Considerations given here will focus on the situation where $|\eta(V)| \leq \frac{1}{3}|V|$. In sections that follow we shall be allowing a higher proportion of involutions to occur. The $\frac{1}{3}|V|$ restriction will help us later to deal with more involutions.

Lemma 4.1. Let p be a prime. If V is a group such that $|\eta(V)| \leq \frac{1}{3}|V|$ and $|V| > 2p$, then $M_0(V)$ is p–gen.

Proof. By [4] and [5], it can be assumed that $p \geq 5$ (V is not elementary two because $|\eta(V)| \leq \frac{1}{3}|V|$). Let $|V| - 1 = rp + s$, where $r \geq 1$ is an integer and s an integer ≥ 0 and $\leq p - 1$. Since $|V| - 1 \geq 2p$, it follows that $r \geq 2$. We take

$$\alpha = [g_1, \ldots, g_p][g_{p+1}, \ldots, g_{2p}] \ldots [g_{(r-1)p+1}, \ldots, g_{rp}],$$

where the rp elements $g_1, \ldots, g_{rp}$ of V^* are to be specified. First considerations are to show how to take

$$g_p, g_{p+1}, g_{2p}, g_{2p+1}, \ldots, g_{(r-1)p}, g_{(r-1)p+1}. \tag{4.1}$$

The number of such elements is $< 2r$ which is $\leq \frac{2}{5}(|V| - 1)$ (from above $p \geq 5$ and $rp \leq |V| - 1$). Thus the number of such elements is for $|V| > 2p$ necessarily $\leq \frac{2}{3}|V| - 1$ which is $\leq |\tau(V)|$ because $|\tau(V)| = |V^*| - |\eta(V)|$ and $|\eta(V)| \leq \frac{1}{3}|V|$. As $\tau(V)$ can be partitioned into two element subsets $\{h, -h\}$ (h in $\tau(V)$) it is possible to take the elements of (1) such that $g_p = -g_{p+1}, \ldots, g_{(r-1)p} = -g_{(r-1)p+1}$. Three steps specifying more of the elements of $\{g_1, \ldots, g_{rp}\}$ are now taken.

Step 1. When $|\eta(V)| = 0$ all elements of V^* are partitioned into two element subsets $\{h, -h\}$ (h in V^*) so we can (and do) now take $g_1 = -g_2, \ldots, g_{p-2} = -g_{p-1}$.

Step 2. When $|\eta(V)| > 2$ the elements of the sequence

$$g_1, g_2, \ldots, g_{p-1}, g_{p+2}, \ldots, g_{2p-1}, g_{2p+2}, \ldots, g_{(r-1)p-1}, g_{(r-1)p+2} \tag{4.2}$$

are successively chosen as being from $\eta(V)$ (note that none of these elements are in those of (1)). It will be shown all of $\eta(V)$ is used up. This happens if

$$p + (r-2)(p-2) \geq \frac{1}{3}|V|, \tag{4.3}$$

because $\frac{1}{3}|V| \geq |\eta(V)|$. However, r is equal to $(|V| - 1)/p - s/p$ and, since $s/p \leq (p-1)/p$, it follows that $r \geq |V|/p - 1$. Thus (3) holds if

$$p + (|V|/p - 3)(p-2) \geq \frac{1}{3}|V|$$

or

$$p - 3p + 6 \geq |V|(\frac{1}{3} - (p-2)/p).$$

Because $p \geq 5$, $\frac{1}{3} - (p-2)/p$ is negative, and dividing by $\frac{1}{3} - (p-2)/p$, we see (3) holds if

$$(-2p+6)/(\frac{1}{3} - (p-2)/p) \leq |V|$$

or

$$|V| \geq (6p^2 - 18)/(2p-6).$$

This last inequality holds if $|V| \geq 3p$. It remains to show step 2. holds when $|V| < 3p$. Here $r = 2$ and the number of elements of (2) is p so that because $|\eta(V)| \leq \frac{1}{3}|V| < p$ all of $\eta(V)$ is used in successively defining elements of (2).

Step 3. In step 1. and 2. the elements of the set $\{g_{(r-1)p+3}, \ldots, g_{rp}\}$ did not enter into consideration. Also they did not come into those that occur in (1), so we are still free to adjust the elements of this set. This is done in the following way. This set has $p-2$ elements while $F(\alpha)$ has order s where $s \leq p-1$. The elements of these two sets are in $\tau(V)$ (all of $\eta(V)$ was used up in step two) so by 2.3 we may adjust the $g_{(r-1)p+3}$ to g_{rp} in such a way that $F(\alpha)$ does not contain all non-zero elements of a non-zero subgroup of V.

The α given by steps 1. to 3. will now be shown to confuse proper subgroups of V. By step 3. a non-zero α–invariant subgroup K of V cannot be such that $K^* \subseteq F(\alpha)$. This means $K \cap M(\alpha) \neq \emptyset$ and from the definition of α and 3.1, $M(\alpha) \subseteq K$ so that simple order arguments ensure $K = V$. Thus α confuses proper subgroups of V. By 3.2 the lemma will follow if it is shown there is no fixed–point–free automorphism μ of V of prime order q say so that $\alpha\mu = \mu\alpha$. There are two cases involved here.

Case 1. This is where $|\eta(V)| = 0$. Here we have from the definition of α and step 1. that either $[g_1, \ldots, g_p]$ is the only p–cycle α_1 in the definition of α with a single element (viz. g_p) without an additive inverse in $M(\alpha_1)$ or $[g_1, \ldots, g_p]$ and $[g_{(r-1)p+1}, \ldots, g_{rp}]$ are the only two such p–cycles. Because $\alpha_1\mu$ is another such p–cycle (see §.3) we have either $[g_1\mu, \ldots, g_p\mu] = [g_1, \ldots, g_p]$ and the uniqueness of g_p means $g_p\mu = g_p$ (a contradiction) or $[g_1, \ldots, g_p]\mu = [g_{(r-1)p+1}, \ldots, g_{rp}]$ and $[g_{(r-1)p+1}, \ldots, g_{rp}]\mu = [g_1, \ldots, g_p]$. This last situation (the first is now excluded) gives $[g_1, \ldots, g_p]\mu^2 = [g_1, \ldots, g_p]$ so that 2 divides q and $q = 2$, meaning $v\mu = -v$ for all v in V (see 2.9). However $g_1\mu = -g_1$ (in $M(\alpha_1)$. As $g_1\mu$ would, in this situation, be in $\{g_{(r-1)p+1}, \ldots, g_{rp}\}$ we have a contradiction here also.

Case 2. This is where $|\eta(V)| > 0$. Here $[g_1, \ldots, g_p]$ (α_1 say) is the only p–cycle in the definition of α having elements of $M(\alpha_1)$ in $\eta(V)$ or the only

one with $M(\alpha_1)$ containing $p-1$ elements of $\eta(V)$. It is not difficult to see this from the definition of α and step 2. This fact implies $M(\alpha_1)\mu = M(\alpha_1)$ so that q divides p and $q = p$. Furthermore $M(\alpha_1)$ is an orbit of μ so that $g_1\mu^k = g_p$ (some integer $k \geq 1$). A contradiction has been reached (g_1 is in $\eta(V)$ while g_p is in $\tau(V)$) and 4.1 is therefore proved.

5. Nilpotent with a quantity of involutions

In the last section the order of $\eta(V)$ was quite restricted. It was assumed that $|\eta(V)| \leq \frac{1}{3}|V|$. Here we raise this upper bound to $\frac{9}{16}|V| - 1$. This figure is not arbitrarily chosen. It does in fact fit in quite well with what is known about groups with $|\eta(V)| > \frac{1}{2}|V| - 1$ (see §.2 eg. 2.8). Groups with $|\eta(V)| > \frac{1}{2}|V| - 1$ are necessarily often nilpotent. This is another assumption that will apply to groups studied here. What we prove is as follows.

Lemma 5.1. Let p be a prime. If V is a nilpotent group with $|\eta(V)| \leq \frac{9}{16}|V| - 1$ and $|V| > 3p$, then $M_0(V)$ is p-gen.

Proof. By [4] and [5] it can be assumed $p \geq 5$ (elementary two groups are excluded because $|\eta(V)| \leq \frac{9}{16}|V| - 1$). Now, if V is a group of odd order, then the result follows by 4.1. It can be assumed V has even order. If V is not a 2–group, then because V is nilpotent, all of $\eta(V)$ is contained in a Sylow 2– subgroup V_1 of V. This means

$$|\eta(V)| \leq |V_1| \leq (|V_1|/|V|)|V| \leq \frac{1}{3}|V|$$

and, by 4.1, $M_0(V)$ is p–gen. Thus it can be assumed $p \geq 5$ and V is a 2–group.

Let $|V| - 1 = rp + s$, where r is an integer ≥ 1 and s is in $\{0, \ldots, p-1\}$. Because $|V| - 1 \geq 3p$, we see $r \geq 3$. Define

$$\alpha = [g_1, \ldots, g_p][g_{p+1}, \ldots, g_{2p}] \ldots [g_{(r-1)p+1}, \ldots, g_{rp}],$$

where the rp elements $g_1, \ldots, g_{rp}$ of V^*, are to be specified. First we specify some of the elements of the sequence

$$g_1, \ldots, g_{p-1}, g_{p+2}, \ldots, g_{2p-1}, g_{2p+2}, \ldots, g_{(r-1)p-1}, g_{(r-1)p+2}, \ldots, g_{rp}. \tag{5.4}$$

These are chosen successively as elements of $\eta(V)$ and all of $\eta(V)$ is used up, if the number of elements of (4) is not less than $|\eta(V)|$. Thus all of

$\eta(V)$ is used up if

$$(p-1)2 + (r-2)(p-2) \geq \frac{9}{16}|V| - 1.$$

Because

$$r = (|V|-1)/p - s/p \geq (|V|-1)/p - (p-1)/p = |V|/p - 1,$$

we see all of $\eta(V)$ is used up if

$$(p-1)2 + (|V|/p - 3)(p-2) \geq \frac{9}{16}|V| - 1$$

or

$$1 + (p-1)2 - 3(p-2) \geq (\frac{9}{16} - (p-2)/p)|V|.$$

However, for $p \geq 5$, $\frac{9}{16} - (p-2)/p$ is negative and all of $\eta(V)$ is used up in successively defining elements of the sequence (4) if

$$|V| \geq (-p+5)/(\frac{9}{16} - (p-2)/p)$$

or

$$|V| \geq (16p^2 - 80p)/(7p - 32)$$

which is the case because

$$(16p^2 - 80p)/(7p - 32) \leq 3p$$

(clearly $16p - 80 \leq 21p - 96$ for $p \geq 5$) while $|V| > 3p$. Thus, some elements of (4) are defined and all the remaining g's come from $\tau(V)$. From the nature of $\tau(V)$ it is now possible to choose all the remaining g's such that

$$g_p, g_{p+1}, g_{2p}, g_{2p+1}, \ldots, g_{(r-1)p}, g_{(r-1)p+1},$$

are chosen with $g_p = -g_{p+1}$ up to $g_{(r-1)p} = -g_{(r-1)p+1}$. So in this manner α is defined.

