Generation of $M_0(V)$ from a Group Theory Perspective

What is the biggest problem (solved or unsolved) that algebra has presented us with? It seems somewhat reasonable to suggest that it is the classification of all finite simple groups. Having, in some sense, given an answer to this question we come to another. What is the biggest problem (unsolved) that algebra has presented us with? It is within possibility that it is solving the n-gen problem (ie. when is the nearring $M_0(V)$ generated by a unit of order n?). In this talk we shall see that the first problem has a great deal of bearing on the second.

In this talk I shall cover something of what is known about the n-gen problem and indicate how Tim Burness and I have solved a very meaningful group theory problem it has tossed up. The solution to the group theory problem rests quite strongly on finite simple group classification.

How is $M_0(V)$ generated? Can it be generated by a single element? This was shown to be the case generally, in my 1979 paper [2], in the Proc. Edin. Math. Soc. The element α involved was a very simple one. It satisfied $\alpha^2=1$. However, much much more to do with $M_0(V)$ generation was possible. The subnearring $N(\alpha)$ of $M_0(V)$ generated by a single element α of $M_0(V)$ is countable and cannot generate $M_0(V)$ when V is infinite as card($M_0(V)$) is uncountable. What [2] says is that for finite V things are radically different. Here a very special unit generates $M_0(V)$. In this regard it should also be noted that when α is not a unit then in no way is $N(\alpha)=M_0(V)$. This is because the set of all β in $M_0(V)$ such that $a\beta=b\beta$ (a and b distinct elements of V) is a proper subnearring of $M_0(V)$. So straight away the generation problem (when does $N(\alpha)=M_0(V)$) imposes on us the finiteness of V and that α is a unit.

Since we are dealing with the symmetric group on the finite set V^* (explain) there is not much that can be said about units generally except that they have an order n say. So a very real problem that presents itself is given an integer n>1 when is $M_0(V)$ (V a finite group) n-gen (generated by a unit of order n). This problem is 'completely solved' in the case of n a prime and is starting to give up its secrets in the case of composite n. In fact the p-gen problem almost seems more complex than the n-gen one (although the solution of the n-gen one is expected to be much much more substantial). What is meant by the word 'completely' used above? It is this:- given a group V and prime p there is now theory that quickly allows us to decide if $M_0(V)$ is p-gen. A large section of this theory is essentially nearring material (although quite meaningful group theory is involved). However the nearring solution is supplied within a group theory framework and this quite deep secondary matter is what most of this talk is about.

The introduction to the group theory problem requires we now briefly cover what nearring considerations yield. This nearring aspect is what my 2007 conference talk was concerned with. If V is a group then the number of minimal subgroups of V (ie.

number of subgroups of prime order) will be denoted by $\delta(V)$. One would expect that in general $\delta(V)$ is considerably less than $|V|$. Apart from elementary two groups this is indeed the case. In fact apart from such groups $\delta(V)\leq 3|V|/4-1/2$. We now define some classes of groups in terms of $\delta(V)$. Given a prime p we let D(n,p), n=1,2,…, be all groups V (not elementary two) of order $\leq np$ where $\delta(V)>(n-1)p$. From above D(n,p) is empty when $n\geq 4$. However, D(n,p) is frequently enough empty when n=3 and generally contains many groups when n=2. For n=1 it is simply all groups (non-zero and not elementary two) of order $\leq p$. With In(p) as all elementary two groups of order incongruent to 1 mod p, we can state the theorem following. This is the main theorem of my 318 page unpublished paper 'Generators of Finite Tranformation Nearrings'. Much of the talk I gave at the 2007 conference was about it.

Theorem A If p is a given prime ≥ 5 (2 and 3 are dealt with in the literature) then $M_0(V)$ is p-gen if and only if V does not belong to one of the following mutually exclusive classes

$$\text{In}(p),\ D^{\#}(1,p),\ D(2,p) \text{ and } D(3,p).$$

The classes $D^{\#}(1,p)$, D(2,p) and D(3,p) are finite, $D^{\#}(1,p)$ is all groups (not elementary two) of order $\leq p$, D(2,p) is all groups (not elementary two) of order $\leq 2p$ with $\delta(V)>p$ and D(3,p) is all groups (not elementary two) of order $\leq 3p$ with $\delta(V)>2p$. This means our theorem (together with results from classification of 2-gen and 3-gen $M_0(V)$) yield the following corollary:-

Corollary If p is a prime then, apart from a finite number of exceptions $M_0(V)$ is p-gen if and only if V is not an elementary 2-group of order incongruent to 1 mod p.

