Research notes

Volume XII

Contents

Lifting endo-permutation modules 1

Conjugacy classes in semi-direct products 17

A problem of Praeger 18

On Catano's equivalence 19

Brauer split complexes 24

On a remark of Brumberg 25

Lifting: a correction 28

Local blocks 29

Smith-Tyrer revisited 36

Endo-simple modules 44

Remarks on local blocks of defect p^2 47

The Brauer correspondence and Cartan matrices 49

A shift and stack functor 57

Double cosets and cohomology 57

Centralizer rings and Hecke algebras 58

Permutation filtrations 60

McKay's conjecture for Σ_n 61

Unipotent conjugacy: double cosets 66

Small centralizers 70

Power products 77

Small centralizers, $p > 2$ 78

Small centralizers, $p = 2$ 82

Small centralizers, revisited 85

Small centralizers, $p = 2$, cont'd 97

Lifting endo-permutation modules

We have the usual set-up : R, k, P where R is the usual valuation ring, k is an algebraically closed field of characteristic p and P is a p-group. All R-modules will be free and we will use "bars" to denote reduction from R to k.

Theorem. Let M be an RP-module satisfying the following conditions :

i) M_Q is an endo-permutation module for each proper subgroup Q of P ;

ii) $\bar{M}$ is an indecomposable endo-permutation module for kP, with vertex P.

It follows that M is an endo-permutation module for RP.

Proof. Since $\bar{M}$ is indecomposable and an endo-perm. module we have $p \nmid \dim_k \bar{M}$ so we have a decomposition

$$\mathrm{Hom}_R(M, M) = R \oplus N$$

of RP-modules where $\bar{N}$ is a permutation module with no trivial orbits. Moreover our hypothesis yields that the map

$$\mathrm{Hom}_{RQ}(R \oplus N,\ R \oplus N) \to \mathrm{Hom}_{kQ}(k \oplus \bar{N},\ k \oplus \bar{N})$$

is an epimorphism for any proper subgroup Q of P.

Express $\bar{N} = U_1 \oplus \dots \oplus U_n$ as a direct sum of transitive (and non-trivial) permutation modules with $u_i \in U_i$ an element of a permutation basis. Let Q_i be its stabilizer in P so Q_i is a proper subgroup of P. Since there is a kQ_i-homomorphism of k to kU_i we deduce there is $y_i \in N$ with $\bar{y}_0 = u_i$ and Ry_i

a trivial RQ_i-module. Hence, the images xy_i, $x \in P$, are a basis of an RP-submodule M_i of $\mathrm{Hom}_R(M, M)$ with $\bar{M}_i = U_i$. Hence, $\mathrm{Hom}_{RP}(M, M) = R + M_1 + \cdots + M_n$ is a direct sum as desired.

The argument easily generalizes, in a direction relevant to us, which we record in passing. Let G be any finite group now. Suppose that M is an RG-module, that $\bar{M}$ is a permutation module and the maps

$$\mathrm{Hom}_{RQ}(M, M) \to \mathrm{Hom}_{kQ}(\bar{M}, \bar{M})$$

are epimorphisms for all subgroups Q of P. Then M is a monomial module. The idea is to use the endomorphisms which are projections onto the one-dimensional space spanned by an element of the permutation basis of $\bar{M}$, lifting them to idempotents.

Further remains to be true but should be checked. The linear characters corresponding to the monomial basis are of p-power order (as they are trivial reduced to k). They are stable in the sense of cohomology. Let H and K be stabilizers of two of the rank one R-modules from the monomial basis. If $g \in G$ then the linear characters on $gHg^{-1} \cap K$ are the same, the ones from gHg^{-1} and from K. Probably, something like these conditions gives a converse result characterizing certain monomial modules which are permutation modules when reduced to k with certain lifting properties for endomorphisms.

However, we leave this digression and now focus on the actual lifting. The above theorem possibly might be used in proving that a lifted module is an endo-permutation module in fact.

Theorem. If V is a kP-endo-trivial module then V lifts to a RP-endo-trivial module.

Here, $0 \to \mathfrak{p} \to R \to k \to 0$ is as usual with $\mathfrak{p} = (\pi)$. The lifting of all that needs to be proved. For $\mathrm{Hom}_{k}(V,V) \simeq k \oplus U$ where U is projective so if M is an RP-module lifting V then the rank of M is not divisible by p so $\mathrm{Hom}_R(M,M) \simeq R \oplus N$ where $\bar{N} = U$ so N is therefore projective.

Before proving the result we turn to congruence subgroups. Let $n > 0$, $GL(n,R;m)$, $m \geq 1$ be the subgroup of all elements of $GL(n,R)$ congruent to I modulo $\mathfrak{p}^m$ so, for example, $GL(n,R)/GL(n,R;1) \simeq GL(n,k)$. Let $V_n(k)$ be the space of column vectors, a module for $GL(n,k)$. We assert that

$$GL(n,R;m) / GL(n,R;m+1)$$

is naturally a module for $GL(n,k)$ isomorphic with $\mathrm{Hom}_k(V_n(k), V_n(k))$. First, under conjugation, $GL(n,R;1)$ acts trivially on the quotient.

$$(I+\pi A)(I+\pi^m B)(I-\pi A+\pi^2 A^2 + \cdots) \equiv I + \pi^m B.$$

Moreover, if $g \in GL(n,R)$ then

$$g(I+\pi^m B)g^{-1} = I + \pi^m g B g^{-1}.$$

Next, let's turn to $SL(n,R)$ and similarly defined subgroups $SL(n,R;m)$. We assert that

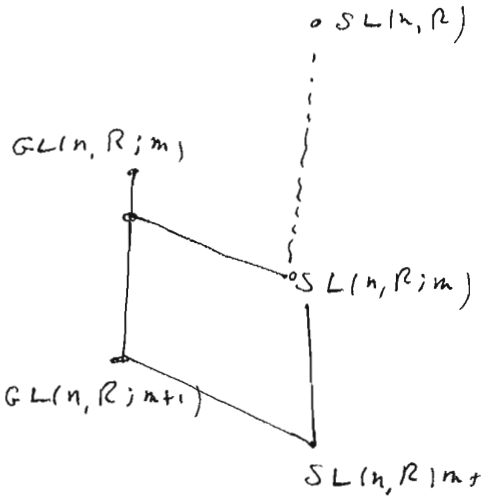
$$SL(n,R;m) / SL(n,R;m+1)$$

is isomorphic to the $SL(n,k)$ module of matrices of trace 0 in $\mathrm{Hom}_k(V_n(k), V_n(k)) \simeq M_n(k)$, matrices, under conjugation. Of course we have an exact sequence, as is easy to see,

$$1 \to SL(n,R;1) \to SL(n,R) \to SL(n,k) \to 1$$

(by lifting generators for example).

We have $SL(n,R;m) = GL(n,R;m) \cap SL(n,R)$ so we have the picture



Now $\det(I + \pi^m A) \equiv 1 + \operatorname{Tr} A \cdot \pi^m \pmod{\pi^{m+1}}$ as is easy to see by expanding the determinant, so we have "half" of our assertion, we need just that the projection of $SL(n,R;m)$ into the factor $GL(n,R;m)/GL(n,R;m+1)$ is of codimension one (over k) for example. But "off-diagonal" entries are easy to "handle" here as matrices like

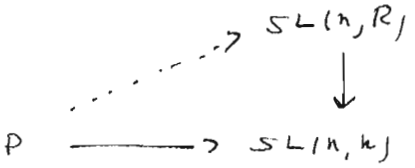
$$\begin{pmatrix} 1+\pi^n a & & 0 & \\ & 1-\pi^n a + \pi^{2n} a^2 - \pi^{3n} a^3 \cdots & & \\ 0 & & 1 & \\ & & & \ddots \end{pmatrix}$$

do the rest.

Proof (of the theorem) Suppose V is n-dimensional and

$$\rho : P \to GL(n,k)$$

is a representation corresponding with V. Then $\rho(P) \subseteq SL(n,k)$ as k^* has no non-identity p-elements! Hence, we wish to lift in the following sense:



But the kernel of the map $SL(n,R)$ to $SL(n,k)$, namely $SL(n,R;1)$, is filtered by a series whose successive quotients are projective modules for P so we are done, by completeness. We are using the fact that the matrices of trace zero, as a kP-module, must be projective, from our hypothesis.

Our next result pushes these ideas.

Theorem. If V is a kP endo-permutation module then it lifts to an $(R/\mathfrak{g}^2)P$-module (which is free as an $R/\mathfrak{g}^2$-module).

We are not claiming that this lift is an endo permutation module.

Lemma If H is a subgroup of the group G, U, V are RG-modules with V relatively H-projective and $n \geq 1$ then the restriction

$$Ext^n_{RG}(U,V) \to Ext^n_{RH}(U,V)$$

is a monomorphism.

Proof (of the lemma). By dimension shifting using U we may assume $n=1$. An exact $0 \to V \to W \to U \to 0$ which splits on H does split as V is relatively H-injective.

Proof (of the theorem). We may assume that V is indecomposable and that the result holds for proper subgroups of P. Our analysis above shows we are reduced to show that an extension of V by P splits when V is the kP-module of elements of trace zero in $\mathrm{Hom}_k(V,V)$. Hence, V is the direct sum of transitive permutation modules, each, by the indecomposability, of degree greater than one. We have an element $\alpha \in H^2(P,V) \cong \mathrm{Ext}^2_{kG}(k,V)$ which is zero on each proper subgroup of P so the direct sum decomposition of V and the lemma show that α is also zero.

Remark: Our first theorem carries over to $R/2^2$ so to lift to an endo-permutation module, rather than just lift, we are reduced to restrictions to proper subgroups, after first reducing to indecomposable modules.

Before proceeding, we wish to state some obvious reductions. To solve the lifting problem, while proceeding by induction, it suffices to consider an indecomposable kP-module V which is endo-permutation. Hence, $\dim_k V$ is prime to p and the permutation module $\mathrm{Hom}_k(V,V)$ has a unique trivial summand. To see this one has only to deal with a subgroup Q of P, a proper one, an indecomposable kQ-module V which has vertex Q and is endopermutation module as well. Suppose that V lifts to an endo-permutation module $\hat{V}$ for RQ and that $\mathrm{End}_{\mathcal{O}}^P V$ is endo-permutation. Is $\mathrm{End}_{\mathcal{O}}^P \hat{V}$ as well?

The answer is "yes!" By Dade's results (we don't need the Kirchhelmann - Harris improvement) we may assume that $\hat{V}$ is in the special linear group. For the determinant representation is of order a power of p and the dimension is prime to p. Then we have a uniqueness. (See 12.1 in the second Dade paper, for example.)

Now, the first Dade paper, in 2.15, gives the conditions for $\mathrm{ind}_Q^P V$, $\mathrm{ind}_Q^P \hat{V}$ to be endo-permutation: V and ${}^g V$ are compatible on $Q \cap {}^g Q$ - similar for $\hat{V}$. But these modules are capped for $Q \cap {}^g Q$ since V, $\hat{V}$ (by induction mod p) have vertex Q and so are capped. Hence, by 6.12 of the first paper, V and ${}^g V$ have the same caps on ${}^g Q \cap Q$ and it applies to be the same for $\hat{V}$ and ${}^g \hat{V}$.

Hence, the reason for the question mark! The problem is whether the cap of $\hat{V}_{{}^g Q \cap Q}$ is also in SL (and the same for ${}^g \hat{V}$). This is a general question about restriction and caps and SL. In any case, the lifting problem is for the cap group so we don't actually have to deal with this problem. But it is worth answering.

We return to our main problem, keeping the situation of going from mod p to mod p^2 and assume the Dade - Kirchhelmann - Harris uniqueness results carry through to mod p^2. So we let V be an indecomposable endo-permutation $\mathbb{Z}P$-module and assume that the desired results hold for proper subgroups of P.

Our first aim is to get a situation like the one in the theorem on page 1 but weaker.

Nevertheless, we can handle odd p with an easy result. Let $\mathcal{O}$ be the usual valuation ring.

Proposition Let U be an indecomposable endo-permutation module for $\mathcal{O}P$, P a p-group, $p > 2$, with vertex P. If $Q \leq P$ and U is "in SL" then so is $\mathrm{Cap}(U_Q)$.

Proof. We proceed by induction so the result holds for all proper subgroups of P and we may assume that Q is such. Let $V = \mathrm{Cap}(U_Q)$ so $V = \lambda \otimes W$, where λ is of rank one, W is "in SL." We want: $\lambda \simeq R$. By Dade's formula,

$$V_Q \simeq \bigoplus_{R \leq Q} n_R \, \mathrm{Ind}_R^Q(\mathrm{Cap}\, V_R)$$

$$\simeq \lambda \otimes \left(\bigoplus_{R \leq Q} n_R \, \mathrm{Ind}_R^Q W_R \right)$$

where W_R is in SL. This is using the induction hypothesis applied to W. Hence, we only need, as V_Q is "in SL", to see that the second factor of the R.H.S. is in SL.

Lemma Let M be an $\mathcal{O}R$-module (a lattice as usual), for a p-group R, $p > 2$ and Q a subgroup of the p-group R. Then $\mathrm{Ind}_R^Q M$ is also in SL.

Proof. The matrices for $\mathrm{Ind}_R^Q M$ are block-permutation matrices for matrices of determinant one and permutations of p-power order. Putting these in block-diagonal form does not change the determinant since we use only even permutations.

We can also now show that the result fails for $p=2$: there are (induced) endo-permutation modules which do not lift to endo-permutation modules. Let's assume $Q \leq P$, a p-group. Let V be an indecomposable kQ endo-permutation module with vertex Q such that $\mathrm{End}_Q^P V$ is also endo-permutation.

Lemma If M is an OP endo-permutation module lifting $\mathrm{End}_Q^P V$ then M is indecomposable with vertex Q and $M \cong \mathrm{End}_Q^P N$ where N is an OQ-endo-permutation module lifting V.

Proof Certainly M is indecomposable as $\bar{M} \cong \mathrm{End}_Q^P V$ is (using bars for reduction mod p). A vertex for M is the largest-ups to conjugacy-subgroup for which $\mathrm{End}_O(M, M)$ has a summand isomorphic with O which is the same for $\mathrm{End}_R(M, M)$ as $\mathrm{End}_O(M, M)$ is a permutation module. Thus M has vertex Q. Thus, $M \cong \mathrm{End}_Q^P N$ where N is an indecomposable OQ-endo-permutation module with vertex Q. Then $\bar{M} \cong \mathrm{End}_Q^P \bar{N}$, i.e. $\mathrm{End}_Q^P V \cong \mathrm{End}_Q^P \bar{N}$ so, after a conjugacy, we assume $\bar{N} \cong V$. Note that dimension considerations force $\bar{N}$ to be indecomposable (or we could quote Dade).