Clearly, $V^* \backslash \{g_1, \ldots, g_{rp}\}$ has no elements of order two and, a proper subgroup K of V, is such that $M(\alpha) \cap K \neq \emptyset$. Certainly if, $K\alpha \subseteq K$, then 3.1 ensures $M(\alpha) \subseteq K$ and, simple order arguments mean $K = V$. Thus α confuses proper subgroups of V. Also, from the manner in which α is defined, it follows that either $[g_1, \ldots, g_p]$ is the unique p–cycle containing $p-1$ elements of order two or $[g_1, \ldots, g_p]$ and $[g_{(r-1)p+1}, \ldots, g_{rp}]$ are the unique pair of p–cycles (in the definition of α) containing $p-1$

elements of order two. We conclude that a fixed–point–free automorphism μ of V of prime order q, such that $\alpha\mu = \mu\alpha$, must satisfy either $\{g_1, \ldots, g_p\}\mu = \{g_1, \ldots, g_p\}$ or $\{g_1, \ldots, g_p\}\mu = \{g_{(r-1)p+1}, \ldots, g_{rp}\}$ and $\{g_{(r-1)p+1}, \ldots, g_{rp}\}\mu = \{g_1, \ldots, g_p\}$. The second case cannot occur, otherwise $q = 2$ and μ fixes all elements of order two (see 2.9). In the first case, $p = q$, $\{g_1, \ldots, g_p\}$ is an orbit under μ and because g_1 is in $\eta(V)$ and g_p in $\tau(V)$, we have a contradiction, so that 3.2 applies and 5.1 is proved.

6. Dealing with V where $|\eta(V)| \leq \frac{1}{2}|V|$

Although in this section we allow V to have more involutions than was the case in four, our groups may be non–nilpotent and the $\frac{9}{16}|V|-1$ bound of section five is, for our present purposes too high. A bound that helps us go quite a long way to establishing 1.1 is $\frac{1}{2}|V|$. Thus the result that we aim at here, is showing V with $|V| > 3p$ and $|\eta(V)| \leq \frac{1}{2}|V|$ has p–gen $M_0(V)$ (p any prime). However, the ultimate goal of sections four to nine (see 9.1) is in fact to show that the restriction on $|\eta(V)|$ is unnecessary. All that 9.1 requires is that V is not elementary two. Although this is eventually arrived at, intermediate results must be covered. Sometimes, for specific V and p, it is not that difficult to establish the p–gen nature of $M_0(V)$. For example, this can be done for V with $|V| = 16$ and $p = 5$ without too much trouble. Before stating and proving this sections main theorem (announced above) this very special case is attended to.

Proposition 6.1. If V (not elementary two) is a group of order sixteen, then $M_0(V)$ is 5–gen.

Proof. Let α be the product

$$[g_1, \ldots, g_5][g_6, \ldots, g_{10}][g_{11}, \ldots, g_{15}]$$

of three disjoint 5–cycles on V where $g_1, \ldots, g_{15}$ are the 15 elements of V^* chosen in such a way that $g_1, g_2, \ldots, g_{15}$ are successively taken from $\eta(V)$.

Now V has no proper α–invariant subgroup H. This is because if H existed, H^* would have five or ten elements contrary to the fact that $|H|$ divides $|V|$. Also, out of the three 5–cycles defining α there is either a unique one containing elements of $\eta(V)$ and $\tau(V)$ or $\{g_1, \ldots, g_5\}$ is $\eta(V)$ and $\{g_6, \ldots, g_{15}\}$ is $\tau(V)$. This is true since $\eta(V) \neq V^*$ and $|\eta(V)|$ being of odd order must be five. In the case of a unique 5–cycle $[h_1, \ldots, h_5]$ with elements in $\eta(V)$ and $\tau(V)$ it is clear that a fixed–point–free automorphism μ of prime order q must be such that $\{h_1, \ldots, h_5\}\mu = \{h_1, \ldots, h_5\}$, $q = 5$ and $h_i\mu^r = h_j$ ($r \geq 1$ an integer — h_i in $\eta(V)$ and h_j in $\tau(V)$). This

cannot happen so $\eta(V) = \{g_1, \ldots, g_5\} = \{g_1, \ldots, g_5\}\mu$ and again $q = 5$. Clearly$\{g_6, \ldots, g_{10}\}\mu \neq \{g_{11}, \ldots, g_{15}\}$ (otherwise $\{g_{11}, \ldots, g_{15}\}\mu = \{g_6, \ldots, g_{10}\}$ and q is 2). Thus $\{g_6, \ldots, g_{10}\}\mu = \{g_6, \ldots, g_{10}\}$, $q = 5$ and if g_7 (in $\tau(V)$) where to be taken as $-g_6$ we would have $g_6\mu^r = -g_6$ ($r \geq 1$ coprime to 5) contrary to the fact two does not divide five. Thus no such μ exists and α (of order five) is such that $N(\alpha) = M_0(V)$ (ie. 3.2 applies). The proposition has been proved.

The main result of this section is the following.

Theorem 6.2. Let p be a prime. If V is a group with $|\eta(V)| \leq \frac{1}{2}|V|$ and $|V| > 3p$, then $M_0(V)$ is p–gen.

Proof. By [4] and [5] we may assume $p \geq 5$. Also by 5.1, it can be assumed V is non–nilpotent (clearly $\frac{1}{2}|V| \leq \frac{9}{16}|V| - 1$ for $|V| > 3p$ when $p \geq 5$). The situation where V has odd order can be excluded by 4.1. Furthermore, it can be assumed that, all elements of $\eta(V)$ do not additively centralize each other. This is because, if they did, then $i(V)$ is an elementary two proper subgroup of V. Because V is non–nilpotent, this normal subgroup cannot have index ≤ 2 (otherwise V is a 2–group). Hence, in this situation $|\eta(V)| \leq \frac{1}{3}|V|$ and the result follows by 4.1. Thus the assumption that all elements of $\eta(V)$ do not additively centralize each other can (and will) be made.

Let $|V| - 1 = rp + s$, where r is an integer ≥ 0 and s in $\{0, \ldots, p-1\}$. Because $|V| - 1 \geq 3p$, we see $r \geq 3$. Define

$$\alpha = [g_1, \ldots, g_p][g_{p+1}, \ldots, g_{2p}] \ldots [g_{(r-1)p+1}, \ldots, g_{rp}]$$

where the rp elements $g_1, \ldots, g_{rp}$ of V^* are to be specified. Let g_{p-1} and g_p be in $\eta(V)$ and not additively centralize each other. Now, by §.2, $\langle g_p, g_{p-1}\rangle = D_n$ where n is an integer ≥ 3. Let C_n be the normal cyclic subgroup of D_n of order n. Let d be a generator of C_n. Clearly $d \neq -d$ and we may take g_{2p} as d and g_{2p+1} as $-d$. Now $D_n \backslash C_n$ consists of involutions ($\lambda(D_n) = C_n$) and therefore contains an element c of $\eta(V)$, distinct from g_p and g_{p-1}. Certainly $\langle d, c\rangle = D_n$. Take g_{p+1} as c. Out of the elements of the sequence

$$g_1, \ldots, g_{p-1}, g_{p+2}, \ldots, g_{2p-1}, g_{2p+2}, \ldots, g_{(r-1)p-1}, g_{(r-1)p+2}, \qquad (6.5)$$

only g_{p-1} is accounted for. This sequence has $p + (r-2)(p-2)$ elements, and the number of unaccounted for ones is $p - 1 + (r-1)(p-2)$. Let these unaccounted for g's be taken successively from $\eta(V)\backslash\{a, b, c\}$ ($a = g_{p-1}$, and $b = g_p$). All the remainder of $\eta(V)$ has been used up in defining these

g's if

$$p-1+(r-2)(p-2) \geq |\eta(V)|-3.$$

We want to show this holds when $|V| > 3p$. This is certainly the case for $r = 3$ because here $|V| \leq 4p$ and $2p \geq \frac{1}{2}|V| \geq |\eta(V)|$. Now for $|V| \geq 4p$ all of $\eta(V)$ has been used up defining g's if

$$p-1+(r-2)(p-2) \geq \frac{1}{2}|V|-3.$$

Because

$$r = (|V|-1)/p - s/p \geq (|V|-1)/p - (p-1)/p = |V|/p - 1,$$

we see all of $\eta(V)$ has been used up in so far defining g's if

$$p+2-3(p-2) \geq |V|(\frac{1}{2} - (p-2)/p).$$

However, $\frac{1}{2} - (p-2)/p$ is negative, since $p \geq 5$. Thus all $\eta(V)$ has been used up in, so far defining g's if

$$|V| \geq (-2p+8)/(\frac{1}{2} - (p-2)/p) = [2p(-2p+8)]/(-p+4) = 4p$$

which is certainly the case.

The remainder of the g's must be taken from $\tau(V)\backslash\{d, -d\}$. these elements of V^*, can be partitioned into two element subsets consisting of an element and its additive inverse. Thus the remaining g's (in the definition of α) can be chosen in such a way that $g_{2p} = -g_{2p+1}$, up to $g_{(r-1)p} = -g_{(r-1)p+1}$ (vacuous if $r = 3$). All g's have been chosen from V^* and α is apart from the minor adjustment that follows, defined.

The essential features of the above preliminary definition of α are that g_{p-1} and g_p are in $\eta(V)$, $\langle g_{p-1}, g_p\rangle = D_n$, $\langle g_{p+1}, g_{2p}\rangle = D_n$, $g_{2p} = -g_{2p+1}$ is in $\tau(V)$, the elements $g_{3p}, \ldots, g_{(r-1)p}$ are in $\tau(V)$ and $g_{3p} = -g_{3p+1}$ up to $g_{(r-1)p} = -g_{(r-1)p+1}$, while all of $\eta(V)$ is in $\{g_1, \ldots, g_{(r-1)p+2}\}$ (this last statement follows because all of $\eta(V)\backslash\{a, b, c\}$ was used up in defining $S\backslash\{g_{p-1}\}$ — here S is the elements of (5)). These features of α are clearly unchanged if we rearrange the elements of $\{g_{(r-1)p+3}, \ldots, g_{rp}\} \cup (V^*\backslash\{g_1, \ldots, g_{rp}\})$ $(= S_1$ say). The first of these sets has $p-1$ elements and the second has $\leq p-1$ elements (viz. s elements). Clearly S_1 is a disjoint union of the subsets indicated and $S_1 \subseteq \tau(V)$. It is now possible, by 2.3, to write S_1 as a disjoint union of sets S_2 and S_3, where $|S_2| \leq p-2$ and $|S_3| = s$ in such a way that, S_3 does not contain the non–zero elements of a non–zero subgroup of V. Rename the g's so that they remain the

same, apart from the fact that $g_{(r-1)p+3}, \ldots, g_{rp}$, are now taken as the elements of S_2. In this manner we obtain the final definition of α. All the properties of α listed above hold true, but now we have the additional fact that $V^* \backslash M(\alpha)$ (ie. $F(\alpha)$) is S_3 and does not contain the non–zero elements of a non–zero subgroup of V.