This corollary goes a long way but we want precise information. We want to know what the exceptions are and to do this we must classify the groups of D(2,p) and D(3,p). This will be achieved if we classify groups V where $\delta(V)>|V|/2$. However, in keeping with a paper of C.T.C Wall (explain what the main theorem of this paper achieves) leading somewhat in this direction, we seek a classification of finite groups V with $\delta(V)>|V|/2-1$. This is the problem Tim Burness and I have solved. The key theorem here demonstrates such a group has a rather straightforward structure. It is interesting to note that $G=A_5$ is the only non-soluble group with $\delta(G)>|G|/2-1$ while $\delta(G)=|G|/2$ (C_2 exempt) if and only if $G=S_3\pm D_4\pm E$ (explain). We are now almost in a position of being able to state the group theory theorem which gives us full understanding of the nearring one (ie. full understanding of the groups in D(2,p) and D(3,p)). To do this we list ten families of groups

(I) G=D(A) the generalised dihedral group on the abelian group A (explain this),

(II) $G=D_4\pm D_4\pm E$ (explain),

(III) $G=H(r)\pm E$, where $H(r)$ is the direct sum of r copies of D_4 which are completely amalgamated on their centres (explain),

(IV) $G=S(r)\pm E$, where $S(r)$ is the direct sum of r copies of $C_2\pm C_2$ extended by a C_2 acting as the wreath product on each $C_2\pm C_2$ (explain this and also that (I) to (IV) are precisely the groups with $i_2(G)>|G|/2-1$),

(V) $G=T(r)$, where $T(r)$ is the direct sum of r copies of $C_2\pm C_2$ extended by a C_3 where the C_3 acts on each $C_2\pm C_2$ as an A_4 (explain this),

(VI) G is a group of exponent three (explain),

(VII) G is a $S_3\pm D_4\pm E$,

(VIII) G is a $S_3\pm S_3$,

(IX) G is a S_4 , and

(X) G is a A_5 .

With the class of groups which belong to any of (I) to (X) called L we have the following theorem

Theorem B A non-trivial finite group G has $\delta(G)>|G|/2-1$ if and only if G is in L.

The precise value of $\delta(G)$ for each G in L can be listed according to whether it belongs to (I), (II)… or (X), and allows us to determine exactly what groups are in D(2,p) or D(3,p) (given p --- see theorem A).

The proof of theorem B involves us in a relatively deep group theory investigation. It will be outlined how this goes. One of the first things to note is that the proof can in some sense be handled inductively. We have:-

Lemma B_1 If G is a finite group with proper normal subgroup H where $\delta(G/H)\leq|G/H|/2-1$ then $\delta(G)\leq|G|/2-1$.

The second thing to note is that, in a sense, quite often we do not need to look further than elements of order two and three. Here we have another fairly easily proved lemma.

Lemma B_2 If $3+3i_2(G)+ i_3(G)\leq|G|$, then $\delta(G)\leq|G|/2-1$ (explain).

This last lemma is very relevant to the non-soluble situation but for the moment it is the first lemma we will talk about. If G is a finite group with a maximal normal subgroup H, then G/H is a finite simple group. This means it is a C_p (p a prime) or a finite non-abelian simple group. The case of $p\geq5$ certainly has $\delta(G/H)=1\leq|G/H|/2-1$ so B_1 gives the result. Thus G/H is a C_2 or a C_3 or a finite non-abelian simple group. It is the last case that is of immediate interest. According to B we should have for all finite non-abelian simple groups either $\delta(G)\leq|G|/2-1$ or $G=A_5$. This can be proved. In the

case of the alternating groups A_n $n>5$, we make use of B_2. Combinatorial arguments can be used to give precise expressions for $i_2(A_n)$ and $i_3(A_n)$ and then show $3+3i_2(A_n) + i_3(A_n)\leq|A_n|$. The argument here although quite clever is not that difficult. But non-abelian finite simple groups are divided into three categories. The alternatings, the sporadics and those of Lie type, so we are a third of the way through this initial problem. For the sporadics the character table of G is available in the GAP character library and it is easy enough to calculate $\delta(G)$ precisely. In all cases $\delta(G)\leq|G|/2-1$. Groups of Lie type remain. Certain exceptional cases are here dealt with by easy enough calculation or using GAP. The remaining cases can be handled without too much difficulty by using results that give bounds for $i_2(G)$ and $i_3(G)$ heavily based on what has been handed down to us by those who have worked on these groups. Using these bounds we show B_2 holds.