Now, assume that N is an OQ endo-permutation module lifting V. We need to find an example where there is $g \in P$ so that

$$\mathrm{cap}(N_{Q \cap {}^gQ}) \neq \mathrm{cap}({}^gN_{Q \cap {}^gQ}).$$

Let $P = (Z_1 \times Z_2) \wr Z_4$ as

$$P = \langle x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 \rangle \rtimes \langle t \rangle$$

where $t x_i t^{-1} = x_{\pi(i)}$ where $\pi = (1357)(2468)$. Let $Q = \langle x_1, x_2, x_3 \rangle \cong Z_2^3$. Let $V = \Omega^1_{Q/\langle x_3 \rangle}(k)$ as a kQ-module.

First, we claim that $\mathrm{End}_{kQ}^P V$ is also endo-permutation. The four conjugates of Q are

$$Q = \langle x_1, x_2, x_3 \rangle, \ \langle x_3, x_4, x_5 \rangle, \ \langle x_5, x_6, x_7 \rangle, \ \langle x_7, x_8, x_1 \rangle$$

Hence, by Dade's criteria, we have only to calculate "caps" in

$$Q \cap tQt^{-1} = \langle x_3 \rangle, \quad Q \cap t^3 Q t^{-3} = \langle x_1 \rangle$$

two different ways. Each time we get trivial modules k so $\mathrm{End}_{kQ}^P V$ is as stated.

Hence, by the lemma, we need only show that $\mathrm{End}_{kQ}^P N$ is not endo-permutation for a set N; but any set will do as the orders differ only by a one-dimensional tensor factor, by Dade's results. We take $N = \Omega^1_{Q/\langle x_3 \rangle}(O)$ as OQ-module. We work with $Q \cap tQt^{-1}$. First, restricting from ${}^tQ$ we get a cap which is the one-dimensional "sign" module for $O\langle x_3 \rangle$ which restriction from Q gives the trivial module.

Thus, our example is of dimension $2^7 \cdot 3$ for a 2-group of order 2^{10}. Looks like we could get by with $E \rtimes \langle t \rangle$ where $E \cong J_3 \oplus J_-$ as modules but this needs checking. If that works we would get by with a module of dimension $2^9 \cdot 3$ for a group of order 2^7.

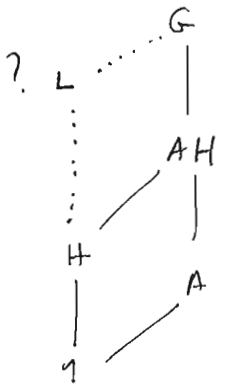
Preliminary to the next steps we need a result on the extension of splittings.

Set-up: $G \rhd (A \rtimes H)$, $A \lhd G$, A abelian, G/AH cyclic of order n, $G = A\,N_G(H)$.

Question: Is $G = A \rtimes L$, $L \geq H$.

(That is why we assumed $G = A\,N_G(H)$ as would have $H \lhd L$.)

Picture:



Claim: There is a well-defined element in $\hat{H}^0(G/AH, A^H)$, the "obstruction," which is zero iff the answer is "yes."

Remark: Not surprising as expect obstruction in $H^2(G/AH, A^H)$ and G/AH is cyclic

Proof. Let g be a generator mod AH with $g \in N(H)$. Hence, $g^n = a h$, $a \in A$, $h \in H$ as $a \in N(H) \cap A = A^H$. This element, mod traces, is the obstruction. We just need to see that it is well-defined and that it determines the splitting.

First, consider $b h g$, $b \in A$, $h \in H$ also in $N_G(H)$. What is $(b h g)^n$? We have $b \in N(H) \cap A = A^H$ and

$$(bkg)^n = b \cdot {}^{kg}b \cdot \cdots {}^{(kg)^{n-1}}b\,(kg)^n,$$
$$= b \cdot {}^{g}b \cdot \cdots {}^{g^{n-1}}b \cdot k\,{}^{g}k \cdots {}^{g^{n-1}}k\,g^n,$$

since A^H is invariant under conjugation by g,

$$= (b\,{}^{g}b \cdots {}^{g^{n-1}}b\,a)(k \cdot {}^{g}k \cdots {}^{g^{n-1}}k\,h)$$

as a centralizes H, so the well-defined statement holds.

This calculation also shows that if a is a trace then the extension splits as desired: inspect the last equality.

Remark: When A is the direct product of G-invariant subgroups we can calculate the obstruction summand by summand using a different choice of g for each summand if we wish, subject to the condition that $g \in N_G(H)$.

We return to the inductive situation described above with the given notation.

Proposition If Q is a maximal subgroup of P then V lifts to an RP-module which is an endo-permutation module for RQ.

Since we are proceeding by induction we may assume, without loss of generality, that P acts faithfully on V - else we are done!

We have an exact sequence, where $n = \dim_R V$,

$$1 \to A \to SL(n, R) \xrightarrow{\pi} SL(n, k) \to 1$$

where the kernel A is isomorphic, as module for $SL(n, k)$, to the matrices of trace zero - and size $n \times n$ - under conjugation.

Let $\rho : P \to SL(n,k)$ be a representation corresponding to V. Suppose that λ, μ are lifts to endo-permutation modules as follows:

$$1 \to A \to SL(n,R) \to SL(n,k) \to 1$$

We are assuming commuting. Note, as $(n,p)=1$, there are such lifts to $SL(n,R)$ if there are any such lifts.

Lemma. There is $a \in A$ so that $\mu(x) = a\,\lambda(x)\,a^{-1}$ for all $x \in Q$.

Proof. By the Dade-Harris-Knörr-Robinson result, the two lifts give isomorphic modules (as $(p,n)=1$). Hence, there is $t \in SL(n,R)$ so that $t\,\lambda(x)\,t^{-1} = \mu(x)$, for all $x \in Q$. Thus $\pi(t)$ is in the centralizer of $\rho(Q)$. But any endomorphism (automorphism) of V lifts to an endomorphism (automorphism) of any lift of V which is an endo-permutation module, by inspection. Hence, there is s in the centralizer of $\lambda(Q)$ in $SL(n,R)$ so that $\pi(s) = \pi(t)$. Thus $\pi(ts^{-1}) = 1$ and

$$ts\,\lambda(x)\,s^{-1}t^{-1} = t\,\lambda(x)\,t^{-1} = \mu(x)$$

for all $x \in Q$ as desired.

Now, with the same notation, let $t \in SL(n,R)$ with $\pi(t) = \rho(g)$, $g \in P$.

Lemma. The subgroups $\lambda(Q)$ and $t\,\lambda(Q)\,t^{-1}$ are conjugate by an element of A.

Proof. Let $\mu(x) = t(\lambda(g^{-1}xg))t^{-1}$ for $x \in Q$ another lift as above. Indeed,

$$\pi\mu(x) = \pi(t\,\lambda(g^{-1}xg)\,t^{-1}) = \rho(g)\,\rho(g^{-1}xg)\,\rho(g)^{-1} = \rho(x).$$

Hence, by the previous lemma, there is a $\in A$ so that

$$\lambda(x) = a\,t\,\lambda(g^{-1}xg)\,t^{-1}a^{-1}$$

for all $x \in Q$, i.e.

$$\lambda(Q) = a\,(t\,\lambda(Q)\,t^{-1})\,a^{-1}$$

as required.

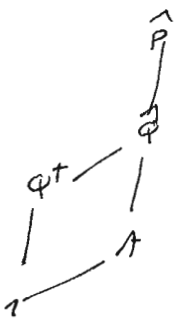
Let's introduce some notation. Let $\hat{P}$ be the subgroup of $SL(n,R)$ containing A so that $\pi(\hat{P}) = \rho(P)$, (so $\hat{P} = \pi^{-1}\rho(\pi)$) and let $\hat{Q}$ similarly be defined so $\pi(\hat{Q}) = \rho(\hat{Q})$. We picture these as follows:

$$\begin{array}{ccccccc} 1 & \to & A & \to & SL(n,R) & \to & SL(n,k) \to 1 \\ & & \| & & \uparrow & & \uparrow \\ 1 & \to & A & \to & \hat{P} & \to & \rho(P) \to 1 \\ & & \| & & \uparrow & & \uparrow \\ 1 & \to & A & \to & \hat{Q} & \to & \rho(Q) \to 1 \end{array}$$

Set $Q^t = \lambda(Q)$ - we know such exists by conduction. The previous result gives us the next, by the Frattini argument:

<u>Lemma</u> We have the factorization $\hat{P} = A\,N_{\hat{P}}(Q^t)$.

Another picture:



We want to read "P^t" to put in the obvious way, i.e. to extend λ to P. This is the situation studied above, as $|\hat{P} : \hat{Q}| = p$.

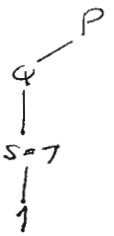
One result we used implicitly above and will now use again was unstated and we shall correct this situation. This arises when we apply induction to a restriction of our module and this restriction is not necessarily indecomposable. However, it is capped.

Lemma If W is an indecomposable endo-permutation module for the algebra kT, T a p-group, which lifts to the same for RT then the same holds for any capped kT-module with cap W.

Proof. Follows directly from Dade 6.10, 12.1.

Now, let's finish the proof of the proposition on page 12. We have an obstruction to computing what we should be "summand by summand." Let kX be a transitive permutation summand of A so $|X| \neq 1$.

Let $x \in X$ with stabilizer $S \leq P$, $T = S \cap Q$, $\hat{S}, \hat{T}$ defined in the obvious way. First, suppose that $S = T$.

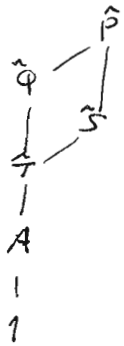


Then

$$(kX)^Q \simeq (kP/S)^Q \simeq k[P/Q]$$

as $k[P/Q]$-module, as $k[P/Q]$ is an image and dimensions are right. Hence, as this is a free module the obstruction vanishes.

Next, suppose that $S > T$ so $P = QS$. Hence, $(kX)^Q$ is one dimensional spanned by $\sigma = \sum_X x$. The only possible obstruction then is a multiple of σ. Pick $g \in \hat{S} - \hat{T}$, $g \in N_{\hat{S}}(Q^t)$ so $g \in N_{\hat{S}}(\hat{T} \cap Q^t)$. Set $T^t = \hat{T} \cap Q^t$. We are in an inductive situation with $\hat{T}, \hat{S}, T^t$ and so on so the obstruction is zero there. But



$\{x\}$ is an orbit in this situation as no multiple of it occurs in the subtraction. Hence, the proposition is proved.

Let's list some ideas of how to proceed next.

1. We can choose a good permutation submodule of the lift corresponding to orbits with a stabilizer $= Q$ just as in the argument for the theorem on page 1
2. Somehow all we've using $Ext^1(V,V) \cong H^1(P, Hom_k(V,V))$ and calculate out a formula for these cocycles.
3. Keep in mind how other lifts where the role of Q is played by another maximal subgroup of P.
4. Assume the theorem we want holds. What do we deduce about these 1-cocycles?

Conjugacy classes in semi-direct products

Let $G = N \rtimes H$ and assume that N is abelian. In this case, Clifford theory is especially effective in describing the characters of G. We give a description of the conjugacy classes.

If $h \in H$ let $C^N(h)$, the "co-centralizer" of h in N, be the quotient $N / \{ n^h(n^{-1}) \mid n \in N \}$ (as these commutators are a subgroup). Hence, $C_H(h)$ acts on $C^N(h)$.

Lemma The conjugacy classes of G intersecting hN are in one-to-one correspondence with the orbits of $C_H(h)$ on $C^N(h)$.

That is, "centralizer co-centralizer" orbits.

Proof. Suppose $x, y \in N$ and xh, yh are conjugate in G so there is $z \in N$, $k \in H$ with $^{zk}(xh) = yh$. But

$$^{zk}(xh) = {}^{zk}x \, {}^{zk}h = {}^{k}x \cdot {}^{z}({}^{k}h)$$
$$= {}^{k}x \cdot z({}^{k}h) z^{-1} ({}^{k}h)^{-1} \cdot {}^{k}h.$$

Hence, ${}^{k}h = h$ and ${}^{k}x \cdot z({}^{k}h) z^{-1} ({}^{k}h)^{-1} = y$, i.e. ${}^{k}h = h$ and

$$y = {}^{k}x \, z h z^{-1} h^{-1}$$

as required. Conversely, if $k \in C_H(h)$ and y has such an expression, we can reverse the argument.

A problem of Preeda

Prop. If φ is an automorphism of the finite group G and H is a subgroup of G then the number of elements $g \in G$ with $g\varphi(g) \in H$ is at least $|H|$.

Proof. Let $E = \langle \varphi \rangle \ltimes G$. Now $H\varphi H \subseteq \varphi G$ so each element of $H\varphi H$ has an expression $g\varphi(g)$, $g \in G$. Also

$$(g\varphi)^2 = g\,\varphi g \varphi = g\,\varphi(g)$$

so it suffices to show that the double coset $H\varphi H$ contains at least $|H|$ elements whose square lies in H. Hence, we are reduced to the following result:

Prop. If H is a subgroup of the finite group E and t is an involution of E then the number of elements of HtH with square in H is exactly $|H|$.

Proof. Let X be a transversal to $tHt \cap H$ in H so each element of HtH has a unique expression as xth, $x \in X$, $h \in H$. But $(xth)^2 \in H$ iff $thxt \in H$ iff $hx \in tHt$ iff $h^{-1} \in xtHt$. But $h^{-1} \in H = xH$ so the last statement is iff $h^{-1} \in x(tHt \cap H)$. Thus, for $x \in X$ there are exactly $|tHt \cap H|$ elements $h \in H$ for which xth has square in H. But $|X| = |H : H \cap tHt|$ so we are done.

Remark. This also works for $t \in E$ only assuming $t^2 \in H$. For $thxt \in H \Leftrightarrow h^{-1} \in x(tHt) = x(tHt^{-1})t^2 \Leftrightarrow h^{-1} \in x(tHt^{-1})$. Hence, the number of elements e of E with $e^2 \in H$ is a multiple of $|H|$.

On Cabanes' equivalence

We shall give an exposition. As usual, A is an algebra, M is an A-module, $E = \mathrm{End}_A(M)$ acting on the right. All modules will be finitely generated.

Theorem The full subcategory of A-modules which are isomorphic with submodules and quotient modules of direct sums of copies of M is equivalent with the category of E-modules.

Remark. The proof shows that $\mathrm{Hom}_A(M, -)$ gives the equivalence but $M \otimes_E -$ is not an inverse equivalence.

Step 1 If U, V are A-modules, $\oplus M \to U \to 0$ is exact then $\mathrm{Hom}_A(M, -)$ embeds $\mathrm{Hom}_A(U, V)$ into $\mathrm{Hom}_E(\mathrm{Hom}_A(M, U), \mathrm{Hom}_A(M, V))$.