It will now be shown that α confuses proper subgroups of V. Firstly, a non–zero subgroup H of V cannot be such that $M(\alpha) \cap H = \emptyset$. If $H\alpha \subseteq H$ and an element of $\{g_{p+1}, \ldots, g_{rp}\}$ is in H, then $\{g_{p+1}, \ldots, g_{rp}\} \subseteq H$. This follows by 3.1, because $g_{2p} = -g_{2p+1}$ up to $g_{(r-1)p} = -g_{(r-1)p+1}$. However, in this case, g_{2p} and g_{p+1} are in H, implying $\langle g_{p+1}, g_{2p} \rangle \subseteq H$ and g_p is in H. This means $M(\alpha) \subseteq H$. On the other hand, if an element of $\{g_1, \ldots, g_p\}$ is in H, then $\langle g_p, g_{p-1} \rangle$ is contained in H and g_{p+1} is in H.. Thus, in this case also, $M(\alpha) \subseteq H$. Simple order arguments mean $H = V$ and α confuses proper subgroups of V. Now V is non–nilpotent and by 2.10 has no fixed–point–free automorphisms of prime order. It follows from 3.2 that $N(\alpha) = M_0(V)$ and because α is a disjoint product of p–cycles on V, $M_0(V)$ is p–gen. 6.2 has been proved.

7. When V is not a $D(A)$

Now that theorem 6.2 has been proved it is time to move towards looking at V with $|\eta(V)| > \frac{1}{2}|V|$. The idea is to extend 6.2 to any V not elementary two. The situation here is in one regard more complex and in another simpler. The complexity comes from the fact that, in constructing an α of order p in $u(M_0(V))$ with $N(\alpha) = M_0(V)$, there are more elements of order two that must be lost within the disjoint p–cycles into which α decomposes. The other side of the coin is that V has limited structure (see 2.8). In some sense the difficult issue is what to do about groups of type (II), (III) and (IV). All these are 2-groups and many have $|\eta(V)|$ coming within the $\frac{9}{16}|V| - 1$ bound used in 5.1. Groups of type (II), (III) and (IV) certainly have $|\eta(V)| \leq \frac{5}{8}|V| - 1$ so a fairly real problem is handling those $\eta(V)$ of order $> \frac{9}{16}|V| - 1$ and $\leq \frac{5}{8}|V| - 1$. This is accomplished in this section. What is proved here is the following.

Lemma 7.1. Let $p \geq 5$ be a prime. If the group V is not a $D(A)$ and has order $> 3p$, then $M_0(V)$ is p–gen.

Proof. By 6.2 we may assume $|\eta(V)| > \frac{1}{2}|V|$. Since V is not a $D(A)$ it follows from 2.8 that V is a 2-group and by 2.5, 2.6 and 2.7 $|\eta(V)| \leq \frac{5}{8}|V| - 1$.

Let $|V|-1 = rp+s$, where r is an integer ≥ 1 and s is in $\{0,\ldots,p-1\}$. Because $|V|-1 \geq 3p$, we see $r \geq 3$. Define

$$\alpha = [g_1,\ldots,g_p][g_{p+1},\ldots,g_{2p}]\ldots[g_{(r-1)p+1},\ldots,g_{rp}],$$

where the rp elements of V^* are to be specified. First we specify some of the elements of the sequence

$$g_1,\ldots,g_{p-1},g_{p+2},\ldots,g_{2p-1},g_{2p+2},\ldots,g_{(r-1)p-1},g_{(r-1)p+2},\ldots,g_{rp}. \tag{7.6}$$

These are chosen successively as elements of $\eta(V)$ and all of $\eta(V)$ is used up, if the number of elements of (6) is not less than $|\eta(V)|$. Thus all of $\eta(V)$ is used up if

$$(p-1)2+(r-2)(p-2) \geq \frac{5}{8}|V|-1.$$

However, p does not divide $|V|$ (V is a 2-group) so $s \leq p-2$ and

$$r = (|V|-1)/p - s/p \geq (|V|-1)/p-(p-2)/p = |V|/p-(p-1)/p$$

so that all of $\eta(V)$ is used up if

$$1+2p-2+(1-3p)(p-2)/p \geq (\frac{5}{8}-(p-2)/p)|V|.$$

This holds if

$$8p+16p^2-16p+8(1-3p)(p-2) \geq (-3p+16)|V|$$

or

$$8p+16p^2-16p-16+56p-24p^2 \geq (-3p+16)|V|.$$

Thus all of $\eta(V)$ is used up if

$$(-8p^2+48p-16) \geq (-3p+16)|V|.$$

For $p=5$ this reduces to $24 \geq |V|$ which is satisfied because $|V|$ is 16, 32,, etc., and $|V|=16$ can, by 6.1, be excluded. For $p \geq 7$, we see this inequality reduces to

$$(8p^2-48p+16)/(3p-16) \leq |V|$$

since $-3p+16$ is negative and is satisfied if $8p^2-48p+16 \leq 3p(3p-16)$ or $8p^2-48p+16 \leq 9p^2-48p$ (certainly the case since $|V| \geq 3p$ and $p \geq 7$). In this way some of the elements of (6) are defined (all of $\eta(V)$

has been used up) and the remaining g's must come from $\tau(V)$. From the nature of $\tau(V)$ it is now possible to choose the remaining g's such that $g_p = -g_{p+1}$ up to $g_{(r-1)p} = -g_{(r-1)p+1}$. So in this manner α is defined.

Clearly, $V^* \backslash \{g_1, \ldots, g_{rp}\}$ has no elements of order two and, a proper subgroup K of V, is such that $M(\alpha) \cap K \neq \emptyset$. Certainly if $K\alpha \subseteq K$, then 3.1 ensures $M(\alpha) \subseteq K$ and simple order arguments mean $K = V$. Thus α confuses proper subgroups of V. Also, from the manner in which α is defined, it follows that either $[g_1, \ldots, g_p]$ is the unique p–cycle containing $p-1$ elements of order two or $[g_1, \ldots, g_p]$ and $[g_{(r-1)p+1}, \ldots, g_{rp}]$ are the unique pair of p–cycles (in the definition of α) containing $p-1$ elements of order two. We conclude that, a fixed–point–free automorphism μ of V of prime order q, such that $\alpha\mu = \mu\alpha$, must satisfy either $\{g_1, \ldots, g_p\}\mu = \{g_1, \ldots, g_p\}$ or $\{g_1, \ldots, g_p\}\mu = \{g_{(r-1)p+1}, \ldots, g_{rp}\}$ and $\{g_{(r-1)p+1}, \ldots, g_{rp}\}\mu = \{g_1, \ldots, g_p\}$. The second case cannot occur, otherwise $q = 2$ and μ fixes all elements of order two (see 2.9). In the first case, it follows $g_1\mu^k = g_p$ for some integer $k \geq 1$ (here $q = p$) and, because g_1 is in $\eta(V)$ and g_p in $\tau(V)$, we have a contradiction. By 3.2, 7.1 stands proved.

8. V a $D(A)$ with p dividing $|V|$

In this section we continue to deal with groups having $|\eta(V)| > \frac{1}{2}|V|$. The situation where V is of type (II), (III) or (VI) has been dealt with in 7.1. By 2.8 there remain those groups of the form $D(A)$ (A abelian). Because this paper is not concerned with elementary two groups the possibility of such an A ($D(A)$ is elementary two precisely when A is elementary two and in all other cases $D(A)$ is non-abelian and $\lambda(D(A)) = A$ — see §.2) is excluded. However this section makes another assumption also. Here we assume that p divides $|V|$ (ie. p divides $|D(A)|$). In the next the full cycle of dealing with all V having $|V| > 3p$ is completed by showing when p does not divide the order of a $D(A)$ having $|D(A)| > 3p$, $M_0(D(A))$ is p–gen.

Lemma 8.1. Let p be a prime and V a group of type (I) (not elementary two) which is such that p divides $|V|$. If $|V| > 3p$, then $M_0(V)$ is p–gen.

Proof. The case where $p = 2$ or 3 respectively follows from [4] or [5]. Thus it can be assumed that $p \geq 5$. Also, because $|V|$ is even and p divides $|V|$, we have $|V| \geq 4p$. Furthermore $|\lambda(V)|$ can be assumed to be even. This is because otherwise $\eta(\lambda(V))$ is empty and $|\eta(V)| = \frac{1}{2}|V|$ (see §.2), so that the result would follow by 6.2. Thus $|\lambda(V)|$ can be assumed even and $\lambda(V)$ (which contains $\tau(V)$) contains an element of order two and

order p. Thus $\lambda(V)$ contains a subgroup of the form $C_2 \oplus C_p$ and has at least $p-1$ elements of composite order.

Now $\lambda(V)$ is an abelian group containing $\tau(V)$ (see §.2). Thus $\lambda(V)$ has a subgroup A of index p and all elements of $\lambda(V)\backslash A$ have order divisible by p. Thus $|i(\lambda(V))| \leq \frac{1}{p}|\lambda(V)|$ and, since $|\lambda(V)| = \frac{1}{2}|V|$ and all elements of $V\backslash\lambda(V)$ are in $\eta(V)$ (see §.2), it follows that

$$|i(V)| \leq \frac{1}{2p}|V| + \frac{1}{2}|V| = [(p+1)|V|]/2p,$$

which means

$$|\tau(V)| \geq [1-(p+1)/2p]|V| = [(p-1)|V|]/2p.$$

From what has been proved we can therefore assume $p \geq 5$, $|V| \geq 4p$, V has at least $p-1$ elements of composite order and $|\tau(V)| \geq [(p-1)|V|]/2p$.