Our problem has been reduced to the situation where G/H is a C_2, C_3 or A_5. The nice thing about this is that when G/H is a C_2 all elements of order three are in H and when G/H is a C_3 all elements of order two are in H. This means there is some chance of applying B_2 in both cases. This is accomplished for non-soluble G. In the C_2 situation we have a result of Potter [1] telling us that $i_2(G)\leq 4|G|/15-1$. However, the elements of order three in a non-soluble group K are bounded by $7|K|/20-1$ (this is quite a big result with proof depending on investigation into the three classes of finite simple non-abelian groups and taking it further to the non-soluble case). So now in the C_2 situation $i_3(G)=i_3(H)\leq 7|G|/40-1$ and it follows that $3+3i_2(G)+ i_3(G)\leq| G|$. C_2 is dealt with for non-soluble G. For the C_3 case $i_2(G)=i_2(H)\leq 4|G|/45-1$ (see above) and $i_3(G)\leq 7|G|/20-1$ (above again) so that $3+3i_2(G)+i_3(G)\leq|G|$. For the A_5 with H non-soluble we again use the $7|G|/20-1$ bound, the fact that $i_2(H)\leq 3|H|/4-1$ (explain) and information about A_5 to obtain the result. The situation where H (non-zero) is soluble is easily enough dealt with (it depends on $\delta(A_5)$ being close to $|A_5|/2$ --- explain). The above process means showing theorem B holds can be reduced to the case of soluble G.

The fact that theorem B holds for soluble G is, in some ways, the hard part of the proof. However, something like this was known to me at the time of the 2007 conference. I had in place nearly all characterisation of G (soluble) for which $\delta(G)>|G|/2$. This material indicated that the $|G|/2-1$ bound might be more natural. So this is what Tim and I have done (classify all such G --- soluble or non-soluble). Tim's knowledge of finite simple groups (even finite non-soluble groups) was invaluable. Previously Erhard Aichinger and I had worked on the non-soluble group case. Our computer investigations indicated B held for these, but it was only experimental evidence. I am very grateful to everyone who has contributed to this effort, but particularly to Tim Burness for filling the non-soluble gap so successfully.

The problem has reduced to showing if G is a group (soluble) with a minimal normal subgroup (necessarily elementary abelian) H with G/H an L-group, then G is an L-group or $\delta(G) \leq |G|/2-1$. Thus we must look at the possibility of G/H being as in (I) to (IX). Three of these categories are not so hard to cover. First there is the situation (IX) where G/H is an S_4. Here $\delta(G) \leq |G|/2-1$. Next comes the situation where G/H is an $S_3 \pm S_3$. Here again $\delta(G) \leq |G|/2-1$. Next we look at (VII) where G/H is a $S_3 \pm D_4 \pm E$. This is only slightly different. Here G is a $S_3 \pm D_4 \pm E_1$ (explain) or $\delta(G) \leq |G|/2-1$.

Next in the proof for G soluble it is needful to look at certain G/K (K normal in G) of more elementary nature. The first is with K minimal normal and G/K an S_3. Here we have either G is a D(A) (A abelian of exp$\geq$3) or G a S_4 or G has $\delta(G) \leq |G|/2-1$. The second is with K elementary two and G/K a C_3. Here it follows that G is a T(r) $\pm$E or a $C_3 \pm$K. The only situation in this where $\delta(G)$ is not $\leq |G|/2-1$ is G a T(r) for some r$\geq$1. The third situation we look at is where K is an abelian 2-group of index nine. Here $\delta(G) \leq |G|/2-1$ (*).

At this stage things begin to become very much more complicated. It is not my intension to go into too much explanation but to outline what is reasonably accessible. A major result allowing more to be said about soluble G with G/H (H minimal normal) an L-group is the following. For soluble G with non-trivial normal subgroup K of odd order and G/K a 2-group we have either G is a D(A) (exp(A)$\geq$3) or G is a $S_3 \pm S_3$ or G is a $S_3 \pm D_4 \pm E$ or $\delta(G) \leq |G|/2-1$ (**). This allows the case of G/H of type (I) to be handled. Again this is a major result. Here we have either G is a 2-group or a D(B) (B abelian of exp$\geq$3) or G is a $S_3 \pm D_4 \pm E$ or G is a $S_3 \pm S_3$ or G is a S_4 or $\delta(G) \leq |G|/2-1$. The first case of G a 2-group introduces us to Wall's result [3] because here $\delta(G)$ is just $i_2(G)$ (explain). Thus in the case of G/H a D(A) we have either G is an L-group or $\delta(G) \leq |G|/2-1$. But (**) allows us to handle more. It is easy enough to see that it allows us to handle G/H being as in (II), (III) or (IV) because when H is elementary two G is a 2-group and Wall's theorem applies. So we have shown so far that when G/H is as in (I), (II), (III), (IV), (VII), (VIII) or (IX), then G is an L-group or $\delta(G) \leq |G|/2-1$.