Indeed, let $\varphi \in \mathrm{Hom}_A(U, V)$, $\varphi \neq 0$. Hence, by assumption there is $\alpha : M \to U$ such that $\varphi(\alpha(U)) \neq 0$. Thus, $\mathrm{Hom}_A(M, \varphi) \neq 0$, as it sends α to a non-zero element of $\mathrm{Hom}_A(M, V)$, namely $\varphi \circ \alpha$.

Step 2 Suppose that U, V are A-modules as in the theorem and $i : U \to \bigoplus_I M$, $j : V \to \bigoplus_J M$ are injections. Hence, we get injections (by Step 1) $\mathrm{Hom}_A(M, i) : \mathrm{Hom}_A(M, U) \to \mathrm{Hom}_A(M, \bigoplus_I M)$, $\mathrm{Hom}_A(M, j) : \mathrm{Hom}_A(M, V) \to \mathrm{Hom}_A(M, \bigoplus_J M)$. Suppose that $\Phi \in \mathrm{Hom}_E(\mathrm{Hom}_A(M, U), \mathrm{Hom}_A(M, V))$. We want to show that $\Phi = \mathrm{Hom}_A(M, \varphi)$, $\varphi \in \mathrm{Hom}_A(U, V)$.

We have the diagram :

$$\begin{array}{ccc} \mathrm{Hom}_A(M, \bigoplus_I M) & & \mathrm{Hom}_A(M, \bigoplus_J M) \\ \uparrow{\scriptstyle \mathrm{Hom}_A(M,i')} & & \uparrow{\scriptstyle \mathrm{Hom}_A(M,j')} \\ \mathrm{Hom}_A(M, U) & \xrightarrow{\Phi} & \mathrm{Hom}_A(M, V) \end{array}$$

so, by our assumption on E, as $\mathrm{Hom}_A(M, \bigoplus M) \cong \bigoplus E$ as E-modules, there is $\overline{\Psi} : \mathrm{Hom}_A(M, \bigoplus_I M) \to \mathrm{Hom}_A(M, \bigoplus_J M)$ making the diagram commute. Hence, as $\overline{\Psi} = \mathrm{Hom}_A(M, \psi)$ for some $\psi \in \mathrm{Hom}_A(\bigoplus_I M, \bigoplus_J M)$ (Fitting's theorem) we have a diagram

$$\begin{array}{ccc} \bigoplus_I M & \xrightarrow{\psi} & \bigoplus_J M \\ \uparrow{\scriptstyle i'} & & \uparrow{\scriptstyle j'} \\ U & & V \end{array}$$

Hence, it suffices to show that $\psi(U) \leq V$ as the letting $\varphi \in \mathrm{Hom}_A(U, V)$ in the restriction we are done by the embedding result (Step 1) as $\mathrm{Hom}_A(M, \varphi)$ and Φ both make the diagram, at the top of the page with $\overline{\Psi}$ in it, commute. But we have $\mathrm{Hom}_A(M, \psi(U)) \leq \mathrm{Hom}_A(M, V)$ and both $\psi(U)$ and V epimorphic images of direct sums of copies of M, so this step is completed.

What remains to prove is only the following:

Step 3 If V is an E-module then there is an A-module U, as in the theorem, with $V \cong \mathrm{Hom}_A(M, U)$.

Here we follow Cabanes with one extra fact as well.

We may assume that we have an inclusion

$$V \hookrightarrow \mathrm{Hom}_A(M, \bigoplus_I M)$$

We get a commutative diagram

$$\begin{array}{ccc} M \otimes_E V & \longrightarrow & M \otimes \mathrm{Hom}_A(M, \bigoplus_I M) \\ & \searrow \quad \swarrow & \\ & \bigoplus_I M & \end{array}$$

as follows. The horizontal arrow is clear. The right vertical arrow is the adjunction (via evaluation) and is an isomorphism. The left vertical arrow sends $m \otimes v$ to $v(m)$ so the diagram commutes. Hence, if K is the kernel of the horizontal arrow then $M \otimes_E V/K \simeq VM$ the image in $\bigoplus_I M$. But Cartan shows that $\mathrm{Hom}_A(M, VM) \simeq V$ so $\mathrm{Hom}_A(M, M \otimes_E V/K) \simeq V$ as well. One uses $M \otimes_E V/K$ instead of $M \otimes_E V$.

Let's just record Cartan's proof in our notation (an argument which mimics one of Burnside's as Cartan points out). We have $V \subseteq \mathrm{Hom}_A(M, VM)$ and we want equality. Suppose otherwise and choose W so

$$V \subseteq W \subseteq \mathrm{Hom}_A(M, VM) \subseteq \mathrm{Hom}_A(M, \bigoplus_I M)$$

with W/V a simple E-module. But then

$$VM \subseteq WM \subseteq \mathrm{Hom}_A(M, VM)M = VM$$

so $VM = WM$. Let Φ be an E-homomorphism of W to E with kernel V (and remember $E = \mathrm{Hom}_A(M, M)$). Let $\tilde{\Phi}$ be an extension to $\mathrm{Hom}_A(M, \bigoplus_I M)$, which exists as E is injective, so we have the picture

$$\begin{array}{ccc} \mathrm{Hom}_A\left(M, \bigoplus_I M\right) & \xrightarrow{\Psi} & E \\ \cup\!| & & \cup\!| \\ W & \xrightarrow{\Phi} & \Phi(W) \neq 0 \\ \cup\!| & & \cup\!| \\ V & \longrightarrow & 0 \end{array}$$

Let $\psi \in \mathrm{Hom}_A\left(\bigoplus_I M, M\right)$ so $\mathrm{Hom}_A(M, \psi) = \Psi$. Now if $m \in M$, $v \in V$ then

$$0 = \Psi(v)\, m = (\psi \circ v)(m) = \psi(vm).$$

Hence, $\psi(VM) = 0$ so $\psi(WM) = 0$ as $VM = WM$. But if $w \in W$

$$\Psi(w)\, m = \psi(wm) \in \psi(WM) = 0$$

so $\Psi(w) = 0$ for all $w \in W$, a contradiction.

In conclusion, we want to point out one new fact. Without loss of generality, we can assume we have an epimorphism of $\bigoplus_I E$ to V as well as one embedding of V to $\bigoplus_I E$:

$$\bigoplus E \longrightarrow V \longrightarrow \bigoplus E$$

(a non-exact sequence!). Now, using adjunctions we get a commutative diagram

$$\begin{array}{ccccc} \bigoplus E & \longrightarrow & V & \longrightarrow & \bigoplus E \\ \simeq\downarrow & & \downarrow & & \downarrow\simeq \\ \bigoplus E & \longrightarrow & \mathrm{Hom}_A(M, M \otimes_E V) & \longrightarrow & \bigoplus E \end{array}$$

from which follows immediately that V injects into $\mathrm{Hom}_A(M, M \otimes_E V)$ which is a direct sum of this image and the kernel of the bottom right horizontal map.

We can do a little better. Recall the maps

$$V \longrightarrow \mathrm{Hom}_A(M, \oplus M)$$

$$0 \to K \to M \otimes_E V \longrightarrow M \otimes_E \mathrm{Hom}_A(M, \oplus M)$$

$$\searrow \quad \swarrow$$

$$\oplus \eta$$

where the image of $M \otimes_E V$ in $\oplus M$ is VM, so we have an exact sequence

$$0 \to K \to M \otimes_E V \to VM \to 0$$

and another

$$0 \to \mathrm{Hom}_A(M, K) \to \mathrm{Hom}_A(M, M \otimes_E V) \to \mathrm{Hom}_A(M, VM)$$

But we have proved that $V = \mathrm{Hom}_A(M, VM)$. We claim there is a splitting namely the adjunction $V \to \mathrm{Hom}_A(M, M \otimes V)$. Indeed, $v \in V$ goes to the map $m \to m \otimes v$ which then is sent to the map $m \to vm$, which is v. Hence, we have a split exact sequence

$$0 \to \mathrm{Hom}_A(M, K) \to \mathrm{Hom}_A(M, M \otimes_E V) \to V \to 0$$

We also remark that $\mathrm{Hom}_A(M, K) \simeq \mathrm{Tor}_1(M, \Omega^{-1}(V))$. For the exact sequence

$$0 \to V \to \oplus E \to \oplus E/V \to 0$$

gives

$$\mathrm{Tor}_1(M, \oplus E) \to \mathrm{Tor}_1(M, \oplus E/V) \to M \otimes_E V \to M \otimes_E (\oplus E) \to M \otimes (\oplus E/V) \to 0$$

and $\mathrm{Tor}_1(M, \oplus E) = 0$ as E is flat thus free. (As E is self-injective we can speak of $\Omega^{-1}(V)$ and $\mathrm{Tor}_1(M, \oplus E/V) \simeq \mathrm{Tor}_1(M, \Omega^{-1}V)$.) And then have $\mathrm{Hom}_A(M, M \otimes V) \simeq V \oplus \mathrm{Hom}_A(\mathrm{Tor}_1(M, \Omega^{-1}V))$.

Brauer split complexes

Suppose the finite p-group P acts admissably on the finite simplicial complex Y and C is the corresponding chain complex with basis X of simplices. Thus X^Q spans a subcomplex which is, in particular closed under the boundary map.

We wish to have a weaker form of this in terms of maps. Let C be a finite kP-permutation complex, where k is a field of characteristic p. We say that C has a compatible family of Brauer splittings provided the following two conditions are fulfilled:

(1) For each subgroup Q of P the epimorphism

$$Br_Q : C^Q \longrightarrow C(Q)$$

splits via a $kN(Q)$-homomorphism s_Q from $C(Q)$ to C^Q;

(2) For each such subgroup Q and subgroup R of P containing Q there is a map of $C(R)$ to $C(Q)$ making the following diagram commute

$$\begin{array}{ccc} Q^C & \xleftarrow{\ s_Q\ } & C(Q) \\ {\scriptstyle inc.}\uparrow & & \uparrow \\ R^C & \xleftarrow{\ s_R\ } & C(R) \end{array}$$

It is, since the other maps are monomorphisms, unique. It's existence is just a way of saying, in terms of maps, that the image of s_R is contained in the image of s_Q.

Of course, these conditions are fulfilled in the admissable case.

On a remark of Gruenberg

Gruenberg remarked that it was easy to relate $H^2(G,A)$, A a $\mathbb{Z}G$-module and $Ext^1_{\mathbb{Z}G}(\Delta G, A)$ for the augmentation ideal ΔG, using the group algebra and the "map" $g \to g-1$. We carry out the details of this "hint" here.

Suppose we have an exact sequence

(*) $$1 \to A \to E \to G \to 1$$

(now A is multiplicative, abelian and we write A^+ for the additive version, a $\mathbb{Z}G$-module via conjugation). We wish to construct an exact sequence

$$0 \to A^+ \to \; ? \; \to \Delta G \to 0$$

which splits if, and only if, the original sequence splits. (Note: working over $\mathbb{F}_p$ instead of $\mathbb{Z}$ we get directly that Maschke's theorem implies the Schur-Zassenhaus theorem).

We have inclusions

$$\mathbb{Z}E \supseteq \Delta E \supseteq \mathbb{Z}E.\Delta A \supseteq \Delta E.\Delta A$$

of ideals, not just left ideals, since A is normal: $ae = e(e^{-1}ae)$. Now if T is a transversal to A in E then the elements ta are a $\mathbb{Z}$-basis of $\mathbb{Z}E$ as t runs over T and $a \in A$. Thus, it follows directly that ΔE has a $\mathbb{Z}$ basis of elements $e-1$, $1 \neq e \in E$, $\mathbb{Z}E.\Delta A$ has a basis of elements $t(a-1)$, $t \in T$, $1 \neq a \in A$ and $\Delta E.\Delta A$ has a basis of elements $(t-1)(c-1)$ when $c \in A$, $t \neq 1$ and we are assuming that $1 \in T$ is the representative of the coset A. Hence, $\Delta E / \mathbb{Z}E.\Delta A \simeq \Delta G$, $\mathbb{Z}E.\Delta A / \Delta E.\Delta A \simeq A^+$. Moreover, the last isomorphism is as a $\mathbb{Z}G$-module. To see this we need that

$$e(a-1) \equiv eae^{-1} - 1 \quad (\Delta E.\Delta A)$$

as the isomorphism just given with A^+ uses the elements $a-1$.
So, we are asking

$$ea - e \stackrel{?}{=} eae^{-1} - 1$$
$$ea - e - eae^{-1} + 1 \stackrel{?}{=} 0$$
$$(e-1)(a-1) + a - 1 - eae^{-1} + 1 \stackrel{?}{=} 0$$
$$a - 1 - eae^{-1} + 1 \stackrel{?}{=} 0$$
$$a - eae^{-1} \stackrel{?}{=} 0$$
$$ae - ea \stackrel{?}{=} 0$$

But $(a-1)(e-1) \equiv 0$, i.e. $e+a \equiv ae+1$. Similarly, $(e-1)(a-1) \equiv 0$ so $e+a \equiv ea+1$, so we are done.

Hence, we have an exact sequence of $\mathbb{Z}G$-modules:

$$(**) \qquad 0 \to A^+ \to \Delta E / \Delta E . \Delta A \to \Delta G \to 0$$

and we have to see that $(*)$ splits if, and only if, $(**)$ splits.

First, suppose $(*)$ splits and T is a subgroup. Then $T^+ = \{ t-1 \mid t \in T,\ t \neq 0 \}$ span the desired complement. The above arguments show that $\mathbb{Z}T^+$ is a complement as $\mathbb{Z}$-module; we only need that it is a $\mathbb{Z}E$-module. But if $a \in A$, $u \in T$

$$a(t-1) = (t-1) + (a-1)(t-1) \equiv t-1$$
$$u(t-1) = ut - u = (ut-1) - (u-1).$$

Second, suppose the module extension splits. This means that for each $t \in T$, our transversal, there is $a_t \in A$, so that the elements

$$(t-1) + (a_t - 1)$$

a $\mathbb{Z}$-basis of $\Delta E / \mathbb{Z}E . \Delta A$. But $(t-1) + (a_t - 1) \equiv ta_t - 1$ modulo $\Delta E . \Delta A$, pretty much as above:

$$ta_t - 1 - t + 1 - a_t + 1 \equiv ta_t - t - a_t + 1 = (t-1)(a-1) \equiv 0.$$

Thus, the elements ta_t are a new transversal. Hence, without loss of generality, we may assume T is a transversal

with the elements $t-1$ a $\mathbb{Z}$-basis of a complement, a module complement. We need to show that T is closed under multiplication. But say $t, u \in T$, $tu = vq$, $v \in T$, $a \in A$. Want to prove that $a = 1$. But

$$\begin{aligned} t(u-1) &= tu - t \\ &= va - t \\ &\equiv (v-1) + (a-1) + 1 - t \end{aligned}$$

(as $va - 1 \equiv (v-1) + (a-1)$ as above)

$$= (v-1) - (t-1) + (a-1)$$

where $(v-1) + (t-1)$ is on the module. Hence, $a - 1 = 0$, i.e. $a = 1$.