Take $|V| - 1 = rp + p - 1$, where r is an integer ≥ 3 (remember $|V| \geq 4p$ and p divides $|V|$). Define α as a product

$$[g_1, \ldots, g_p][g_{p+1}, \ldots, g_{2p}] \ldots [g_{(r-1)p+1}, \ldots, g_{rp}],$$

where the rp elements $g_1, \ldots, g_{rp}$, of V^* are to be specified. We do this by first specifying the elements of $V^*\backslash\{g_1, \ldots, g_{rp}\}$ $(= F(\alpha))$ and then the elements of

$$\{g_p, g_{p+1}, g_{2p}, g_{2p+1}, \ldots, g_{(r-1)p}, g_{(r-1)p+1}\} \tag{8.7}$$

and finally allowing the remaining g's to be taken arbitrarily as the remaining elements of V^*.

First $\tau(V))$ is partitioned into two element subsets of the form $\{h, -h\}$, with h in $\tau(V)$. This means the elements of composite order are so partitioned. Take $(p-1)/2$ such pairs ($p-1$ elements forming a set S — possible from above) and the elements of $F(\alpha)$ (order $p-1$) are those of S. Thus $\tau(V)\backslash S$ is partitioned into two element subsets (as indicated) and the elements of (7) can be chosen so that

$$g_p = -g_{p+1}, g_{2p} = -g_{2p+1} \ldots, g_{(r-1)p} = -g_{(r-1)p+1},$$

provided $|\tau(V)\backslash S| \geq (r-1)2$ (ie. $|\tau(V)| \geq (r-1)2 + p - 1$). Thus the elements of (7) can be chosen as indicated (see above) if

$$[(p-1)/2p]|V| \geq (r-1)2 + p - 1.$$

However,

$$r = (|V| - 1)/p - (p - 1)/p = |V|/p - 1,$$

and the elements of (7) can be chosen as indicated if

$$[(p - 1)/2p]|V| \geq (|V|/p - 2).2 + p - 1$$

or, on multiplying by $2p$

$$(p - 1)|V| \geq 4|V| - 8p + 2p^2 - 2p = 4|V| - 10p + 2p^2.$$

Thus, the elements of (7) can be chosen as indicated provided, $(p-5)|V| \geq 2p^2 - 10p$. For $p = 5$ both sides are zero and all is well. If $p > 5$, then since $|V| \geq 3p$ this is satisfied if,

$$(p - 5)3p = 3p^2 - 15p \geq 2p^2 - 10p$$

or $p \geq 5$, which is certainly true. Thus the elements of (7) can be chosen as indicated, while the remaining g's are simply taken as the rest of the elements of V^*, namely those of the set

$$V^* \backslash (F(\alpha) \cup \{g_p, g_{p+1}, g_{2p}, g_{2p+1}, \ldots, g_{(r-1)p}, g_{(r-1)p+1}\}).$$

Now suppose H is a non-zero α–invariant subgroup of V. If $F(\alpha) \supseteq H^*$, then $F(\alpha)$ would contain a non-zero element of prime order. Since this cannot happen (the elements of $F(\alpha)$ have composite order), we see $M(\alpha) \cap H \neq \emptyset$. By 3.1, $M(\alpha) \subseteq H$ and simple order arguments ensure $H = V$.

Suppose V has a fixed–point–free automorphism μ of prime order (q say), such that $\alpha\mu = \mu\alpha$. Now $\lambda(V)$ is by §.2, characteristic and, it readily follows that $\lambda(V)\backslash\{0\}$ and $V\backslash\lambda(V)$ are partioned under μ, into q element orbits. However, $|V\backslash\lambda(V)| = |\lambda(V)|$ (see §.2) and $|\lambda(V)\backslash\{0\}| = |\lambda(V)| - 1$. Since q cannot divide both $|\lambda(V)|$ and $|\lambda(V)| - 1$, no such μ can exist and an application of 3.2 completes the proof.

9. A substantial Theorem

Although the goal of this paper is the proof of 1.1, virtually all previous material has been developed with a view to proving an intermediate result. This is that for a prime p and group V (not elementary two) with $|V| > 3p$, $M_0(V)$ is p–gen. The theorem alluded to is proved in this section. Allowing as it does, considerations to focus on groups where $|V| \leq 3p$ it is essential to the proof of 1.1. There is only one small detail of all that has preceeded that is very slightly different. All material so far has been developed for

V having $|V| > 3p$ with one small exception. This is 4.1 where the weaker assumption of $|V|$ being $> 2p$ is made. It seems this slightly more inclusive detail for groups with $|\eta(V)| \leq \frac{1}{3}|V|$ is also needed for proving 1.1. This however does not concern us here. The theorem we prove is the following.

Theorem 9.1. Let p be a prime and V a group (not elementary two) with $|V| > 3p$, then $M_0(V)$ is p-gen.

Proof. By [4], [5] and 7.1 we may (and will) assume $p \geq 5$ and V is a $D(A)$. Also by 8.1 it can (and will) be assumed that p does not divide $|V|$. One further assumption is also made. $|\lambda(V)|$ is taken as even since if $|\lambda(V)|$ is odd, $V \backslash \lambda(V) = \eta(V)$ and, by 2.4, $|\eta(V)| = \frac{1}{2}|V|$.

An Initial Step. It will be proved here that, the number of elements of $\lambda(V)$ of composite order is $\geq \frac{1}{2}|\lambda(V)| - 1$. Now $\lambda(V)$ is an abelian group with $|\lambda(V)|$ even. Also, it is easy to see that it is not elementary two. If $\lambda(V)$ is a 2–group, then because $i(\lambda(V))$ is a subgroup of $\lambda(V)$ of index at least two and elements of $\lambda(V) \backslash i(\lambda(V))$ have composite order, this step follows. Otherwise, $\lambda(V)$ has a maximal subgroup H_1 of odd order and a maximal non–zero 2–subgroup H_2, and $\lambda(V) = H_1 \oplus H_2$. Now elements $a + b$, a in H_1^* and b in H_2^*, have composite order. The number x of such elements is $|H_1||H_2| - |H_1| - |H_2| + 1$. So that if $|H_2| = 2$, $x = |\lambda(V)| - |H_1| - 1 = \frac{1}{2}|\lambda(V)| - 1$ and the result follows. Thus it can be assumed that $|H_2| \geq 4$ and if $|H_1| > 3$,

$$x \geq |\lambda(V)| - \frac{1}{4}|\lambda(V)| - \frac{1}{4}|\lambda(V)| + 1 \geq \frac{1}{2}|\lambda(V)| - 1.$$

Hence we may assume $|H_1| = 3$. Now the subgroup $i(\lambda(V))$ of $\lambda(V)$ has index ≥ 3 in $\lambda(V)$, and further $|i(\lambda(V))| \leq \frac{1}{3}|\lambda(V)|$ and $|\tau(\lambda(V))| \geq \frac{2}{3}|\lambda(V)| > \frac{1}{2}|\lambda(V)|$ so that $|\tau(\lambda(V))| \geq \frac{1}{2}|\lambda(V)| + 1$. However, every non–zero element of $\tau(\lambda(V))$ has order $2^{k_1}3^{k_2}$ (k_1, k_2 integers ≥ 0), and only two have order three (none have order two). Thus the number of elements of $\lambda(V)$ of composite order is $\geq \frac{1}{2}|\lambda(V)| + 1 - 2 = \frac{1}{2}|\lambda(V)| - 1$ and our initial step is proved.

From what has been proved above it can (and will) be assumed the $p \geq 5$, V is of type (I) (not elementary two), p does not divide $|V|$, $|\lambda(V)|$ is even and the number of elements of $\lambda(V)$ of composite order is $\geq \frac{1}{2}|\lambda(V)| - 1$.

Now $|V \backslash \lambda(V)| = \frac{1}{2}|V|$ (see §.2) and $|V \backslash \lambda(V)| > \frac{3}{2}p$. Let $|V \backslash \lambda(V)| = r_1 p + s_1$, where $r_1 \geq 1$ is an integer and s_1 is an integer in $\{0, \ldots, p-1\}$. Define

$$\alpha_1 = [v_1, \ldots, v_p][v_{p+1}, \ldots, v_{2p}] \ldots [v_{(r_1-1)p+1}, \ldots, v_{r_1 p}],$$

where $v_1, \ldots, v_{r_1 p}$ are any $r_1 p$ elements of $V \backslash \lambda(V)$. Certainly there is at least one p–cycle in the definition of α_1 since $r_1 \geq 1$. Also α_1 is a product of disjoint p–cycles and has order p. Now let $a_1, \ldots, a_{s_1}$, be the remaining elements of $(V \backslash \lambda(V)) \backslash \{v_1, \ldots, v_{r_1 p}\}$. Certainly $s_1 \leq p-1$ and, because p does not divide $|V|$, $s_1 \geq 1$ and a_1 exists. Let $b_1, \ldots, b_{p-s_1}$, be $p - s_1$ elements of $\lambda(V)^*$ (the element b_1 of $\{b_1, \ldots, b_{p-s_1}\}$ is to be chosen). Take $\alpha_2 = [a_1, \ldots, a_{s_1}, b_1, \ldots, b_{p-s_1}]$. Clearly α_2 is disjoint from α_1.

In order to define α_3 it must be shown that

$$\lambda(V)^* \backslash \{b_1, \ldots, b_{p-s_1}\}, \tag{9.8}$$

has at least p elements. If $|V| \geq 4p$, then $\frac{1}{2}|V| \geq 2p$ and $|\lambda(V)^*| \geq 2p - 1$ so that, because $\{b_1, \ldots, b_{p-s_1}\}$ has $\leq p - 1$ elements, $|\lambda(V)^* \backslash \{b_1, \ldots, b_{p-s_1}\}| \geq p$. Now $|V| > 3p$, so to prove the set (8) has $\geq p$ elements we can assume, $4p > |V| > 3p$. Thus $2p > \frac{1}{2}|V| > \frac{3}{2}p$ and $|V \backslash \lambda(V)|$ $(= \frac{1}{2}|V|)$ is $< 2p$ and $> \frac{3}{2}p$ (thus $\geq p + (p+1)/2$), implying $r_1 = 1$ and $s_1 \geq (p+1)/2$ so that $p - s_1 \leq (p-1)/2$. Since $|\lambda(V)^*|$ coincides with $\frac{1}{2}|V| - 1$, and is $< 2p - 1$ and greater than $p + (p+1)/2 - 1$ $(= p + (p-1)/2)$, we see that

$$|\lambda(V)^* \backslash \{b_1, \ldots, b_{p-s_1}\}| \geq p + (p-1)/2 - (p-1)/2 = p,$$

and the required fact about (8) is established. Let $|\lambda(V)^* \backslash \{b_1, \ldots, b_{p-s_1}\}| = r_2 p + s_2$, where r_2 is an integer ≥ 1 and s_2 is in $\{0, \ldots, p-1\}$.