All that remains is G/H being as in (V) or (VI). Here we assume G is minimal for not being an L-group or having $\delta(G) \leq |G|/2-1$. In both cases G has a maximal normal subgroup K of index three. If $\delta(K) \leq |K|/2-1$, then it is relatively easy to show $\delta(G) \leq |G|/2-1$. Thus the minimality of G allows the conclusion that K is an L-group. If K is of type (I), (VII), (VIII) or (IX), K has a maximal characteristic

subgroup K_1 of index two and G/K_1 is easily seen to be a C_6. So here $\delta(G) \leq |G|/2-1$ (explain). For K as in (VI) things are easy enough (explain --- either G is of type (VI) or $\delta(G) \leq |G|/2-1$). For K of type (V) (*) applies. Thus we only have K of type (II), (III) or (IV). Type (II) can be eliminated because $D_4 \pm D_4$ has no automorphism of order three (explain). Type (III) and (IV) are a little harder to deal with. Essentially these can be eliminated because both H(r) and S(r) have order two to an odd power. In this way the proof of B is completed.

We now make out a list of L-groups in terms of type, giving their order and the value of $\delta(G)$. Here E is elementary two of order 2^n.

G=D(A)	2|A|	|G|/2+δ(A)
$G=D_4 \pm D_4 \pm E$	2^{n+6}	$9\|G\|/16-1$
$G=H(r) \pm E$	2^{2r+n+1}	$\|G\|/2+2^{r+n}-1$
$G=S(r) \pm E$	2^{2r+n+1}	$\|G\|/2+2^{r+n}-1$
$G=T(r)$	3.2^{2r}	$2\|G\|/3-1$
G has exp 3	3^m	$(\|G\|-1)/2$
G is a $S_3 \pm D_4 \pm E$	3.2^{n+4}	$\|G\|/2$
G is a $S_3 \pm S_3$	36	19
G is a S_4	24	13
G is a A_5	60	31

Theorem A tells us that the groups V for which $M_0(V)$ is not p-gen ($p \geq 5$ a prime) is the union of In(p), $D^{\#}(1,p)$, D(2,p) and D(3,p). The groups of In(p) and $D^{\#}(1,p)$ create no real difficulties. They are excluded on very natural grounds (explain). However, the groups of D(3,p) and very much more those of D(2,p), are certainly harder to find. But this can now be done. The list given allows it. If we can determine when G (not elementary two) having order $\leq 3p$ has $\delta(G) > 2|G|/3$ then we have the groups of D(3,p). If we can determine when G (not elementary two) having order $\leq 2p$ has $\delta(G) > |G|/2$ then we have the groups of D(2,p). This is just a matter of looking at the above list.

We still have some further interesting questions about D(2,p) and D(3,p). These are finite classes so how many groups do they contain. Here D(3,p) is very rudimentary. It is often empty and contains at most two groups (ie. $|D(2,p)|\leq 2$ --- explain what these two groups are). Things are more complicated for D(2,p). What we have here is that $|D(2,p)|>\log_2 p-3$ so that $|D(2,p)|$ tends to infinity as p does. Indeed it looks as though this lower bound may not be too far from $|D(2,p)|$ generally. It was calculated in Tim and my paper that $|D(2,p)|\leq 576$ for all primes $p\leq 10^6$. It was also calculated that for p=257 (a Fermat prime --- give explanation here) $|D(2,p)|=35$.

The p-gen problem is of course part of the very much bigger n-gen problem. It is explained now how a solution of this appears to go. The literature handles the situation where n=2 or 3. For n a prime ≥ 5 this is handled by theorems A and B. For n=pq where p<q are distinct primes and V not elementary two it would seem that the only groups that must be excluded are those where $|V|\leq p+q$ or $p+q<\delta(V)\leq 3p$, while for elementary two groups it appears we need only exclude those where $|V^*|$ is not positively spanned (explain what this means) by p and q. For n being an integer other than above and not a prime power a result similar to the pq case appears to hold apart from the $\delta(V)$ requirement (explain). This would mean all n and V can be handled except where $n=p^m$ ($m\geq 2$). Also here it looks very likely things can be tied up. What is conjectured is that those V not elementary two having $|V^*|\leq n$ are excluded and those V elementary two with $|V^*|\leq n$ or $|V|$ incongruent to 1 mod p are also. If this were to be true (it is beginning to look that way) the n-gen problem would be completely sown up. However, this is a huge problem. The number of pages needed in its solution is hard to estimate. I feel it could easily be upward of 600.

References

[1] W.M.Potter, 'Non-solvable groups with an automorphism inverting many elements', Arch. Math. (Basel) 30 (1988), 292--299.

[2] S.D.Scott, 'Involution near-rings', Proc. Edin. Math. Soc. 22(1979), 241--245

[3] C.T.C.Wall, 'On groups consisting mostly of involutions', Math. Proc. Cambridge Philos. Soc. 67 (1970). 251--262.