Lifting : a correction

We refer to the top of page 13. Let $GL^{p'}(n, R)$ be the subgroup of $GL(n, R)$ of elements whose determinant is a unit in R in the group of units isomorphic with k^*, the multiplicative group of k. Hence, we still have

$$1 \to A \to GL^{p'}(n, R) \to GL(n, k) \to 1$$

and

$$\begin{array}{ccccccccc} & & & & & \overset{\lambda}{\swarrow} & Q & & \\ & & & & & \underset{\mu}{\searrow} & \downarrow p & & \\ 1 & \to & A & \to & GL^{p'}(n, R) & \to & GL(n, k) & \to & 1 \end{array}$$

where the image of $p(Q)$ is still in $SL(n, k)$ as Q is a p-group and the two lifts are in $SL(n, R)$ but conjugate in $GL^{p'}(n, R)$ as they are conjugate in $GL(n, R)$ (and the center of $GL(n, R)$ times $GL^{p'}(n, R)$ is $GL(n, R)$ as $(p, n) = 1$). We can now proceed as above.

Local blocks

We are interested in blocks with just one simple module, that is local blocks. We begin by giving another treatment of stable equivalence and p-groups (see Feichtmann, Carlson). Let P be a p-group, k an algebraically closed field of characteristic p. Suppose A is a symmetric algebra with no projective simple modules.

Prop If kP and A are stably equivalent then A is local.

Proof. Let U, V be the kP-modules corresponding with non-isomorphic simple A-modules S, T. Then $\underline{Hom}_{kP}(U,V) = 0$ as $U \otimes V^*$ is projective so $Ext^1_{kP}(U,V) = 0$. Hence, by Auslander-Reiten-Smalø, p 344, $Ext^1_A(S,T) = 0$. Indeed, the quoted result says that the stable equivalence commutes with the Heller operator Ω so

$$Ext^1_A(S,T) = \underline{Hom}_A(\Omega S, T) = \underline{Hom}_{kP}(\Omega U, V) \simeq Ext^1_{kP}(U,V) = 0.$$

Hence, each block of A is local. But k is an indecomposable kP-module with $\underline{Hom}_{kP}(k,W) \neq 0$ for each non-projective kP-module W and now A has no such modules, a contradiction.

Now let B be a block of the group G with defect group D and suppose B is stably equivalent with its Brauer correspondent which is local. Is B local? Can the above argument be adapted? Let H be the inertial subgroup of B, $DC(D) \leq H \leq N(D)$, with b the corresponding block of H so b is Morita equivalent with the Brauer correspondent of B, as usual by induction. Thus b and B are stably equivalent. Using the above notation as above, namely S, T; U, V, the key is to prove that

$$\underline{Ext}^1_{kH}(U, V) = 0$$

using the fact that

$$\underline{Hom}_{kH}(U, V) = 0.$$

Remark: It suffices to prove that $\underline{Hom}_{kD}(U, V) = 0$.

Indeed, then $U \otimes V^*$ is a projective kD-module. Then $\Omega U \otimes V^*$ is as well since the sequence

$$0 \to \Omega U \otimes V^* \to P_U \otimes V^* \to U \otimes V^* \to 0$$

is exact, where P_U is the projective cover of U as a kP-module, and two terms are already projective. Hence, $\underline{Ext}^1_{kD}(U, V) = 0$. Thus, $\underline{Ext}^1_{kH}(U, V) = 0$ as U is relatively D-projective: for $\underline{Ext}^1_{kH}(U, V)$ is a direct summand of

$$\underline{Ext}^1_{kH}(\mathrm{Ind}_D^H \mathrm{Res}_D^H U, V)$$

which is, by reciprocity, isomorphic with $\underline{Ext}^1_{kD}(U, V)$.

Remark: It suffices to prove that $\underline{Hom}_{kDC(D)}(U, V) = 0$.

Indeed, let the unique simple module of b_D have dimension n so then there is a kP-module u with $\mathrm{Res}_D^{DC(D)} U \simeq \overbrace{u \oplus \dots \oplus u}^{n}$ and $b_D \cdot \mathrm{Ind}_D^{DC(D)}(u) \simeq \overbrace{U \oplus \dots \oplus U}^{n}$. This follows from Kulshammer's results (see: Morita equivalent blocks in Clifford theory of finite groups). For if e is the central idempotent of b_D then $b_D \cdot ekP \cdot m \simeq m_n(kP)$ where $m \subseteq kDC(D)$, $m \simeq m_n(k)$. As usual (D, b_D) is a Sylow b-subgroup. Restriction is now clear and b_D-induction is induction "in" the algebra b_D so is also clear.

This gives the remark then by the usual reciprocity arguments. $\underline{Hom}_{kD}(U, V) \simeq \underline{Hom}_{kDC(D)}(U, \mathrm{Ind}_D^{DC(D)} \mathrm{Res} V) = 0$ as U is in b_D so only $b_D \mathrm{Ind}_D^{DC(D)}$ "counts".

Remark. It suffices to prove that $\mathrm{ind}_{DC(D)}^{H} \mathrm{Res}_{DC(D)}^{H} U \cong U \oplus \dots \oplus U$

Indeed, then

$$0 = \mathrm{Hom}_{kH}(U \oplus \dots \oplus U, V) = \mathrm{Hom}_{kDC(D)}(\mathrm{Res}_{DC(D)}^{H} U, \mathrm{Res}_{DC(D)}^{H} V)$$

as desired in the previous (reduction) remark.

References: Kulshammer gives some other references for the result — folklore — which quotes him above. See his paper, "On the structure of block ideals in group algebras of finite groups," Comm. Algebra 8 (1980), 1867-1872 and Lemmas B and D give the result. This approach has also been used in Landrock's book (L III, p. 25).

Guess: The following may be occurring. The "source" of U, in $DC(D)$, is stable under conjugation and the property in the remark at the top of the page, holds. May need more than U having a one-dimensional stable endomorphism algebra. The other cases probably lead to modules with one-dimensional stable endomorphism algebras for subgroups, like stabilizers

Remark: Suppose u is an indecomposable $kDC(D)$-module, $u/\mathrm{Res} U$ $U/$ and a conj $DC(D)$ is the stabilizer of u. Then $U \cong \mathrm{ind} u$, $\mathrm{Res} U = u + \dots$ (all conjugates each once), as is easy to see. Hence, $\mathrm{ind}\,\mathrm{Res} U \cong U \oplus \dots \oplus U$ ($|H : DC(D)|$ times) so this can be no problem. What about other stabilizers?

Suggestion: Try $Z_p \times Z_p \rtimes Q_8$ not faithful action!

Lemma. Let N be a normal subgroup of the group G and V a stable kN-module. Suppose that W is a submodule of V, also stable, satisfying the following properties:

i) $(\mathrm{End}_{kN} V)\, W \subseteq W$;

ii) The induced map $\mathrm{End}(V) \to \mathrm{End}(V/W)$ is surjective.

Then the submodule $\mathrm{ind}_N^G W$ of $\mathrm{ind}_N^G V$ also has these two properties.

Proof. Suppose that $|G:N| = n$ so

$$\mathrm{ind}_N^G V = V_1 \oplus \dots \oplus V_n$$

where each $V_i \simeq V$ as kN-module and it contains

$$\mathrm{ind}_N^G W = W_1 \oplus \dots \oplus W_n$$

where $W_i \simeq W$ under an isomorphism (and hence all isomorphisms, by i)) of V_i and V. As usual, the notation is chosen so that G permutes the summands V_i, $1 \le i \le n$, transitively. If Φ is an endomorphism of the kG-module $\mathrm{ind}_N^G V$ then ΦW_i has projections in the summands which, according to i), are all in the corresponding W_j's, so i) certainly holds as required for the induced modules.

Let φ be a kN-homomorphism of V_1/W_1 to V_j/W_j; it suffices now, in order to establish ii) for the induced modules, to show that the corresponding (via Frobenius reciprocity) endomorphism of $\oplus V_i/W_i$ is an image from $\mathrm{End}(\mathrm{ind}_N^G V)$ since $\mathrm{End}(\oplus V_i/W_i)$ is generated by such endomorphisms. Let ψ be a kN-homomorphism of V_1 to V_j (which must take W_1 to W_j) and reduces φ in the image. Then the kG-endomorphism Ψ induced by ψ induces a kG-endomorphism Φ on the quotient which extends φ, so we are done.

Lemma Let N be a normal subgroup of the group G and T a stable simple kN-module such that

$$\mathrm{Ind}_N^G T = S \oplus \dots \oplus S \quad (m \text{ times})$$

for a simple kG-module S. If V is a stable and indecomposable kN-module, with T as a homomorphic image, then

$$\mathrm{Ind}_N^G V = U \oplus \dots \oplus U \quad (m \text{ times})$$

for an indecomposable kG-module U.

Proof. First, note that we have the "usual situation" where $\mathrm{End}(\mathrm{Ind}_N^G S) \cong M_n(k)$, $n = |G:N|$, $m^2 = n$, $\mathrm{Res}_N^G S = T \oplus \dots \oplus T$ (m times). It follows from reciprocity and considering $\mathrm{Res}_N^G \mathrm{Ind}_N^G T$. Since the usual Fitting analysis shows that $\mathrm{End}(\mathrm{Ind}_N^G V)$ has an ideal which is nilpotent of codimension n, it suffices, in order to prove the lemma, that $\mathrm{End}(\mathrm{Ind}_N^G T)$ is a homomorphic image of $\mathrm{End}(\mathrm{Ind}_N^G V)$, again by the usual Fitting theory. Hence, we need a submodule W of V, with $V/W \cong T$ and W satisfying the two properties of the previous lemma.

Now $\mathrm{End}(V)$ leaves invariant $\mathrm{rad}\, V$ and so leaves invariant the pre-image in V of any Wedderburn component of $V/\mathrm{rad}\, V$. Hence, there is a submodule W_1 with $V/W_1 \cong T \oplus \dots \oplus T$ (some number) and $\mathrm{End}(V) W_1 \subseteq W_1$. Thus $\mathrm{rad}\, \mathrm{End}(V)$ induces nilpotent transformations on V/W_1 so there is a submodule W of V, $W \supseteq W_1$, $V/W \cong S$ and $\mathrm{rad}\, \mathrm{End}(V)\, V \subseteq W$. But $\mathrm{End}(V) = k\mathrm{I} + \mathrm{rad}\, \mathrm{End}(V)$ so $(\mathrm{End}\, V) W \subseteq W$. We are done.

We are now going to prove Clifford's reduction theorem for the blocks we have been studying. We have G, H, B, b and so on as above, b is local etc.... Let S be a simple B-module, U the corresponding kH-module. Let M be an indecomposable kD-module which is a summand of $\mathrm{Res}^H_D U$ and such that U is a summand of $\mathrm{Ind}^H_D M$ (so M is unique up to conjugacy in H).

Theorem If M is stable in H then B is local.

Proof. We first use the Morita equivalence mentioned on page 30 (paper by Külshammer) which shows the corresponding module M' for $DC(D)$ in the "root" is also stable. We must then have that the restriction of U to $DC(D)$ is a multiple of M' (since we get M on kD and because of the Morita equivalence). The previous lemma shows that $\mathrm{Ind}^H_{DC(D)} M' = U \oplus \dots \oplus U$ so we are done. Note that we mean that there is an induction-restriction relation between U and M' because there is for M, etc ...

Theorem Assume furthermore that D is abelian and the stable equivalence is of Morita type. Then the two blocks are Morita equivalent.

Proof. We keep all the above notation. Let T be the simple b-module. It suffices* to prove that $U \cong \Omega^i T$ for some integer i. But $\underline{\mathrm{Hom}}(M', M') \cong k$ by reciprocity:

$$m = \underline{\mathrm{Hom}}_{kH}(\mathrm{Ind}^H_{DC(D)} M', U) \cong \underline{\mathrm{Hom}}_{kDC(D)}(M', M' \overbrace{\oplus \dots \oplus}^{m} M')$$

as $\mathrm{Ind}^H_{DC(D)} M' \cong U \oplus \dots \oplus U$ (m times, $m^2 = |H : DC(D)|$).

G S
H U
DC(D) M'
D M

* by Linckelmann's theorem

Hence, by the Morita equivalence, the same holds for M so $M = S^i k$ by Carlson's theorem. Hence, the same holds for M' and then U using the induction and restriction which "commute" with the Heller operator.

Remark. Note that we have proved now, that $U \subset \Omega^i T$ for some i. Hence, it is plausible that the assumption on the stability of M does hold. We have also eliminated (*) above the possibility that the stabilizer of M in H is just $DC(D)$, which is the smallest it can be ($\because PC(D) = C(D)$ here, of course). We can also restate all this in terms of the Brauer correspondent for $N(D)$ rather than H and b. We do so:

Theorem Let B be a block of the group G with abelian defect group D and Brauer correspondent b. Assume that B and b are stably equivalent by a stable equivalence of Morita type. Assume that k is finite and that S is a simple B-module. If the maximal subgroup of b stabilizes the source of the correspondent of S then B is local.

Remark. By Knorr, the vertex of the correspondent of S is D. Also, the Morita equivalence between the stabilizer of the "vertex", the maximal subgroup, and $N(D)$ says that the correspondent of S is a Heller translate of the simple module in b.

(*) Needs further argument; uses Carlson again. The Heller shifts of the trivial kD-module are stable, characterized by their vertex and radical quotients.

Smith - Tyrer revisited

Let's recall the Smith - Tyrer key result. Let P be an elementary abelian Sylow p-subgroup of the group G with $|P| = p^n$, $n > 1$, p odd and assume $N(P)/C(P) \simeq Z_2$ which inverts P. Then $G/O_{p'}(G)$ is isomorphic with $P \rtimes Z_2$ with inverting action. Suppose k is an algebraically closed field of characteristic p. Then the result is equivalent with the following statement: the principal p-block of G is isomorphic with its Brauer correspondent. For the Brauer correspondent is isomorphic with $k[P \rtimes Z_2]$. Then an annual problem. Reprove this result by standard means, or, at least, show the two blocks are Morita equivalent. Generalize to non-principal blocks, proving a Morita equivalence (following Broué's ideas), perhaps even showing the block is a matrix algebra over the correspondent. Finally, perhaps generalize the method of Smith - Tyrer to blocks by some extension algebras.

Let's stick to the original situation now. What do we have? The principal block has two simple modules by Brauer (J. of Alg 3, 225 - 255). By Puig and Rouquier, the principal block and its Brauer correspondent are stably equivalent by a stable equivalence of Morita type (a summand of restriction) which preserves duality, sends the trivial module to the trivial module also. We would like that the other simple module in the principal block goes to the other one-dimensional module for the correspondent to be able to apply Fitzpatrick's theorem.