Now take $g_1, \ldots, g_{r_2 p}$, as $r_2 p$ elements of the set (8) and define

$$\alpha_3 = [g_1, \ldots, g_p][g_{p+1}, \ldots, g_{2p}] \ldots [g_{(r_2-1)p+1}, \ldots, g_{r_2 p}], \tag{9.9}$$

where some of the g's, b_1 and the s_2 elements of

$$(\lambda(V)^* \backslash \{b_1, \ldots, b_{p-s_1}\}) \backslash \{g_1, \ldots, g_{r_2 p}\} \ (= S_2 \text{ say}),$$

are to be specified (the remaining g's can be taken arbitrarily as the elements of $\{g_1, \ldots, g_{r_2 p}\}$ that remain). In this way α_3 will be specified as an element of $u(M_0(V))$ of order p ($r_2 \geq 1$ and the r_2 p–cycles of (9) are disjoint) disjoint from α_1 and α_2. Concerning the g's (and b_1) we wish to specify, these elements are $g_p, g_{p+1}, g_{2p}, g_{2p+1}, \ldots, g_{r_2 p}, b_1$. Thus if $r_2 = 1$, this simply reduces to specifying g_p and b_1.

It follows that the set of elements to be specifed is the disjoint union

$$S_2 \cup \{g_p, g_{p+1}, g_{2p}, g_{2p+1}, \ldots, g_{r_2 p}, b_1\} \ (= S_3 \text{ say}),$$

which has $|S_2| + r_2 2$ elements. The set of elements chosen arbitrarily as the remainder of $\lambda(V)^* \backslash \{b_1, \ldots, b_{p-s_1}\}$ is necessarily

$$\{g_1, \ldots, g_{r_2 p}\} \backslash \{g_p, g_{p+1}, g_{2p}, g_{2p+1}, \ldots, g_{r_2 p}, b_1\}$$

and has $(p-1)+(r_2-1)(p-2)$ elements which together with $\{b_2, \ldots, b_{p-s_1}\}$ constitute the remainder set S_4 of the elements of $\lambda(V)^*$. This remainder set of $\lambda(V)^*$ has $(p-1)+(r_2-1)(p-2)+(p-s_1)-1$ $(= |S_4|)$, elements. Clearly S_3 and S_4 are disjoint with union $\lambda(V)^*$ and if it is shown that $|S_3| \leq |S_4|$, then $|S_3| \leq \frac{1}{2}|\lambda(V)^*| \leq \frac{1}{2}|\lambda(V)| - \frac{1}{2}$, showing $|S_3| \leq \frac{1}{2}|\lambda(V)| - 1$ ($|S_3|$ is an integer) and meaning, by our assumptions, all elements of S_3 can be chosen from the set C of elements of $\lambda(V)$ with composite order.

In order to prove the last statement of the above paragraph, it must be shown that

$$|S_2| + r_2 2 \leq (p-1) + (r_2 - 1)(p-2) + p - s_1 - 1. \tag{9.10}$$

Now $p - s_1 \geq 1$ and $s_2 \leq p-1$ so, if $s_2 \leq p-3$, (10) will hold, in this case, if it is shown that $p - 3 + r_2 2 \leq p - 1 + (r_2 - 1)(p-2)$. This holds if $0 \leq 2 + (r_2 - 1)p - r_2 2 + 2 - r_2 2$, which holds if $0 \leq 4 + r_2 p - r_2 4 - p$ or $p - 4 \leq r_2(p-4)$, which is certainly so since $r_2 \geq 1$ and $p \geq 5$. In the case where $s_2 \leq p-3$, (10) must therefore hold. Let us assume $s_2 = p-2$. In this situation $|\lambda(V)^*| = p - 2 + r_2 p + p - s_1$ and if $p - s_1 = 1$ ($p - s_1$ is non–zero), then $|\lambda(V)^*| = r_2 p + p - 1$ and $|\lambda(V)| - 1 = r_2 p + p - 1$ showing $|\lambda(V)| = (r_2 + 1)p$, which is a contradiction (p does not divide $|V|$). It follows in the case $s_2 = p-2$, we have $p - s_1 \geq 2$. Thus (10) holds, in this case, if $p - 2 + r_2 2 \leq p - 1 + (r_2 - 1)(p-2) + 1$ or $p - 3 + r_2 2 \leq p - 1 + (r_2 - 1)(p-2)$, which was seen to hold in arguments above. In the case where $s_2 = p-2$, (10) must therefore hold. It can therefore be assumed that $s_2 = p-1$. If $p - s_1 = 1$, then $|\lambda(V)| - 1 = (r_2 + 1)p$ and $|V \backslash \lambda(V)| = (r_2 + 1)p + 1$, showing $s_1 = 1$ and $p - s_1 \geq 4$ (a contradiction). If $p - s_1 = 2$, then $|\lambda(V)| - 1 = p(r_2 + 1) + 1$ and $|V \backslash \lambda(V)| = (r_2 + 1)p + 2$, showing $s_1 = 2$ and $p - s_1 \geq 3$ (a contradiction). Thus $p - s_1 \geq 3$ and (10) holds if $p - 1 + r_2 2 \leq p - 1 + (r_2 - 1)(p-2) + 2$ or $p - 3 + r_2 2 \leq p - 1 + (r_2 - 1)(p-2)$, which was seen to hold in arguments above. In all cases $|S_3| \leq |S_4|$. It has been shown that S_3 can be chosen from the set C of elements of $\lambda(V)$ with composite order.

Now C can be partioned into two element subsets $\{h, -h\}$ with h in C. Since S_3 is the disjoint union of S_2 and $\{g_p, g_{p+1}, g_{2p}, g_{2p+1}, \ldots, g_{r_2 p}, b_1\}$, we may choose $g_p = -g_{p+1}, g_{2p} = -g_{2p+1}, \ldots, g_{r_2 p} = -b_1$, in C, with S_2 contained in the remainder of C.

Now $\alpha_1\alpha_2\alpha_3$ is an element of $u(M_0(V))$ of order p. If H is a non–zero $\alpha_1\alpha_2\alpha_3$–invariant subgroup of V, then it contains a non–zero element d of V. If d is in $\{v_1, \ldots, v_{r_1p}\}$, then because $H\alpha_1 \subseteq H$, $d, d\alpha_1, \ldots, d\alpha_1^{p-1}$ are p elements of H and the subgroup K_1 they generate has non–zero intersection with $\lambda(V)$ (index two in V). Since $K_1 \leq H$, in this case, $\lambda(V) \cap H \neq \{0\}$. If d is in $M(\alpha_2)$, then since $H\alpha_2 \subseteq H$, $M(\alpha_2) \subseteq H$ and H contains $\{b_1, \ldots, b_{p-s_1}\}$ and intersects $\lambda(V)$ non–trivially. Clearly if d is in $V^*\backslash(\{v_1, \ldots, v_{r_1p}\} \cup M(\alpha_2))$, then $\lambda(V) \cap H \neq \{0\}$. It has been shown $\lambda(V)$ intersects H non–trivially and $\lambda(V)$ contains an element d_1 of H of prime order. Since S_2 consists of elements of $\lambda(V)$ of composite order, d_1 is not in S_2. Thus d_1 is in $M(\alpha_2)$ or $M(\alpha_3)$ and $H \cap M(\alpha_2\alpha_3) \neq \emptyset$. Now, from the manner in which $g_p, g_{p+1}, g_{2p}, g_{2p+1}, \ldots, g_{r_2p}, b_1$, are defined and 3.1 we conclude that $M(\alpha_2\alpha_3) \subseteq H$. However,

$$\langle M(\alpha_2\alpha_3)\rangle \geq \langle \{g_1, \ldots, g_{r_2p}\} \cup \{b_1, \ldots, b_{p-s_1}\}\rangle,$$

where the last group is, by simple order arguments $= \lambda(V)$. Thus $H \geq \lambda(V)$ and, since $M(\alpha_1) \subseteq H$, $H > \lambda(V)$ and $H = V$ (see §.2). It has been shown that $\alpha_1\alpha_2\alpha_3$ confuses proper subgroups of V.

Suppose μ is a fixed–point–free automorphism of V of prime order (q say) such that $\mu\alpha_1\alpha_2\alpha_3 = \alpha_1\alpha_2\alpha_3\mu$. Since $\lambda(V)$ is, by §.2 characteristic, the elements of $\lambda(V)\backslash\{0\}$ and $V\backslash\lambda(V)$ (respective orders $\frac{1}{2}|V| - 1$ and $\frac{1}{2}|V|$) are, under μ, partitioned into q element subsets. This is a contradiction (q cannot divide $\frac{1}{2}|V|$ and $\frac{1}{2}|V| - 1$). No such μ exists and an application of 3.2 completes the proof of the theorem.

10. Proving 1.1 simplified

Let $p \geq 5$ be a prime. It is a very pleasing fact that, the question of which $M_0(V)$ (V not elementary two) are p–gen can be solved. The full solution of this problem was announced in the statement of 1.1. Here we move toward the proof of this theorem. The material of sections two to nine is a lead up to 10 to 13. What they have done is establish an essential ingredient (viz. 9.1) needed for the proof.

At this stage in developments the group invariant $\delta(V)$ comes into its own. Possibly it may seem strange that it has not appeared sooner. However, there is reason for this. Only V with $|V| \leq 3p$ need involve its use. Thus 9.1 has fully covered the p–gen nature of $M_0(V)$ where consideration of $\delta(V)$ is irrelevant. Since that is what 9.1 achieves, we must now use this important invariant. Things start with a proposition.

Proposition 10.1. If V is a group, then a subset S of V^* of order $> |V^*| - \delta(V)$, must contain the non-zero elements H^* of a non-zero subgroup H of V.

Proof. Clearly $|S| \geq 1$ and V is non–trivial. Let A_i, $i = 1, \ldots, \delta(V)$, be the collection of all cyclic subgroups of V of prime order. If S does not contain an H^* (H as indicated), then for each A_i, $i = 1, \ldots, \delta(V)$, we can find non–zero a_i in A_i, not in S. Thus $S \subseteq V^* \backslash \{a_1, \ldots, a_{\delta(V)}\}$ and $|S| \leq |V^*| - \delta(V)$, contrary to the nature of S. 10.1 has been proved.

In one direction the proof of 1.1 is not that difficult. It is easy enough to show that V (not elementary two) with p–gen $M_0(V)$ ($p \geq 5$ a prime) cannot be in $\mathcal{D}^{\#}(1,p)$, $\mathcal{D}(2,p)$ or $\mathcal{D}(3,p)$. This is the contents of the proposition that follows.