Some notation: $k = k_+ = k$, $k_- = -$ on the simple k-modules, A the principal block of $N(P)$, k, S the simples of the principal block B of G, U, the k-module corresponding with S, A the Brauer correspondent.

Our goal is to try and prove the following (true) result:

Theorem If $p^n = q$ then B and b are Morita equivalent.

Suppose $P = \langle x, y \rangle$, $X \equiv x-1$, $Y \equiv y-1$ as the monades (with X acting via $\swarrow$, Y by $\searrow$)

make sense and must decompose the indecomposable projectives in b. Since $\underline{Hom}_b(k, U) = \underline{Hom}_b(U, k) = 0$ routine analysis shows that the upper and lower Loewy slices of U coincide and unless $U \cong k_-$, we have the picture

$$U = \begin{array}{c} - \cdots - \\ \hline + \cdots + \\ \hline - \cdots - \end{array}$$

We want to demonstrate this possibility and establish $U \cong k_-$ so Eilenberg's theorem applies and we are done.

Lemma. Suppose U is a b-module with the structure just described (Loewy length three, etc.). Then the following are equivalent:

1) U has a one-dimensional stable endomorphism algebra

2) The image of $End(U)$ in $End(U, \Omega U)$ is one-dimensional and any homomorphism of U to ΩU has image in $soc(\Omega U)$.

Proof. We have the exact sequence

$$0 \to \Omega U \to PU \to U \to 0$$

where PU is the projective cover of U. This gives

$$0 \to Hom(U, \Omega U) \to Hom(U, PU) \to Hom(U, U) \to Ext^1(U, \Omega U) \to 0$$

where, as usual, $\mathrm{Ext}^1(U, \Omega U) \simeq \underline{\mathrm{Hom}}(U, U)$. Hence,

$$\dim \underline{\mathrm{Hom}}(U,U) = \dim \mathrm{Hom}(U,U) - \dim \mathrm{Hom}(U, PU) + \dim \mathrm{Hom}(U, \Omega U).$$

Hence, if the dimensions of the Loewy layers are, from the top, d, e, f then

$$\dim \mathrm{Hom}(U,U) \geq 1 + df$$
$$\dim \mathrm{Hom}(U, PU) = d^2 + df$$
$$\dim \mathrm{Hom}(U, \Omega U) \geq d^2$$

Hence, (1) holds if, and only if, $\dim \mathrm{Hom}(U,U) = 1 + df$ and $\dim \mathrm{Hom}(U, \Omega U) = d^2$, so we are done.

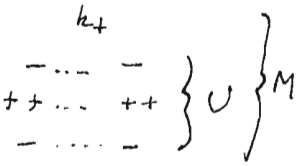
Now let U be the correspondent of S so now U is also self-dual, as B has two simples, the block is self-dual and k is in B. In particular, using the above notation, we have $d = f$. Because of the structure of the projective modules in A, we must have $e \leq 2d$.

Lemma $e < 2d$.

Proof. Suppose that $e = 2d$. It suffices to prove that $\mathrm{Ext}^1(k, U) = 0$ as then A decomposes and is not a block (remember U is self-dual). Suppose we have an exact sequence

$$0 \to U \to M \to k \to 0.$$

Now $M/\mathrm{soc} M = M/\mathrm{rad}^2 M$ is a projective $A/\mathrm{rad}^2 A$ module, by hypothesis. Similarly, $\mathrm{soc}^2 M$ is an injective $A/\mathrm{rad}^2 A$ module. Suppose first, that the extension does not split modulo $\mathrm{rad} U$. Then, if $m \in M$ is non-zero image in k, we have $Xm \neq 0$ or $Ym \neq 0$ modulo $\mathrm{rad} U$. If $Xm \neq 0$ then $YXm \neq 0 \bmod \mathrm{rad}^2 U$ or $XYm \neq 0 \bmod \mathrm{rad}^2 U$ or $Ym \neq 0 \bmod \mathrm{rad} U$. In all is way, using this can



combinations of X and Y we get that Xm, Ym are linearly independent mod rad U. Then X^2m, YXm, XYm, Y^2m are independent mod $\mathrm{rad}^2 U$ by the freeness, which is a contradiction as $XYm = YXm$. Hence, the extension of $U/\mathrm{rad}\,U$ by k splits. Thus, if the lemma fails there is a non-split extension of $\mathrm{soc}^2 U$ by k which is also a module for $b/\mathrm{rad}^2 b$. But the injectivity shows this cannot be either so the lemma is proved.

The goal next is to construct b modules which have a series of submodules with successive factors $U, k, U, k, U, \ldots$ such that each extension of one factor by the next does not split. Using the stable equivalence, as it is of Morita type, and "stripping out" the projectives we get a module with a series with successive factors $S, k, S, k, S, \ldots$ with similar non-splitting so it is uniserial (by calculating the radical series), a contradiction to Brauer Loewy length. (Note that the lemma just proven immediately implies the existence of a non-split extension of k by U. Of course this is true anyways as there is no non-split extension of k by k.)

We first want to make explicit the structure of the projectives as pictured above and not use the "equivalence" $X \equiv x - 1$ (which means mod rad^2). From the obvious truncated polynomial algebra on X, Y, so $X^3 = Y^3 = 0$. Adjoin $Z_2 = \langle t \rangle$ inverting X, Y, i.e. $t(X) = -X$, $t(Y) = -Y$. Then this is isomorphic with b in fact. Here are two proofs. Modulo the square of the radical of the polynomial algebra we have $1+X, 1+Y$

are inverted by t. Hence, in the same coset there are, by Mesdhe's theorem, elements of the polynomial algebra inverted by t and these give the isomorphism. Second, we can do this explicitly. Let $x = 1 + X - X^2$ so $x^{-1} = 1 - X - X^2$ (calculate) so x is carried to x^{-1} by t, the same for Y, y.

Suppose now that M is a module for $k[X,Y]\langle t\rangle$ annihilated by the square of the radical of $k[X,Y]$ and we consider M^* with respect to the group $\langle x, y, t\rangle$. So we can assume that $x = 1+X$, $y = 1+Y$ when acting with M. If $\varphi \in M^*$ then

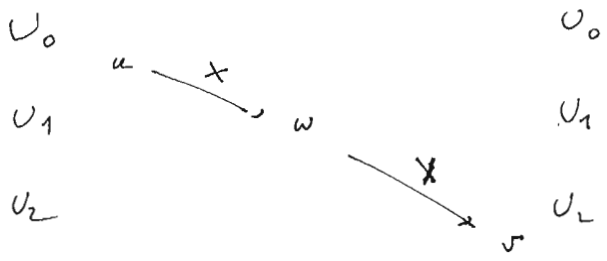
$$X\varphi = (x-1)\varphi = \varphi(x^{-1}-) - \varphi(-) = \varphi((x^{-1}-1)\,-) = \varphi(-X\,-) = -\varphi(X-).$$

The same then holds for Y and any linear combination of X and Y and we get the usual consequences for example that the kernel of X on M and the kernel of X on M^* have the same dimension.

Now write a vector space direct sum $U = U_0 + U_1 + U_2$ where $U_1 + U_2 = \operatorname{rad} U$, $U_2 = \operatorname{rad}^2 U$, U_1 is the -1 eigenspace for t on U, $U_0 + U_2$ is the $+1$ eigenspace for t on U. Then tXu, for $u \in U_0$, equals $-Xtu = Xu$ so lies in U_1. Similarly $XU_1 \subseteq U_2$.

Suppose now that X, or any linear combination of $X+Y$, with not both coefficients zero, acting on $U/\operatorname{soc} U$ has kernel bigger than $\dim U_1$. Then X acting on $\operatorname{rad} U$, the dual of $U/\operatorname{soc} U$, as $U \cong U^*$, has the same property so $XU_1 \subsetneq U_2$. And conversely as well. Let us pursue this case to get a construction that will show that this case can be dismissed in the manner we hoped for.

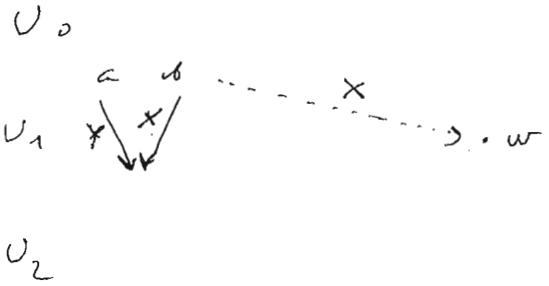
Let $0 \neq a \in U_0$ be in the kernel of X and let $v \in U_2$ be not in the image of U_1 under X. Using basis "adjoin" an element w so the following picture makes sense (i.e. a module by generators and relations):



So we start with the vector space $U \oplus kw \oplus U$. Usual action of X, Y except Xu is the sum of the image of u in U under X (given) plus w. $Yw = 0$, $Yw = v$ etc... It is easy to see this makes sense (test that X, Y commute; e.g. say $YXu = Yw = 0$, $XYu = X(Yu) = 0$ since X, Y commute on U). This module is a triple extension as desired. The non-splitting is what remains to prove. But the calculation of radicals and socles gives this easily. For example, modulo the "second U" we have w in the radical as $Xu = w$. Now "iterating" this construction "to the right" and we have the construction we want. Hence, we can now assume that X, and any $\lambda X + \mu Y$, $(\lambda, \mu) \neq (0,0)$, has no kernel on U_0.

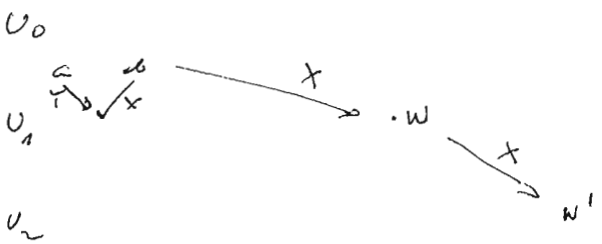
We now have that $\dim XU_0 = \dim YU_0 = \dim U_0$ while $\dim U_1 < 2 \dim U_0$, by the lemma, so $XU_0 \cap YU_0 \neq 0$. Hence, there are a, b non-zero elements of U_0 with $Xa = Xb$. By the elimination of the above case we have that a and b are linearly independent.

Using a basis of U_0 construct a new module as follows:

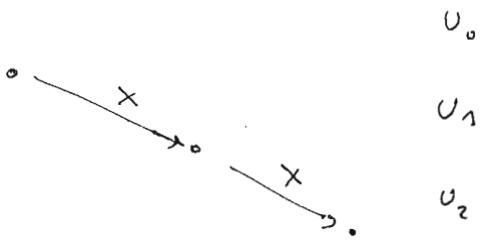


So now Xb is the sum with the new term W. Now when we apply X, Y to a basis of U_0 containing a and b we want to check that we get $U_1 + kW$. The only problem is we get $v+w$ instead of v, where $v = Xb$ in U. But we pick up $v = Ya$ anyways so we now get w in the radical and since we get all of U_1 modulo W we have what we want. This gives a non-split extension of k by U.

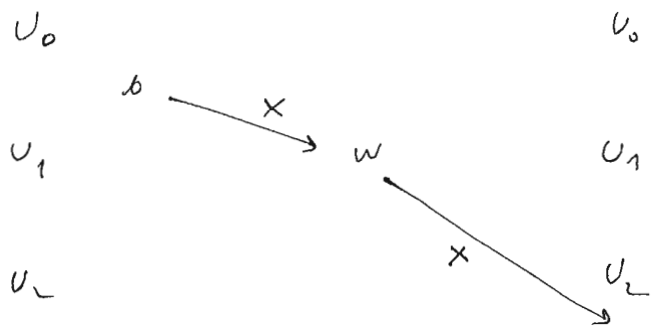
There is a bigger module:



which is a triple extension of k by k by U each extension non-split. By duality we get such a module

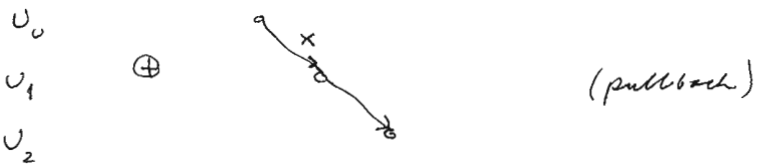


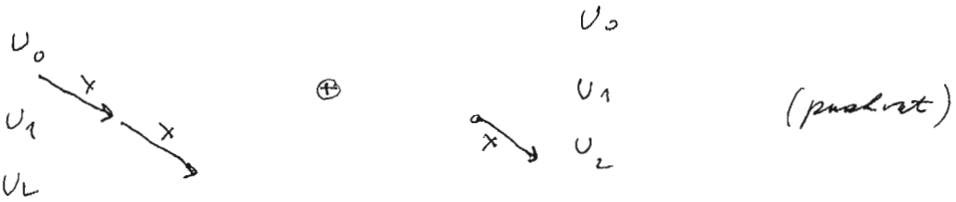
All the generators and relations must work! Hence, when we construct the following module it works and gives an extension of k by U non-split as a quotient and a submodule which is a non-split extension of k by U:



So we are done.

We can do these constructions and pushouts and pullbacks:





Endo-simple modules

Let A be an algebra over an algebraically closed field k. An A-module M is endo-simple if $\mathrm{End}_A(M) \cong k$. Let $\mathcal{M}$ be a family of endo-simple A-modules with $\mathrm{Hom}_A(M, M') = 0$ whenever M and M' are distinct members of $\mathcal{M}$. Let $\mathcal{A}$ ($= \mathcal{A}_{\mathcal{M}}$) be the full subcategory of $\mathrm{mod}\, A$ of modules which have a filtration (a "dipping filtration," below) with each successive quotient isomorphic with a member of $\mathcal{M}$. Then $\mathcal{A}$ is an abelian category, its simples are the modules isomorphic with members of $\mathcal{M}$ and it satisfies the Jordan-Hölder theorem. It is closed under sums and intersections (of submodules in $\mathcal{A}$ of a module in $\mathcal{A}$).

Thus, we have a "baby" result analogous to Richard's construction for derived categories of symmetric algebras, in that we have modules that "look like" simple modules, a generation condition (dipping $\mathcal{A}$) and a structure result. Is there a corresponding result for $\underline{\mathrm{mod}}\, A$, the stable category?

First, before proofs, an example. Suppose S and T are non-isomorphic simple A-modules and $\mathcal{M}$ consists of non-split extensions of T by S (T the submodule). It is easy to check that the conditions above are satisfied. However, it can be that $\mathcal{M}$ is even infinite!

Let's turn to the proofs. We keep all the above notation.

Lemma. If M is in $\mathcal{M}$, U in $\mathcal{A}$ and $0 \neq \varphi \in \mathrm{Hom}_A(M, U)$ then φ is 1-1 and there is a dipping filtration of U through $\varphi(M)$.