Proposition 10.2. If $p \geq 5$ is a prime, then no group V in $\mathcal{D}^{\#}(1,p)$, $\mathcal{D}(2,p)$ or $\mathcal{D}(3,p)$ has p–gen $M_0(V)$.

Proof. If V is in $\mathcal{D}^{\#}(1,p)$ and $M_0(V)$ is p-gen, then we can find α in $u(M_0(V))$ of order p such that $N(\alpha) = M_0(V)$. By §.3, $M(\alpha)$ (a subset of V^*) has order $\equiv 0 \ mod\ p$ and has $\geq p$ elements. This implies $|V| > p$ contrary to the nature of $\mathcal{D}^{\#}(1,p)$. Thus, no V in $\mathcal{D}^{\#}(1,p)$, is such that $M_0(V)$ is p-gen.

If V is in $\mathcal{D}(2,p)$ or $\mathcal{D}(3,p)$ and $M_0(V)$ is p–gen, then there exists α in $u(M_0(V))$ of order p such that $N(\alpha) = M_0(V)$. Because $|M(\alpha)| \equiv 0 \ mod\ p$ and $|M(\alpha)| = p$, when $|V^*| < 2p$ and $|M(\alpha)| = p$ or $2p$, when $|V^*| < 3p$, it must follow that $\delta(V) > |M(\alpha)|$. Thus $|F(\alpha)| = |V^* \backslash M(\alpha)| > |V^*| - \delta(V)$ and, by 10.1, $F(\alpha)$ contains the non–zero elements H^* of a non–zero subgroup H of V. Because $M(\alpha)$ is non–empty, H is proper and a proper non–zero α–invariant subgroup of V. This would imply $H.N(\alpha) \subseteq H$, contrary to the fact that $N(\alpha) = M_0(V)$. Thus 10.2 stands proved.

The proof of 1.1 can be reduced to considering groups with $|V| > 2p$, $|V| \leq 3p$ and $\delta(V) \leq 2p$. This is what this section is about. We prove:-

Lemma 10.3. To prove 1.1 it is only required that we show that if $p \geq 5$ is a prime then a group V (not elementary two) with $2p < |V| \leq 3p$ and $\delta(V) \leq 2p$ has p–gen $M_0(V)$.

Proof. By 10.2 it must be shown that a V (not elementary two) not in $\mathcal{D}^{\#}(1,p) \cup \mathcal{D}(2,p) \cup \mathcal{D}(3,p)$ with $M_0(V)$ not p–gen has $2p < |V| \leq 3p$ and $\delta(V) \leq 2p$.

Firstly 9.1 implies $|V| \leq 3p$. Secondly as V is not in $\mathcal{D}^{\#}(1,p)$ and $\mathcal{D}^{\#}(1,p)$ is clearly all groups G (G not elementary two) with $|G| \leq p$

we see $|V| > p$. This means the possibilities for $|V|$ are $p < |V| \leq 2p$ or $2p < |V| \leq 3p$.

Case 1. This is where $p < |V| \leq 2p$. Here we have $\delta(V) \leq p$ or $\delta(V) > p$ but since when $\delta(V) > p$, V is in $\mathcal{D}(2, p)$ this situation cannot occur. Thus we may define α on V as $[v_1, \ldots, v_p]$ where the p elements v_i, $i = 1, \ldots, p$, of V^* (of order $\geq p$) contain a non-zero element of every non-zero cyclic subgroup of V of prime order (possible because $\delta(V) \leq p$). Clearly α has order p and confuses proper subgroups of V (a non–zero α–invariant subgroup of V has an element in $M(\alpha)$ so that $M(\alpha)$ is contained in it — also $|M(\alpha) \cup \{0\}| > \frac{1}{2}|V|$). Clearly there is no fixed–point–free automorphism μ of prime order q such that $\alpha\mu = \mu\alpha$. This is because $M(\alpha)\mu = M(\alpha)$, q divides $|M(\alpha)|$ and must be p, while q divides $|F(\alpha)| < p$. So 3.2 applies and $M_0(V)$ is p–gen.

Case 2. This is where $2p < |V| \leq 3p$. Here we have $\delta(V) \leq 2p$ or $2p < \delta(V)$ but when $2p < \delta(V)$, V is in $\mathcal{D}(3, p)$ and as this situation does not occur we are only left with the possibility of V being such that $2p < |V| \leq 3p$ and $\delta(V) \leq 2p$. Lemma 10.3 is completely proved.

By 10.3 we are now looking at groups V (not elementary two) with $2p < |V| \leq 3p$ and $\delta(V) \leq 2p$, with a view to proving $M_0(V)$ is p–gen (here p is a prime ≥ 5). A lemma that will be of assistance with this is the following.

Lemma 10.4. Let $p \geq 5$ be a prime and V a group of even order $> 2p$ and $\leq 3p$. If α in $u(M_0(V))$ has order p, then there is no fixed–point–free automorphism μ of V of prime order (q say) such that $\alpha\mu = \mu\alpha$.

Proof. Suppose such a μ (prime order q) exists. Since $M(\alpha) \subseteq V^*$ and has order divisible by p (α is a product of mutually disjoint p–cycles) we must have $|M(\alpha)| = p$ or $2p$. From sections two and three $M(\alpha)\mu = M(\alpha)$ and $M(\alpha)$ is partitioned into q element subsets. Thus q divides p or $2p$. In the second case, $q = 2$ or $q = p$. The $q = 2$ possibility cannot occur since by 2.9, μ would fix elements of $\eta(V)$. Thus, in either case, $q = p$. Now, $V^* = V \backslash \{0\}$ is partitioned into q ($= p$) element subsets under μ, and because $|V^*| < 3p$ and $\geq 2p$, it follows that $|V^*| = 2p$. This is a contradiction (V has even order) and 10.4 is proved.

11. Moving into proving 1.1

The three sections ten to twelve are involved in final considerations that establish 1.1. The point of the last was to reduce the proof of 1.1 to looking at those V with $2p < |V| \leq 3p$ and $\delta(V) \leq 2p$ (see 10.3). As

far as this situation goes there are three cases. This section deals with the two cases that arise when V has involutions that do not additively centralize each other. This means that section twelve is about those V which have a largish elementary two subgroup and finalizing the proof of 1.1.

The first lemma we prove is the following.

Lemma 11.1. Let $p \geq 5$ be a prime and V a group of order $> 2p$ and $\leq 3p$ such that $\delta(V) \leq 2p$. If V has a subgroup of the form D_{p_1} (p_1 an odd prime), then $M_0(V)$ is p–gen.

Proof. Since $|V^*| \geq 2p$ and $\delta(V) \leq 2p$, we can take a subset S of V^* consisting of $2p$ elements and such that, S contains a non–zero element of every cyclic subgroup of V of prime order. Now the subgroup D_{p_1} of V, contains a cyclic subgroup C_{p_1} of order p_1 with an element $a \neq 0$ in S. Also $C_{p_1} = \lambda(D_{p_1})$ (see §.2) so that $D_{p_1} \backslash C_{p_1}$ consists of p_1 involutions. Take b, c and d as three such involutions (possible because $p_1 \geq 3$). Clearly $\{b, c, d\}$ is contained in S. Also, because $\langle c, d\rangle > \langle c\rangle$ and $\langle c\rangle$ is a maximal subgroup of D_{p_1} ($|D_{p_1}| = 2p_1$), it readily follows that

$$\langle a, b\rangle = \langle c, d\rangle = D_{p_1}. \tag{11.11}$$

Let the elements of S be $g_1, \ldots, g_{2p}$, where $g_1 = a$, $g_2 = b$, $g_{p+1} = c$ and $g_{p+2} = d$. The other g's come from the remainder $S\backslash\{a, b, c, d\}$ of S which by definition contains a non–zero element of every cyclic subgroup of V of prime order (elements of $\{a, b, c, d\}$ are amongst these). Define

$$\alpha = [g_1, \ldots, g_p][g_{p+1}, \ldots, g_{2p}].$$

Clearly α is in $u(M_0(V))$ and has order p. By 3.2 and 10.4 (V has even order as D_{p_1} is a subgroup), the lemma will follow if it is shown that α confuses proper subgroups of V.

If H is a non–zero α–invariant subgroup of V, then H contains a subgroup of prime order and, the manner in which S was chosen, ensures $\{g_1, \ldots, g_{2p}\}$ contains an element of H. If this is in $\{g_1, \ldots, g_p\}$, then because H is $[g_1, \ldots, g_p]$–invariant, it follows that $\{g_1, \ldots, g_p\}$ and $\{a, b\}$ are contained in H. By (11), $\langle a, b\rangle = \langle c, d\rangle$ and c and d are in H, so that being $[g_{p+1}, \ldots, g_{2p}]$–invariant, H contains $\{g_1, \ldots, g_{2p}\}$. Thus if $\{g_1, \ldots, g_p\}$ contains an element of H, then $S \subseteq H$. The alternative is that $\{g_{p+1}, \ldots, g_{2p}\}$ contains an element of H. A very similar argument to that above (again using (11)), shows that in this case also, $S \subseteq H$. Simple order arguments mean $H = V$ and 11.1 is proved.

The next lemma is, in some regards, very similar to 11.1. It deals with p and V as in 11.1, except that, rather than V having a subgroup of the form D_{p_1} (p_1 an odd prime), it contains a subgroup of the form D_4.

Lemma 11.2. Let $p \geq 5$ be a prime and V a group of order $> 2p$ and $\leq 3p$ such that $\delta(V) \leq 2p$. If V has a subgroup of the form D_4, then $M_0(V)$ is p–gen.

Proof. Since $|V^*| \geq 2p$ and $\delta(V) \leq 2p$, we can take a subset S of V^* consisting of $2p$ elements and such that, S contains a non–zero element of every cyclic subgroup of V of prime order. Now the subgroup D_4 of V, contains a cyclic subgroup C_4 with generator d_1. Since d_1 has order four, it is in $\lambda(D_4)$, which coincides with C_4 (see §.2). Let a be an element of $D_4 \backslash C_4$. All elements of $a + C_4$ are in $D_4 \backslash \lambda(D_4)$ and thus in $\eta(D_4)$. Let $b = a + d_1$, $c = a + d_1 2$ and $d = a + d_1 3$. It follows that because $\langle a, b\rangle$ contains a and d_1, it must coincide with D_4. Similarly, $\langle c, d\rangle$ contains c and d_1 and coincides with D_4. Clearly, $\{a, b, c, d\}$ (a subset of $\eta(V)$) is contained in S and, from what has just been shown,

$$\langle a, b\rangle = \langle c, d\rangle = D_4. \tag{11.12}$$

Let the elements of S be $g_1, \ldots, g_{2p}$, where $g_1 = a$, $g_2 = b$, $g_{p+1} = c$ and $g_{p+2} = d$. The other g's come from the remainder $S \backslash \{a, b, c, d\}$ of S which by definition contains a non–zero element of every cyclic subgroup of V of prime order (elements of $\{a, b, c, d\}$ are amongst these). Define

$$\alpha = [g_1, \ldots, g_p][g_{p+1}, \ldots, g_{2p}].$$

Clearly α is in $u(M_0(V))$ and has order p. By 3.2 and 10.4 (V has even order as D_4 is a subgroup), the lemma will follow if it is shown that α confuses proper subgroups of V. Here the proof that a non–zero α–invariant subgroup of V coincides with V, follows as in the last paragraph of the proof of 11.1, with (12) and (11) playing exactly the same role. 11.2 is therefore proved.