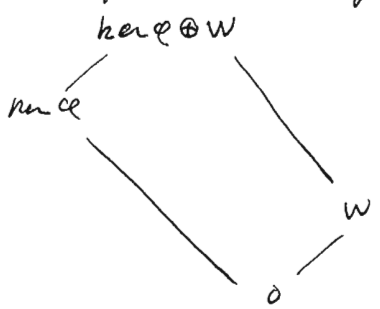
Proof. Let

$$U = U_0 > U_1 > \cdots > U_s = 0$$

be a decreasing filtration of U and choose i so that $\varphi(M) \subseteq U_i$, $\varphi(M) \not\subseteq U_{i+1}$. Hence, a quotient of M is isomorphic with a submodule of U_i/U_{i+1} so this must be an isomorphism between M and U_i/U_{i+1} and $U_i = M \oplus U_{i+1}$ so φ is certainly $1\text{-}1$ and the first isomorphism theorem gives the desired filtration of U.

Lemma If U, V are in $\mathcal{A}$ and $\varphi \in \mathrm{Hom}_A(U, V)$ then $\ker\varphi$, $\mathrm{im}\,\varphi$ are in $\mathcal{A}$ and there are decreasing filtrations of U, V through $\ker\varphi$, $\mathrm{im}\,\varphi$, respectively.

Proof. We proceed by induction on the dimension of U so the previous lemma gets us started. Let W be a submodule in a decreasing filtration of U with W isomorphic with a module in M. If $\varphi(W) = 0$ then we can apply induction to U/W and V and we are done. Hence, by the preceding lemma again, φ is $1\text{-}1$ on W and $\varphi(W)$ is a term of a decreasing filtration of V. We can now apply induction to U/W and $V/\varphi(W)$ so $\varphi(U)$ is as stated. We deal with the kernel of φ as follows. We have $\ker\varphi + W/W$ as a kernel, applying induction and using the first isomorphism theorem gives the desired filtration. (Have a decreasing filtration of U/W through $\ker\varphi \oplus W/W$.)



Next, let V, W be submodules of the module U with U, V, W in $\mathcal{A}$. The embedding of V in U shows, by the previous lemma, that $\mathcal{A}_{/V}$ is a descending filtration of U through V (and similarly one through W). Hence, U/V is also in $\mathcal{A}$. The kernel of the map from U to $U/V \oplus U/W$ is $V \cap W$ so $V \cap W$ is in $\mathcal{A}$. The image of the map from $V \oplus W$ to U is $V + W$ so this also lies in $\mathcal{A}$. The inductive proof of the Jordan-Hölder theorem now applies (see Algebra - Bell for example).

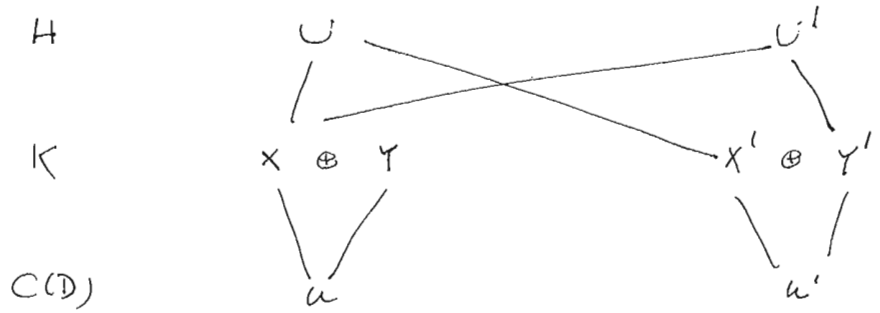
Remarks on local blocks of defect p^2

Suppose B is a block of G with defect group $D \cong Z_p \times Z_p$ and Brauer correspondent b of $N(D)$. Let (D, b_D) be a B-Sylow subpair and H the stabilizer of b_D so $D \leq C(D) \leq H \leq N(D)$ and $H/C(D)$ is the inertial quotient and its order is the inertial index of B. Suppose that b has exactly one simple module (in characteristic p). Now by Rouquier's results (see the Oberwolfach meeting) we know that B and b are stably equivalent by a stable equivalence of Morita type. Broué's conjecture says that B and b are derived equivalent so, as b has a single simple module, results of Richard imply that B and b should be Morita equivalent (a consequence of Broué's conjecture was the single simple).

The structure of b, a matrix algebra over a block of H, in terms of "characters" - using Frobenius reciprocity really - means that the inertial index is a square. If T is the simple b_D-module and S is the simple module in the block of H then $\mathrm{Ind}_{C(D)}^{H} T = S \oplus \cdots \oplus S$ (a terms), $\mathrm{Res}_{C(D)}^{H} S = T \oplus \cdots \oplus T$ (a terms) and $a^2 = |H : C(D)|$. If this index is one we are in the nilpotent case. So, suppose it is four.

Let's take a special case. Say $H = Z_p \times Z_p \rtimes Q_8$ with non-faithful action, $Z(Q_8)$ being the kernel of the action. Let U be the indecomposable kH-module corresponding, via $N(D)$ etc..., with the simple B-module. We know we can assume the stabilizer K of a source of U lies strictly between $C(D)$ and H and we want to derive a contradiction.

Here is the plan. First, get the following induct restrict diagram of groups and modules:



Next, we want to use Dade's rigidity ideas, "perturbing X." to show U does not satisfy the needed properties. We do have to show Dade's ideas carry over to a stable equivalence of Morita type.

Suppose $X \neq 1$, $X \in D$ invariant or controlled by a pair of elements of $Q_g - Z(Q_g)$, which generate Q_g. The module X represents x by a linear transformation

$$x \to 1 + T$$

We "perturb" by sending

$$x \to 1 + aT + \binom{a}{2} T^2 + \cdots + \binom{a}{p-1} T^{p-1}$$

for $a \in b$. This works for $a = 1, \ldots, p-1$ (powers!) so it works for all a as the coefficients polynomial of the right degree.

Next generalize to the general case of $|H : C(D)| = 4$ using Puig's theorem on source algebras which gives explicit structure like we have been using.

The Brauer correspondence and Cartan matrices

A celebrated theorem of Brauer states that the Cartan matrix has determinant a power of the characteristic. Besides the original proof there is another using Brauer's characterization of characters and one by Kawada using the "adams operations." We give a short proof using the Brauer correspondence.

Let G be a finite group, k be an algebraically closed field of prime characteristic p and C be the Cartan matrix.

Theorem The determinant of C is a power of p.

We proceed by induction on the order of G. Let M be a kG-module so, as we observed from the Brauer correspondence,

$$M \oplus P_1 \otimes L_1 \simeq P_2 \otimes L_2$$

for suitable projective modules P_1, P_2 and modules L_1, L_2 each the direct sum of modules induced from p-local subgroups. We want to prove that the direct sum of a power of p copies of M has the same composition factors as a virtual projective module. Hence, we are done unless G has a normal non-identity p-subgroup N. In this case we wish to do the same for the indecomposable projective $k\bar{G}$-modules, $\bar{G} = G/N$, as induction applies to G/N and as every simple kG-module is a $k\bar{G}$-module.

Let $\chi_1, \dots, \chi_r$ be representatives of the conjugacy classes of p'-elements of G, let $\Phi, \underline{\Phi}$ be the $r \times r$ matrices of Brauer characters of the simple and indecomposable

projective kG-modules, compatibly indexed, so $\Phi = C\varphi$. Let $\bar{C}$, $\bar{\Phi}$ be the same for $\bar{G}$ using $\bar{Y}_j = Y_i N$ so $\bar{\Phi} = \bar{C}\varphi$ (the same φ of course). But we can apply the result of Alperin-Cochran-Sibley: each indecomposable projective module of kG has the same composition factors as the tensor product of the corresponding indecomposable projective $k\bar{G}$-module and the permutation module of G acting on N by conjugation. Hence, $\Phi = \bar{\Phi} A$ where A is the diagonal matrix with i-th entry $|C_N(Y_i)|$. Hence $C\varphi = \bar{C}\varphi A$ so we are done.

A shift and stack function

We begin with a construction for arbitrary rings A. For $n \geq 0$ let $C_n(A)$ denote the category of complexes

$$C: \quad C_n \to C_{n-1} \to \cdots \to C_0$$

of A-modules. We shall associate an A-module to C and then show that we have a functor between certain categories. The construction is an iteration attaching an element of $C_{n-1}(A)$ to C (and so forth). This construction is in two steps: first construct another element of $C_n(A)$, second truncate this complex.

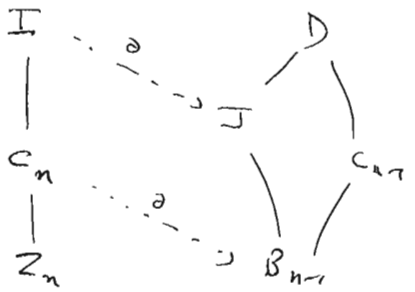
First, let $C_n \to I$ be an injective embedding. Consider the push-out

$$\begin{array}{ccc} I & \cdots\cdots\to & D \\ \uparrow & & \uparrow \\ C_n & \xrightarrow{\partial} & C_{n-1} \end{array}$$

Hence, D is the sum of two modules, one isomorphic with I/Z_n ($Z_n = \ker \partial$, $Z_n = H_n(C)$) and the other C_{n-1} intersecting in a submodule which identifies with C_n/Z_n and B_{n-1} ($= \partial C_n \subseteq C_{n-1}$) respectively. This yields a map of complexes

$$\begin{array}{ccccccccc} I & \to & D & \to & C_{n-2} & \to & \cdots & \to & C_0 \\ \uparrow & & \uparrow & & \uparrow 1 & & & & \uparrow 1 \\ C_n & \to & C_{n-1} & \to & C_{n-2} & \to & \cdots & \to & C_0 \end{array}$$

(using the expression of elements of D as "an element of I/Z_n" and "an element of C_{n-2}"). This can be pictured in the following diagram when $J = I/Z_n$:



$$\begin{array}{ccccc} C_{n-1} & \to & \cdots & \to & C_0 \\ \uparrow 1 & & & & \uparrow 1 \\ C_{n-1} & \to & & \to & C_0 \end{array}$$

Hence, these two complexes are quasi-isomorphic. This is the first step and the second is

$$D \to C_{n-2} \to \cdots \to C_0$$

Note that the $(n-1)$st homology of D is I/Z_n ($H_n(C)$ "shifted") extended by $H_{n-1}(C)$ ("attached" on the shift) and the rest of the homology of this complex agrees with that of C. The construction is now completed by the obvious iteration.

Next, for $m \geq 0$, let $\underline{\underline{C}}_m(A)$ be the category of complexes, as above, modulo the complexes

$$I_m \to 0 \to \cdots \to 0$$

where I_m is an injective A-module. We will now see that we have constructed a functor from $\underline{\underline{C}}_n(A)$ to $\underline{\underline{C}}_{n-1}(A)$. Note that the complex

$$D \to C_{n-1} \to \cdots \to C_0$$

depends on the choice of I. In particular, we could end up with the same complex except D is replaced by the direct sum of D and an injective module, the latter in the kernel of the boundary map so we have a well-defined element of $\underline{\underline{C}}_{n-1}(A)$ in this case. To get a functor we have to worry about composite maps which leads to maps associated to zero maps. But these factor through the complexes we are factoring out, by inspection.

now suppose A is a self-injective finite dimensional algebra over a field k. We want to see that our constructed module (not in $\underline{\mathrm{mod}}(A)$ - we work with finite-dimensional modules now) agrees with Richard's construction. But $I \to D \to C_{n-1} \to \cdots \to C_0$ is quasi-isomorphic to C, we have a triangle (exact)

$$(I \to 0 \to \cdots \to 0) \to (I \to D \to \cdots \to C_0) \to (D \to \cdots \to C_0)$$

in the derived category, the first term goes to zero under Richard's functor and Richard's functor is one of triangulated categories. Hence $I \to D \to \cdots \to C_0$ and $D \to \cdots \to C_0$ have the same image, so we are done by iteration.

We now turn to calculation. The situation is one that Richard has looked at: is a complex of projective A modules

$$X_n \to X_{n-1} \to \cdots \to X_0$$

now regarded as $A \otimes k[Z_2]$ modules, where k has characteristic two and $k[Z_2]$ acts trivially on the right. Let $\Sigma = g - 1$, $\langle g \rangle = Z_2$ so $k[Z_2] = k[\Sigma]$ is the dual numbers. His result is that his functor produces

$$X_n \xrightarrow{\Sigma} X_{n-1} \cdots \xrightarrow{\Sigma} X_0$$

where each boundary is replaced by Σ. Let us see it is from our point of view. First, an injective containing X_n is

$$\begin{array}{c} X_n \\ \Sigma \downarrow \simeq \\ X_n \end{array}$$

so the complex we first construct is

$$(X_n \xrightarrow{\Sigma} X_{n-1}) \xrightarrow{\partial} X_{n-2} \to \cdots \xrightarrow{\partial} X_0$$

Now an injective module which contains $X_n \xrightarrow{\Sigma} X_{n-1}$ is

$$\begin{array}{ccc} X_n & & X_{n-1} \\ {\scriptstyle\Sigma}\downarrow\simeq & \oplus & {\scriptstyle\Sigma}\downarrow \\ X_n & & X_{n-1} \end{array}$$

where $X_n \to X_{n-1}$ injects "diagonally" so $x \in X_n$ goes to $x \oplus \partial x$ where x is in the lower left X_n and ∂x is in the upper right X_{n-1} and X_{n-1} embeds in the lower right X_{n-1}. Picture:

$$\begin{array}{ccc} X_n & & X_{n-1} \\ {\scriptstyle\Sigma}\downarrow\simeq & & {\scriptstyle\Sigma}\downarrow\simeq \\ X_n & & X_{n-1} \end{array}$$

$$X_n \xrightarrow{\Sigma} X_{n-1}$$

It is easy to see that the next complex is

$$(X_n \xrightarrow{\Sigma} X_{n-1} \xrightarrow{\Sigma} X_{n-2}) \xrightarrow{\partial} X_{n-3} \xrightarrow{\partial} \cdots \xrightarrow{\partial} X_0$$

and so on.