12. Finalizing the proof of 1.1

Lemma 10.3 reduced the proof of 1.1 to considering V with $2p < |V| \leq 3p$ and $\delta(V) \leq 2p$. Furthermore 11.1 and 11.2 have looked at such groups in the case of them having certain non–trivial dihedral subgroups. This in fact covers such groups where two involutions do not additively commute. Essentially all that remains is to consider the situation where there is a number of commuting involutions. So now only one preliminary result needs proving before 1.1 is finalized.

Lemmas 11.1 and 11.2 dealt with a wide assortment of groups and covering the commuting involution situation does also. Only the existence of seven mutually commuting involutions is required.

Lemma 12.1. Let $p \geq 5$ be a prime and V a group (not elementary two) of order $> 2p$ and $\leq 3p$ such that $\delta(V) \leq 2p$. If V has a subgroup of the form $C_2 \oplus C_2 \oplus C_2$, then $M_0(V)$ is p–gen.

Proof. Since $|V^*| \geq 2p$ and $\delta(V) \leq 2p$, we can take a subset S of V consisting of $2p$ elements and such that S contains a non–zero element of every cyclic subgroup of V of prime order. From the assumptions, V has a subgroup which is a direct sum $A_1 + A_2 + A_3$ of the subgroups A_i, $i = 1, 2, 3$, of order two. Let a_i, $i = 1, 2, 3$, be the non–zero elements of A_i. Define a_4 as $a_1 + a_2$, a_5 as $a_2 + a_3$ and a_6 as $a_1 + a_2 + a_3$. It is clear $\langle a_1, a_2, a_3\rangle$ must coincide with $A_1 + A_2 + A_3$, but also, since $a_4 + a_5 = a_1 + a_3$ and is distinct from a_6, we conclude that $\langle a_4, a_5, a_6\rangle$ coincides with $A_1 + A_2 + A_3$. It has been shown that

$$\langle a_1, a_2, a_3\rangle = \langle a_4, a_5, a_6\rangle = A_1 + A_2 + A_3. \tag{12.13}$$

Let the elements of S be $g_1, \ldots, g_{2p}$, where $g_1 = a_1$, $g_2 = a_2$, $g_3 = a_3$, $g_{p+1} = a_4$, $g_{p+2} = a_5$ and $g_{p+3} = a_6$ (the other g's come from the remainder $S\backslash\{a_1, \ldots, a_6\}$ of S). This is possible not only because $p \geq 3$, but also because,$\{a_1, \ldots, a_6\}$ is contained in $\eta(V)$ and therefore in S. Define

$$\alpha = [g_1, \ldots, g_p][g_{p+1}, \ldots, g_{2p}].$$

Clearly α is in $u(M_0(V))$ and has order p. By 3.2 and 10.4, the lemma will follow if it is shown that α confuses proper subgroups of V.

If H is a non–zero α–invariant subgroup of V, then H contains a subgroup of prime order and, the manner in which S was chosen, ensures that $\{g_1, \ldots, g_{2p}\}$ contains an element of H. If this is in $\{g_1, \ldots, g_p\}$, then because H is $[g_1, \ldots, g_p]$–invariant, it follows that, $\{g_1, \ldots, g_p\}$ and $\{a_1, a_2, a_3\}$ are contained in H. By (13), $\langle a_1, a_2, a_3\rangle = \langle a_4, a_5, a_6\rangle$ and a_4, a_5 and a_6 are in H, so that being $[g_{p+1}, \ldots, g_{2p}]$–invariant, H contains $\{g_1, \ldots, g_{2p}\}$. Thus if $\{g_1, \ldots, g_p\}$ contains an element of H, then $S \subseteq H$. The alternative is that $\{g_{p+1}, \ldots, g_{2p}\}$ contains an element of H. A very similar argument to that above (again using (13)), shows in this case also, $S \subseteq H$. Simple order arguments mean $H = V$. 12.1 is therefore proved.

Everything is now in place for the final assault on 1.1.

Proof of 1.1. By 10.3, 1.1 will be proved if it is shown that, when $p \geq 5$ is a prime and V a group of order $> 2p$ and $\leq 3p$ such that $\delta(V) \leq 2p$, then it follows that $M_0(V)$ is p–gen. By 4.1 it can and will also be assumed

$\eta(V) \neq \emptyset$. For such a group, it will be shown that we may assume any two elements a and b of $\eta(V)$, additively centralize each other. If a and b do not additively centralize each other, then from §.2 $\langle a, b\rangle$ is a dihedral group of the form D_n, where n is an integer ≥ 3 (the case of $n = 2$ is where $D_n = C_2 \oplus C_2$ and a and b commute). The cyclic subgroup C_n $(= \lambda(D_n))$ of D_n, therefore contains an element of order p_1 ($p_1 \geq 3$ a prime) or order four. It readily follows that D_n contains a subgroup of the form D_{p_1} or D_4 (this can be taken as the normal C_{p_1} or C_4 subgroup of D_n extended by $\langle a\rangle$). From 11.1 and 11.2, $M_0(V)$ is p–gen and thus it can be assumed $\langle a, b\rangle$ is abelian. Hence $i(V)$ is an elementary 2-subgroup of V. It follows readily, from 12.1, that it can be assumed $|i(V)| \leq 4$. Thus $|\eta(V)| \leq 3 \leq \frac{1}{3}|V|$ ($p \geq 5$ and $|V| > 2p$). From 4.1, $M_0(V)$ is necessarily p–gen and theorem 1.1 is established.

13. Discussion

Theorem 1.1, [4], [5] and [1] mean we can determine when a V (not elementary two) has p–gen $M_0(V)$ (p a prime). For $p = 2$ and 3 it is [4] and [5] that respectively allow this. For $p \geq 5$ there is now enough information on $\delta(V)$ at hand (see [1]) so that theorem 1.1 can be applied.

Understanding of when $\delta(V) > \frac{1}{2}|V| - 1$ means, given a prime $p \geq 5$ it can quickly be decided if V is in $\mathcal{D}(2, p)$ or $\mathcal{D}(3, p)$. Since $\mathcal{D}^{\#}(1, p)$ is simply all V (not elementary two) with $|V| \leq p$ the problem is, in a sense solved. Certainly for $p \geq 5$ there is no general presentation of what $\mathcal{D}(2, p)$ and $\mathcal{D}(3, p)$ look like. However, given $p \geq 5$ and a V, rapid determination of whether V lies in $\mathcal{D}(2, p)$ or $\mathcal{D}(3, p)$ is possible. This is an agreeable fact that rests on what T. Burness and myself have proved in [1]. Just how this is the case will now be explained.

A group V in $\mathcal{D}(2, p)$ has $|V| \leq 2p$ and $\delta(V) > p$ so that $\delta(V) > \frac{1}{2}|V| > \frac{1}{2}|V| - 1$. A group V in $\mathcal{D}(3, p)$ has $|V| \leq 3p$ and $\delta(V) > 2p$ so that $\delta(V) > \frac{2}{3}|V| > \frac{1}{2}|V| - 1$. This means knowing the value of $\delta(V)$ and groups V with $\delta(V) > \frac{1}{2}|V| - 1$ supplies precise information on whether V is in $\mathcal{D}(2, p)$ or $\mathcal{D}(3, p)$. In fact what we need only know is the V and $\delta(V)$ when $\delta(V) > \frac{1}{2}|V|$ to do this.

In reference to the above, covering what [1] has achieved will now be undertaken. There those V having $\delta(V) > \frac{1}{2}|V| - 1$ were classified. However, since determining when $M_0(V)$ is p–gen only requires we know when $\delta(V) > \frac{1}{2}|V|$ the full force of the main theorem of [1] is not used here. What [1] states about groups V with $\delta(V) > \frac{1}{2}|V|$ is now uncovered.

There arise in [1] eight possibilities for V with $\delta(V) > \frac{1}{2}|V|$. Type (I) is groups G of the form $D(A)$ (A abelian) having order $2|A|$ and

$\delta(G) = |G|/2 + \delta(A)$. Type (II) is groups G of the form $D_4 \oplus D_4 \oplus E$ (E elementary two of order 2^n) having order 2^{n+6} and $\delta(G)$ being $\frac{9}{16}|V| - 1$. Type (III) is groups of the form $H(r) \oplus E$ ($r \geq 1$ an integer) having order 2^{2r+n+1} with $\delta(G) = |G|/2 + 2^{n+r} - 1$, while type (IV) is those of the form $S(r) \oplus E$ having the same order and same $\delta(G)$. Type (V) is groups G of the form $T(r)$ (see [1]) having order 3.2^{2r} and $\delta(G)$ being $\frac{2}{3}|G| - 1$. The remaining three cases (types (VIII), (IX) and (X) in accordance with [1]) consist of individual groups. (VIII) is simply $S_3 \oplus S_3$ (S_3 the symmetric group on three letters). Here the order of G is 36 and $\delta(G) = 19$. (IX) is simply S_4 (the symmetric group on four letters). Here the order of G is 24 and $\delta(G) = 13$, while type (X) is A_5 with $|G| = 60$ and $\delta(G) = 31$.

The type of groups found in $\mathcal{D}(2,p)$ or $\mathcal{D}(3,p)$ (p a prime ≥ 5) can be restricted still further. It is now shown how types (VIII), (IX) and (X) (the cases where we have isolated groups) need not concern us. For $V = S_3 \oplus S_3$ to be in a $\mathcal{D}(2,p)$ it is necessary that $|V| = 36 \leq 2p$ so that $p \geq 18$ is ≥ 19 while $\delta(V) = 19 > p$. For $S_3 \oplus S_3$ to be in $\mathcal{D}(3,p)$ it is necessary that $p \geq 12$ while $\delta(V) = 19 > 2p$. Thus $S_3 \oplus S_3$ is never in $\mathcal{D}(2,p) \cup \mathcal{D}(3,p)$. For $V = S_4$ to be in $\mathcal{D}(2,p)$ it is necessary that $|V| = 24 \leq 2p$ so that $p \geq 12$ is ≥ 13 while $\delta(V) = 13 > p$. For S_4 to be in $\mathcal{D}(3,p)$ it is necessary that $|V| = 24 \leq 3p$ and $p \geq 11$ while $\delta(V) = 13 > 2p$. Thus S_4 is never in $\mathcal{D}(2,p) \cup \mathcal{D}(3,p)$. For $V = A_5$ to be in $\mathcal{D}(2,p)$ it is necessary that $|V| = 60 \leq 2p$ and p be ≥ 31 while $\delta(V) = 31$ be $> p$. For A_5 to be in $\mathcal{D}(3,p)$ it is necessary that $60 \leq 3p$ or $p \geq 20$ while $\delta(V) = 31$ be $> 2p$. Thus A_5 is never in $\mathcal{D}(2,p) \cup \mathcal{D}(3,p)$.