Let's look at $p = 3$. We begin with

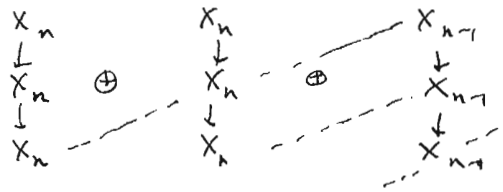
$$\begin{array}{c} X_n \\ \downarrow \\ X_n \\ \downarrow \\ X_n \end{array}$$

$$X_n \to X_{n-1} \to \cdots$$

so our first construction yields

$$(X_n \to X_n \to X_{n-1}) \xrightarrow{\partial} X_{n-2} \to \cdots \to X_0$$

Next we have

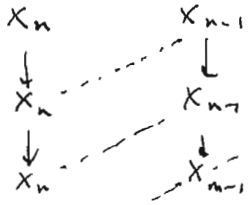


$$X_n \to X_n \to X_{n-1} \qquad \to X_{n-2} \to \cdots$$

where the dotted lines denote the str embedding so $x \in X_n$, "the first X_n" goes to

$$\begin{matrix} 0 & 0 & 2x \\ 0 & x & 0 \\ x & 0 & 0 \end{matrix}$$

Because of the isomorphism between the lower-left X_n and the X_n in the middle we have that the first column intersects the embedded module in zero so it is a projective summand in the kernel so we only have to deal with



so we we factor out the image of

$$X_n \to X_n \to \text{ker}$$

we end up with

$$\left(X_n \to X_{n-1} \to X_{n-1} \to X_{n-2}\right) \to X_{n-3} \to \cdots \to X_0$$

so the pattern is clear.

This also "tells us" the general answer for arbitrary p:

$$\cdots \quad \overbrace{X_3 \to \cdots \to X_3}^{p-1} \to X_2 \to \overbrace{X_1 \to \cdots \to X_1}^{p-1} \to X_0$$

with identity maps inside the groups of $p-1$ modules, Σ acting by 0 elsewhere.

We take another track to prove all this, first going back to $p = 2$. We use tensoring with $k[\Sigma]$ to get an embedding: After the first step:

$$\begin{array}{ccc} X_n & \longrightarrow & X_{n-1} \\ {\scriptstyle \Sigma=1}\downarrow & & \downarrow{\scriptstyle \Sigma=1} \\ X_n & \longrightarrow & X_{n-1} \end{array}$$

$$(X_n \xrightarrow{\Sigma} X_{n-1}) \xrightarrow{\partial} X_{n-2} \to \dots \xrightarrow{\partial} X_0$$

The tensor product is filtered by columns with projective quotients so it is projective! Now factoring out to construct the push-out we get

$$(X_n \xrightarrow{\Sigma} X_{n-1} \xrightarrow{\Sigma} X_{n-2}) \xrightarrow{\partial} X_{n-3} \to \dots \to X_0$$

and so on.

Double cosets and cohomology

We present an exposition of elementary facts about low dimensional non-abelian cohomology of cyclic groups and double cosets. Let α be an automorphism of order n of the group G and let H be the fixed-point subgroup (so $H = H^0(\langle\alpha\rangle, G)$ the zero-th cohomology). Complements to G in $G \rtimes \langle\alpha\rangle$ are in one-to-one correspondence with elements x in G which are norm elements in that

$$x\,\alpha(x)\,\alpha^2(x)\cdots\alpha^{n-1}(x) = 1$$

(as $(x\alpha)^n = x\,\alpha(x)\,\alpha^2(x)\cdots\alpha^{n-1}(x)$ since $\alpha^n = 1$). Now $x\alpha$ and α are conjugate in $G \rtimes \langle\alpha\rangle$ if, and only if, there is $g \in G$ with $x\alpha = g^{-1}\alpha g = g^{-1}\alpha(g)\alpha$, i.e. if and only if $x = g^{-1}\alpha(g)$. (Such elements are norm elements as is trivial to calculate. (Here, the norm elements are $Z^1(\langle\alpha\rangle, G)$ and the x in G which are of the form $x = g^{-1}\alpha(g)$ are $B^1(\langle\alpha\rangle, G)$, so we have cocycles and coboundaries.)

There is a canonical map of $H\backslash G/H$ to H orbits on these coboundaries $B^1(\langle\alpha\rangle, G)$, i.e. the conjugacy class of α in $G \rtimes \langle\alpha\rangle$, sending HgH to $g^{-1}\alpha(g)$, which is well-defined as $(hgh')^{-1}\alpha(hgh') = (h')^{-1}g^{-1}h^{-1}h\,\alpha(g)\,h'$ $= (h')^{-1}g^{-1}\alpha(g)h'$. This is clearly surjective as $g^{-1}\alpha(g)$ comes from $H\backslash G/H$. It is also injective. Suppose that $x^{-1}\alpha(x)$ and $y^{-1}\alpha(y)$ are H-conjugate, where $x, y \in G$. Then

$$\begin{aligned} x^{-1}\alpha(x) &= h^{-1}y^{-1}\alpha(y)h \\ &= (yh)^{-1}\alpha(yh) \end{aligned}$$

so

$$yhx^{-1} = \alpha(yhx^{-1})$$

and $yhx^{-1} \in H$ so $y \in HxH$ as required.

Centralizer rings and Hecke algebras

We shall show how to approach centralizer rings using the standard results on Hecke algebras. Let G be a group and H a subgroup so G is a $G\times H$-set with G acting on the left and H on the right (using inverses) and, if A is a commutative ring (with unit element) then the Hecke algebra (say $\mathcal{H}_A(G\times H, G)$) is isomorphic with the centralizer ring $(AG)^H$ (the right multiplications commuting with H).

We now give a natural one-to-one correspondence between the double cosets of δH in G (as δH is the stabilizer in $G\times H$ of $1\in G$) and the H-classes of G (as their sums are a basis of $(AG)^H$). Consider the map of $G\times H$ to G via $(g,h)\to gh^{-1}$. Then

$$\begin{aligned}(h',k')(g,h)(h'',k'') &= (h'gh'', k'hk'')\\ &\to h'ghk''(h'')^{-1}k^{-1}(h')^{-1}\\ &= h'(gk^{-1})(h')^{-1}\end{aligned}$$

so the whole double coset maps into the same H-class, and, moreover, every element of the class appears and every class appears. All that remains to see is that this is one-to-one as claimed above. But the number of double cosets and the number of H-classes are the same (by the isomorphism of Hecke algebra and centralizer ring, over $\mathbb{C}$ say).

Next, let D be a double coset (of δH in $G\times H$). We want to show that $1/|\delta H|\sum_{d\in D} d$ acts on $1\in G$ the same as the sum of the corresponding H-class. But the map of $G\times H$ to G is $|H|$ to one, so this is immediate.

Let's turn to the characters (should also, perhaps, have a look at central idempotents, perhaps this would yield $Z(\mathbb{C}G)^H = \langle Z(\mathbb{C}G), Z(\mathbb{C}H)\rangle$, but we depend on this.)

Which characters of $G\times H$ occur in $\mathbb{C}[G\times H/\delta H]$?

If χ is an irreducible character of G and ψ is of H then

$$(\chi\otimes\psi, 1)_{\delta H} = 1/|\delta H| \sum_{a} (\chi\otimes\psi)(a,a) = 1/|H| \sum_{a} \chi(a)\psi(a)$$
$$= (\chi, \bar{\psi})_H$$

$\therefore$ used characters of the permutation module are of form $\chi\otimes\varphi$, where $(\chi,\bar{\varphi})\neq 0$ is the multiplicity. Let's calculate the character of the Hecke algebra, say the character corresponding to this character on a double coset. Let K be an H-class, D the corresponding double coset (= set of all elements (g,h), $g\in G, h\in H$, with $gh^{-1}\in K$). Let $\chi\otimes\varphi$ be the character of $G\times H$ we are working with now the corresponding character on this double coset has value

$$1/|\delta H| \sum_{(g,h)\in D} \chi(g)\varphi(h)$$

which is $1/|H| \sum_{\substack{a\in G\\ b\in H\\ ab^{-1}\in K}} \chi(a)\overline{\varphi(b)} = 1/|H| \sum_{\substack{a\in G\\ b\in H\\ a\in K}} \chi(a)\varphi(b)$

But if $x\in K$ then since χ,φ are invariant on H-classes, each element of K occurs equally often, this is, when now D is $1/|H|$ times the num of all elements in the double coset,

$$(\chi\otimes\varphi)(D) = |H : C_H(x)|/|H| \sum_{\substack{a\in G\\ b\in H\\ ab^{-1}=x}} \chi(a)\overline{\varphi(b)}$$

$$= \frac{1}{|C_H(x)|} \sum_{b\in H} \chi(xb)\overline{\varphi(b)}$$

Permutation filtrations

Theorem If M is a kG-module then there are kG-modules X and Y, each filtered by summands of permutation modules, with $M \oplus X \simeq Y$

Can this be improved with X projective, Y filtered by weight conjugates? Yes, if $p=2$ and $G = GL(3,2)$.

Without loss of generality, we may assume that M is simple since if $S_1, S_2, \dots, S_n$ are the composition factors of M and we have X_i, Y_i with $X_i \oplus S_i \simeq Y_i$ then $M \oplus X_1 \oplus \dots \oplus X_n$ is ok, being filtered by $Y_1, \dots, Y_n$. Proceeding by induction on $|G|$, we may also assume $O_p(G) = 1$ so every p-local subgroup is proper. Let Q be the vertex of M and now go by induction on $|Q|$, the case $|Q|=1$ being trivial. Let $L = N(Q)$, M' be the Green correspondent of M so $M' \oplus X' \simeq Y'$ by induction, so $\operatorname{ind}_L^G M' \oplus \operatorname{ind}_L^G X \simeq \operatorname{ind}_L^G Y'$. But $\operatorname{ind}_L^G M' = M \oplus E$ where the vertices of the components of E are contained properly in Q so we have, by induction, $E \oplus X'' \simeq Y''$ and so

$$\operatorname{ind}_L^G M' \oplus X'' \oplus \operatorname{ind}_L^G X' \simeq \operatorname{ind}_L^G Y' \oplus X''$$

$$M \oplus E \oplus X'' \oplus \operatorname{ind}_L^G X' \simeq \operatorname{ind}_L^G Y' \oplus X''$$

$$M \oplus (Y'' \oplus \operatorname{ind}_L^G X') \simeq \operatorname{ind}_L^G Y' \oplus X''$$

as desired.

McKay's conjecture for Σ_n

We are interested in finding structural reasons for the validity of the McKay conjecture for Σ_n when $p = 2$. In particular, a nice one-to-one correspondence between linear characters of the Sylow 2-subgroup and the odd characters (those of odd degree) not just the known combinatorial results. We start with a case when the answer is clear and use this to conjecture about possible approaches.

If P is a Sylow p-subgroup of the group G we say that we have a Navarro correspondence if his result for p-solvable groups carries over, inducing each linear character of P we get exactly one p'-character and a one-to-one correspondence. This leads to the congruence, as we observed in the p-solvable case, of a submatrix of the character table of the Hecke algebra for G/P' using the character table of P/P'. The following standard fact is one way of seeing this:

Lemma If χ is an irreducible character of the group G, H is a subgroup of G and $(\chi_H, 1_H)_H = 0$ then

$$\sum_{k \in H} \chi(xk) = 0$$

for any $x \in G$.

Proof. Let $e = \frac{1}{|H|} \sum_{k \in H} k$, so e is an idempotent and the trace of e on S, a $\mathbb{C}G$-module affording χ, is zero, by hypothesis, so therefore, as e is an idempotent, $eS = 0$ so $xeS = 0$ so xe also has trace zero on S, as required.

Proposition If $G = \Sigma_{2^n}$ and $p = 2$ we have a Navarro correspondence.

Proof. Let P be a Sylow 2-subgroup so $|P/P'| = 2^n$ as $P \simeq Z_2 \wr \cdots \wr Z_2$ (n factors) so there are, since McKay's conjecture holds here, thus 2^n odd characters. But the 2^n hooks are of odd degree, by a direct calculation, so they are the odd characters in this case.

We proceed by induction ($n = 1$ is O.K.) using $P = Z_2 \wr \Sigma_{2^{n-1}}$, $P = B \rtimes \Sigma_{2^{n-1}}$ where $B = \langle (12), (34), \ldots \rangle$ is the base group. We shall use results on plethysms and hooks to finish the proof, and then give a direct argument.

Any linear character of P restricted to B is either the trivial character or the one that sends each generator of B, i.e. $(12), (34), \ldots$ to minus one. Thus the only irreducible characters of $Z_2 \wr \Sigma_{2^{n-1}}$ whose restriction to P might give a linear character as a constituent are the characters arising in calculating plethysms. But the results of the following two papers give what we need:

1. J. O. Carbonara, J. B. Remmel and M. Yang, "S-series and plethysm of hook-shaped Schur functions with power-sum symmetric functions," Series Formelles et Combinatoire Algebrique (ed. P. Leroux and C. Reutenauer) Publications du Laboratoire de Combinatoire et d'Informatique Mathématique (1992), 95-110.
2. T. M. Langley & J. B. Remmel, The plethysm $S_\lambda[S_\mu]$

at hook and near-hook shapes, The Electronic Journal of Combinatorics 11 (2004), 1–26.

Now let's turn to a more direct approach to this result using nothing more than exterior algebras. We consider a more general situation, looking at Σ_{2n}, $\mathbb{Z}_2 \wr \Sigma_n \leq \Sigma_{2n}$, $B = \langle (12), (34), \ldots, (2n-1\ 2n) \rangle$ the base group. Let these generators be denoted by $b_1, b_2, \ldots, b_n$. Let λ_0 be the principal character of B, let λ_i, $1 \leq i \leq n$, be the linear character of B with $\lambda_i(b_i) = -1$, $\lambda_i(b_j) = 1$ if $i \neq j$, $1 \leq j \leq n$. Let η be the character of the natural $2n$-dimensional module so

$$\eta_B = n\lambda_0 + \lambda_1 + \ldots + \lambda_n$$

so the character of the hook $[2n-1, 1]$ on B is $(n-1)\lambda_0 + \lambda_1 + \ldots + \lambda_n$ (since, over $\mathbb{C}$, there is a fixed vector "outside" the augmentation kernel of the natural module). Computing exterior powers and the action of Σ_n ("double one" in $B \rtimes \Sigma_n$) on the exterior powers is easy and yields the desired result.

This suggests an approach to our problem. Study restriction from Σ_{2n+1} to Σ_{2n} and $\mathbb{Z}_2 \wr \Sigma_n \leq \Sigma_{2n}$. In the first situation, there should be a one-to-one correspondence between odd characters of Σ_{2n} and those of Σ_{2n+1} given by induction + restriction, with unique odd components occurring! (Perhaps there should be an extension of the idea of a Navarro correspondence to cover p'-characters of a subgroup and those of the group, arbitrary subgroup?)