The last paragraph shows that in determining groups in $\mathcal{D}(2,p) \cup \mathcal{D}(3,p)$ ($p \geq 5$ a prime) we need only look amongst groups of type (I) to (V). The statement of 1.1 therefore becomes:- A group V (not elementary two) is p-gen ($p \geq 5$ a prime) if and only if none of the following occur

(i) $|V| \leq p$,

(ii) $|V| \leq 2p$ and V is of type (I) to (V) with $\delta(V) > p$, and

(iii) $|V| \leq 3p$ and V is of type (I) to (V) with $\delta(V) > 2p$.

Moreover, since for V of order $\leq 2p$ (or $3p$) we know when $\delta(V) > p$ (when $\delta(V) > 2p$) the groups of (ii) and (iii) are determined.

It would now seem appropriate to give an example based on what is set out above. This consists of specifying all V (not elementary two) which are 31–gen. The prime 31 has been chosen because it is fairly easy to establish which $M_0(V)$ are 31–gen. For 37 things are more difficult. There groups of the form $S(r) \oplus E$ and $H(r) \oplus E$ (E elementary two) creep into those belonging to $\mathcal{D}(2,p)$ ($p = 37$). Also, in spite of this for $p = 37$ there are many more groups in $\mathcal{D}(2,p)$. First considerations for $p = 31$ involve finding the groups of $\mathcal{D}(3,p)$. V is in $\mathcal{D}(3,31)$ if $|V| \leq 3.31 = 93$ and $\delta(V) > 2.31 = 62$. Here $\delta(V) > \frac{2}{3}|V| - 1$ and since $\frac{2}{3} > \frac{5}{8}$ no groups

of type (II), (III), (IV) or (V) (other than those of type (I)) can arise (see [1]). So we are looking at $D(A)$'s where $\delta(A) > \frac{1}{6}|V| - 1$ (ie. A abelian with $\delta(A) > \frac{1}{3}|A| - 1$). It is easily checked that the only possibilities for A are $C_4 \oplus E$ (E elementary two) or A an elementary 3–group (here $\delta(A) = \frac{1}{2}|A| - \frac{1}{2}$). These give rise to a V (ie. $D(A)$) with order 2^m or order 2.3^{m_1} (m and m_1 integers ≥ 1). The only V with such order in the range 62 to 93 has $|V| = 2^6$ ($A = C_2 \oplus C_2 \oplus C_2 \oplus C_4$) but as V ($= D(A)$) has $\delta(V) = 47$ such a V is not in $\mathcal{D}(3, 31)$.

Continuing with the example of $p = 31$, we seek to determine $\mathcal{D}(2, 31)$. If V is in $\mathcal{D}(2, 31)$, then $|V| \leq 62$ and $\delta(V) > 31$. As $T(r)$'s have order $2^{2r}.3$ ($r \geq 1$ an integer) with $\delta(T(r)) = \frac{2}{3}|T(r)| - 1$ no $T(r)$ occurs ($T(2)$ just misses out because $\delta(T(2)) = 31$). For V of the form $S(r) \oplus E$ or $H(r) \oplus E$ (E elementary two) the only possibility not of type (I) is $r = 2$ and $E = \{0\}$. Here $\delta(V) = \frac{5}{8}|V| - 1 = 19$ so such a V is not in $\mathcal{D}(2, 31)$. Clearly no groups of type (II) are in $\mathcal{D}(2, 31)$ (here $|V| \geq 64$). Thus all V in $\mathcal{D}(2, 31)$ are $D(A)$'s.

Specifying the groups of $\mathcal{D}(2, 31)$ is the same as specifying the $D(A)$'s in $\mathcal{D}(2, 31)$. Now a $D(A)$ ($= V$) has $\delta(V) = |A| + \delta(A)$ and for A not elementary two $\delta(A) \leq \frac{1}{2}|A| - \frac{1}{2}$ (equality occurring when A is an elementary abelian 3–group). Thus $\delta(V) \leq \frac{3}{4}|V| - \frac{1}{2}$. However a $D(A)$ ($= V$) in $\mathcal{D}(2, 31)$ has order ≤ 62 with $\delta(V) > 31$ so that $32 \leq \frac{3}{4}|V| - \frac{1}{2}$ and $|V| \geq 44$ so $|A| \geq 22$ and ≤ 31. We now look at possible A (abelian) that can occur. $|A| = 22$ gives $A = C_{22}$, $\delta(A) = 2$ and $\delta(V)$ not > 31. $|A| = 23$ gives $A = C_{23}$, $\delta(A) = 1$ and $\delta(V)$ not > 31. $|A| = 24$ gives $\delta(A) \leq 7$ unless $A = C_2 \oplus C_2 \oplus C_2 \oplus C_3$ (here $\delta(A) = 8$). Thus for $|A| = 24$ only $D(C_2 \oplus C_2 \oplus C_2 \oplus C_3)$ is in $\mathcal{D}(2, 31)$. $|A| = 25$ gives $\delta(A) \leq 6$ and $\delta(V)$ not > 31. $|A| = 26$ gives $\delta(A) = 2$ and $\delta(V) = 28$ not > 31. $|A| = 27$ gives $\delta(A) = 1$, 4 or 13 (the last occurring for $A = C_3 \oplus C_3 \oplus C_3$) so that for $|A| = 27$ only $D(C_3 \oplus C_3 \oplus C_3)$ is in $\mathcal{D}(2, 31)$. For $|A| = 28$, $\delta(A)$ is 2 or 4 (when $A = C_2 \oplus C_2 \oplus C_7$) so that only $D(C_2 \oplus C_2 \oplus C_7)$ is, for $|A| = 28$, in $\mathcal{D}(2, 31)$. For $|A| = 29$, $\delta(A) = 1$ and $\delta(V) = 30$ not > 31. For $|A| = 30$, $A = C_{30}$, $\delta(A) = 3$ and $\delta(V) = 33 > 31$ so D_{30} is in $\mathcal{D}(2, 31)$. For $|A| = 31$, $\delta(A) = 1$ and D_{31} is in $\mathcal{D}(2, 31)$.

Putting together all the material of the above four paragraphs we see that a V (not elementary two) has 31–gen $M_0(V)$ if and only if V is not one of the following. A group of order ≤ 31. Also not one of the groups $D(C_2 \oplus C_2 \oplus C_2 \oplus C_3)$, $D(C_3 \oplus C_3 \oplus C_3)$, $D(C_2 \oplus C_2 \oplus C_7)$, D_{30} or D_{31}.

Before finishing this paper we address questions that 1.1 raise. In the statement of 1.1 only the families $\mathcal{D}^{\#}(1, p)$, $\mathcal{D}(2, p)$ and $\mathcal{D}(3, p)$ arise, so it can be asked why $\mathcal{D}(n, p)$ with $n \geq 4$ do not occur? If we look at groups V (not elementary two) with $\delta(V) > \frac{2}{3}|V|$, paragraphs four to six of this

section supply the fact that such a V must be of type (I) (ie. $D(A)$'s) and have $\delta(V) = |V|/2 + \delta(A)$. This means we are looking at abelian groups A with $\delta(A) > \frac{1}{3}|A|$. It is an easy matter to check that the only such A are of the form $C_4 \oplus E$ (here $\delta(A) = \frac{1}{2}|A| - 1$) or A an elementary abelian 3–group (here $\delta(A) = \frac{1}{2}|A| - \frac{1}{2}$). The V (ie $D(A)$) in these cases has $\delta(V)$ which is respectively $\frac{3}{4}|V| - 1$ and $\frac{3}{4}|V| - \frac{1}{2}$. Thus all V (not elementary two) have $\delta(V) \leq \frac{3}{4}|V|$. Since this implies $\mathcal{D}(n, p)$, $n \geq 4$, is empty it becomes apparent why such a family is excluded.

Above analysis yields even more. We see that $\mathcal{D}(3, p)$ can contain at most only two groups ($D(A)$'s with A one of the two groups given above). Often $\mathcal{D}(3, p)$ will be empty (simple order arguments ensure this). From time to time it will contain one of the two $D(A)$'s specified and quite infrequently, when the order of both $D(A)$'s conform with being $\leq 3p$ and having $\delta(V) > 2p$, it necessarily contains both.

The mystery of when $M_0(V)$ (V not elementary two) is p–gen has been resolved. Basic (in a sense complete) understanding of the families $\mathcal{D}^{\#}(1, p)$, $\mathcal{D}(2, p)$ and $\mathcal{D}(3, p)$ has been supplied. Why it is that the $\mathcal{D}(n, p)$ ($n \geq 4$) do not occur has been covered. Also the somewhat rudimentary nature of the family $\mathcal{D}(3, p)$ has been given coverage. What more remains? There are still questions that arise. Reasonably tight upper and lower bounds for $|\mathcal{D}(2, p)|$ (in terms of p) would be of quite real interest. Questions as to what happens when p is of a special nature surface and, of course there remains the deep and intriguing question of when $M_0(V)$ is n–gen (n any integer ≥ 2).

References

[1] T. C. Burness and S. D. Scott, *On the Number of Prime Order Subgroups of Finite Groups*, J. Austr. Math. Soc **87** (2009), 329–357.

[2] D. Gorenstein, *Finite Groups*, Harper and Row, New York (1968).

[3] G. Pilz, *Near–rings*, North–Holland Pub. Amsterdam (1983).

[4] S. D. Scott, *Involution Near–rings*, Proc. Edin. Math. Soc **22** (1979), 241–245.

[5] S. D. Scott, *Transformation Near–rings Generated by a Unit of Order Three*, Alg. Col. **4:4** (1997), 371–392.

[6] C. T. C. Wall, *On Groups Consisting Mostly of Involutions*, Proc. Camb. Phil. Soc **67** (1970), 251–262.

CONTACT INFORMATION

S. D. Scott University of Auckland, New Zealand

Received by the editors: 24.04.2010
and in final form 08.09.2012.