But there seems to be a much better conjecture, quite surprising. Let's fix some notation. Let

$$n = 2^{a_1} + 2^{a_2} + \dots + 2^{a_t}$$

where $a_1 > a_2 > \dots > a_t \geq 0$, the dyadic expansion of n. We explain, conjecturally, how to give a construction of all the young diagrams (all $2^{a_1+\dots+a_t}$ of them) belonging to the odd characters of Σ_n. Start with the 2^{a_1} hooks of length 2^{a_1}. To each one of these consider adding hooks of length 2^{a_2} in arbitrary ways, but "keep" only those diagrams which are odd. For each of the 2^{a_1} hooks there will be exactly 2^{a_2} ways of doing this so that the resulting diagram for $\Sigma_{2^{a_1}+2^{a_2}}$ is odd and all the $2^{a_1} \cdot 2^{a_2}$ such diagrams are distinct and all the odd ones for this group. This behavior persists for 2^{a_3} and so on. We have a sort of "layering" of the odd diagrams of Σ_n, a sort of "onion" structure.

We can "peel" also, starting with an odd diagram for Σ_n, there is a unique removable 2^{a_t} hook which results in an odd diagram, and so on.

Notice that when $a_t = 0$ we have the situation of "$2n+1$ versus $2n$" discussed above. That situation could be studied with characters, 2-groups, the known perfect matching which should pick out the correspondence we are seeking. But how would that generalize? Very murky.

We have calculated many examples, let's do a few more here. For example, $n=7$, up to ducks, so only after from odd characters. Use x, y, z for notation for successive books!

$x\,x\,x\,x$ $\quad$ $x\,x\,x\,x\,y\,y\,z$
$y\,y$
z

$x\,x\,x\,y\,y$ $\quad$ $x\,x\,x$
x $\quad$ $y\,y\,y$
z $\quad$ z

For example, some of the answers for $n=12$

$x\,x\,x\,x\,x\,x\,x\,x\,x\,\ldots$
$x\,x\,x\,x\,x\,x\,x\,x$
$\cdot\,\cdot\,\cdot\,\cdot$
$x\,x\,x\,x\,x\,x\,x\,>$
$\cdot\,\cdot\,\cdot$
$\cdot$
$x\,x\,x\,x\,x\,x\,x\,x$
$\cdot\,\cdot$
$\cdot$
$\cdot$

$x\,x\,x\,x\,x\,x\,x\,\ldots$
x
$x\,x\,x\,x\,x\,x\,x$
$x\,\cdot\,\cdot\,\cdot\,\cdot$
$x\,x\,x\,x\,x\,x\,x$
$x\,\cdot\,\cdot$
$\cdot\,\cdot$
$x\,x\,x\,x\,x\,x\,>$
$x\,\cdot$
$\cdot\,\cdot$
$\cdot$

For odd p everything goes wrong, but should have a book of character with $n = p^{a_1} + \cdots + p^{a_t}$, $a_1 > \cdots > a_t \geq 0$.

Finally the "peeling" suggests how to get a correspondence for $p=2$. Use the connection between linear characters and books for powers of 2 in connection with the direct product structure of the Sylow 2-subgroups.

Unipotent conjugacy : double cosets

This is an addendum to our note. Let $G = GL(n,q)$, $U = U(n,q)$ (upper uni-triangular group), H the diagonal group. We are interested in the U-conjugacy in each U,U double coset. Let W be the Weyl group of all permutation matrices.

Proposition: If $h \in H$, $w \in W$ then the number of U-conjugacy classes in $UhwU$ equals the number of $U \cap w^{-1}Uw$ classes in Uhw.

Proof. Clearly every element of $UhwU$ is U-conjugate with an element of Uhw, so the question is when are two elements of Uhw U-conjugate and the answer is if, and only if, they are $U \cap w^{-1}Uw$ conjugate. But suppose $v \in U$ and $v(uhw)v^{-1} \in Uhw$, where $u \in U$. That is,

$$v\,u\,h\,w\,v^{-1}w^{-1}w = u'hw$$

for some $u' \in U$ so

$$v\,u\,h\,w\,v^{-1}w^{-1}h^{-1}h = u'h$$

$$w\,v^{-1}w^{-1} = h^{-1}(u^{-1}v^{-1}u')h \in U$$

and $v \in w^{-1}Uw$ as desired. Conversely, if $v \in w^{-1}Uw$ then $v(uhw)v^{-1} = v\,u\,h\,w\,v^{-1}w^{-1}\cdot w = v\cdot u\cdot h(w\,v^{-1}w^{-1})h^{-1}hw$ as desired.

Remarks. The structure of $U \cap w^{-1}Uw$ is well known, the set Uhw is Uh with the columns permuted. We would like the number of $U \cap w^{-1}Uw$ classes in Uhw to be polynomial with a finite number of cases for each fixed w and varying h.

Let's turn to the case $w=1$, i.e. U-conjugacy in Uh where $h \in H$ is fixed. The situation is quite simple.

Proposition 2. If $h \in H$ then any element of Uh is U-conjugate to an element of the form ch, where $c \in C_U(h)$. Two elements $c_1 h$, $c_2 h$, where $c_1, c_2 \in C_U(h)$, are U-conjugate if, and only if, c_1 and c_2 are conjugate in $C_U(h)$.

Remark. It is easy to see that $C_U(h)$ is a direct product of groups each isomorphic to some $U(m, g)$, $m \leq n$. For the ij entry, $i \neq j$, of an element of U commuting with h is zero if the ii and jj entries of h are distinct.

Proof. The element uh has a canonical factorization as the product of a p-element and a commuting p'-element, the latter being conjugate with h in $B = UH$, so the rest is clear.

The "same" result holds over an arbitrary field F.

Prop. 3. If M is an $n \times n$ upper triangular matrix then M is conjugate, by an element of $U(n, F)$, to a matrix where the ij entry is zero whenever the ii and jj entries are distinct.

Since $B(n, F) = U(n, F) \rtimes H$ it suffices to show that any conjugacy by an element of B. Let $e_1, \ldots, e_n$ be the standard

basis of the space $V_n(F)$ of column vectors, let $0 = V_0 < V_1 = Fe_1 < \dots < V_n = V_n(F)$ be the standard flag. Suppose the ii entry of M is λ so M induces multiplication by λ on V_i/V_{i-1} and there is $v_i \in V_i - V_{i-1}$ which is a generalized eigenvector for λ for M. Using the basis $v_1, \dots, v_n$ we need only verify that the matrix corresponding to the action of M on this basis has the needed properties. But if $j < i$, the action of M on V_j/V_{j-1} is multiplication by $\mu \neq \lambda$ then there is no vector in $V_j - V_{j-1}$ which lies in the λ generalized eigenspace (third isomorphism theorem, for example). So the λ space is spanned by the V_i where the ii entry of M is λ and we are done.

The "point" of the above, if we wish to make "reductions" for arbitrary double cosets of U, not just those in B, is that the methods will likely work for all fields. Hence, we turn to another proof of the previous result, one just using matrix calculations, in the hope that more elementary is easier to generalize.

We still proceed by induction on n, so we can assume that

$$M = \begin{pmatrix} N & X \\ 0 \cdots 0 & a_{nn} \end{pmatrix}$$

where N is $(n-1) \times (n-1)$ and has the desired vanishings, X is a $n-1 \times 1$ column vector and $a_{nn} \in F$. We want to find a matrix

$$\begin{pmatrix} I_{n-1 \times n-1} & Y \\ 0 \cdots 0 & 1 \end{pmatrix}$$

which conjugates M into the right sort of matrix. But calculating

$$\begin{pmatrix} I & Y \\ 0 & 1 \end{pmatrix}\begin{pmatrix} N & X \\ 0 & a_{nn} \end{pmatrix}\begin{pmatrix} I & -Y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} N & X + a_{nn}Y \\ 0 & a_{nn} \end{pmatrix}\begin{pmatrix} I & -Y \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} N & -NY + X + a_{nn}Y \\ 0 & a_{nn} \end{pmatrix}$$

By subtracting a scalar matrix from M we can, without any loss of generality, assume that $a_{nn} = 0$. So all we are "doing" is replacing X by $X - NY$. We want to make certain entries of $X - NY$ to be zero. Let's do this step by step, rather than by a single diagonalization, in another induction. Say the k-th entry of X is not zero, but all entries k-th on later, $l > k$, are as desired, but we want it to be zero. That is, the k-th entry of N on the diagonal is not zero. Taking Y to have a suitable non-zero entry in its k-th position and zero elsewhere leads to replacing X by a vector with one more zero (the previous ones are left alone).

The case $n = 2$ is quite clear, but $n = 3$ is already more touchy. Let's take a look. So assume $n = 3$ $w = (12)$ $h = \begin{pmatrix} \alpha & \beta & \gamma \end{pmatrix}$ so $Uh = \begin{pmatrix} \alpha & * & * \\ 0 & \beta & * \\ 0 & 0 & \gamma \end{pmatrix}$ and $UhW = \left\{ \begin{pmatrix} a & \alpha & b \\ \beta & 0 & c \\ 0 & 0 & \gamma \end{pmatrix} \right\}$ while $U \cap w^{-1}Uw = \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$. We calculate the conjugation:

$$\begin{pmatrix} 1 & 0 & x \\ 1 & y & \\ & & 1 \end{pmatrix}\begin{pmatrix} a & \alpha & b \\ \beta & 0 & c \\ 0 & 0 & \gamma \end{pmatrix}\begin{pmatrix} 1 & 0 & -x \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a & \alpha & b + \gamma x \\ \beta & 0 & c + \gamma y \\ 0 & 0 & \gamma \end{pmatrix}\begin{pmatrix} 1 & 0 & -x \\ 1 & -y & \\ & & 1 \end{pmatrix} = \begin{pmatrix} a & \alpha & -ax - ay + b + \gamma x \\ \beta & 0 & -\beta x + c + \gamma y \\ 0 & 0 & \gamma \end{pmatrix}$$

In order to replace b & c by zeros we need $\det \begin{pmatrix} a - \gamma & -\alpha \\ \beta & \gamma \end{pmatrix} \neq 0$, i.e. $a \neq \gamma + \frac{\alpha\beta}{\gamma}$. So can't do always!

Small centralizers

Def If P is a p-group then $\mathcal{E}(P)$ is the set of elementary abelian subgroups of order p^2 which are also maximal elementary abelian. We set $E(P) = \langle E \mid E \in \mathcal{E}(P) \rangle$.

Problem: Find a bound, in terms of p, for the number of conjugacy classes of subgroups in $\mathcal{E}(P)$.

Let's look at an example, $P = Z_{p^e} \wr Z_p = \langle x_1, \dots, x_p, s \rangle$ with $s x_i s^{-1} = x_{i-1}$, mod p and so forth. Then $\langle s, x_1^{p^{e-1}} \cdots x_p^{p^{e-1}} \rangle$ is in $\mathcal{E}(P)$. Moreover $s x_1^{a_1} \cdots x_p^{a_p}$, $a_i \in \mathbb{Z}/p^e\mathbb{Z}$, has order p, if, and only if, $\sum a_j = 0$ (in $\mathbb{Z}/p^e\mathbb{Z}$, remember) as is easy to see by "collection." Any element of order p, of this form, has centralizer in P of the form $Z_p \times Z_{p^e}$ so lies in an element of $\mathcal{E}(P)$. $E(P)$ is generated by those subgroups of order p^2 consisting of one of these elements, the central subgroup of order p & the gp. they generate. In particular $E(P) \trianglelefteq P$. Moreover, $E(P)$ is of maximal class, by looking at the centralizer of such elements of order p.

Let us check such examples are no problem.

Prop Let P be a p-group of maximal class. Then the number of conjugacy classes of subgroups in $\mathcal{E}(P)$ is at most $p+1$.

Lemma Let P be a p-group of maximal class. Let $x \in P - P'$ be of order p with $C_{P_1}(x)$ cyclic. Then $C_{P_1}(x) = Z(P)$, $x^P = xP'$ and, consequently, there are at most $p^2 - p$ such conjugacy classes of elements.

Pf. The case $p = 2$ is trivial so assume $p > 2$. If $|P| \leq p^{p+2}$ then P_2 has exponent p (see Leedham-Green + McKay book) and so the first statement holds in this case. If $|P| > p^{p+2}$ then P has positive degree of commutativity (see L-M) so all 2-step centralizers agree. $\therefore x \notin P_1$ (or it would centralize $Z_2(P) \cong Z_p \times Z_p$). $\therefore x$ centralizes no 2-step quotient P_i / P_{i+2} so $C_{P_1}(x) > Z(P)$ would contradict this (using an element of $C_{P_1}(x) - Z(P)$ and where it lies in the lower central series). The second assertion now follows by counting. Finally, $x \notin C(Z_2(P_1))$ which lies between P and P' (no matter the degree of commutativity) so we get the final count.

Pf (of Proposition). Follows from the lemma (at most p classes of such subgroups of order p^2 not contained in P') once the fact that there is at most one such subgroup ($Z_2(P_1)$) inside P'.

Note that the bound is achieved in groups of order p^3 and exponent p. Note also that it is easy to modify the above to deal with $P \circ Z_{p^n}$, P of maximal class. Need

to work at elements of order p^2 in P like what happens in the Lemma.

In order to have an inductive approach to the problem possible we have the following:

Proposition If P is a p-group with $P = E(P)$ then P has a maximal subgroup M generated by subgroups of $\mathcal{E}(P)$ which it contains, so $M = E(M)$

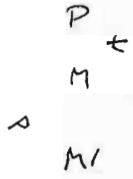
Proof. Since $P = E(P)$ there are subgroups $E_1, \dots, E_d$ of $\mathcal{E}(P)$ such that $P/\Phi(P)$ (of order p^d) is the direct product of the images in $P/\Phi(P)$. Let N be the normal subgroup generated by all the conjugates of $E_2, \dots, E_d$ so P/N must be cyclic (generated by the image of E_1) and of order p as E_1 is of exponent p. Hence $|P:N| = p$ and we are done.

We can go "further down" to smaller subgroups in the same way using conjugacy classes of elements of $\mathcal{E}(P)$ in subgroups, i.e. the classes above of the subgroups.

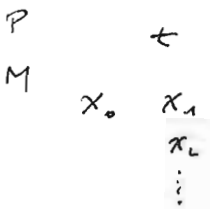
Also note that the number of generators of P, with $P = E(P)$, is at most $\binom{p}{2}$, for p odd, by a result of Thompson (see Huppert) since every normal abelian subgroup of P has rank at most p. Hence to get bounds on the number of classes in $\mathcal{E}(P)$, it suffices to bound $|C_P(E) \cap \Phi(P)|$ for $E \in \mathcal{E}(P)$, where $P = E(P)$, $E \notin \Phi(P)$. This is because we have only to

count elements from the subgroup $E \in \mathcal{E}(P)$ which lie in $P - \Phi(P)$ divided up into conjugacy classes

Let's look at one case, assume M is a maximal subgroups of the p-group P with M generated by the elements of $\mathcal{E}(P)$ which it contains and $t \in P - M$ with $C_P(t) = \langle t \rangle \times$ cyclic. If t does not centralize M/M' then P is of maximal class again. Otherwise, if $s \in M - M'$ with $C_M(s) = \langle s \rangle \times$ cyclic then $s^t \in sM'$ which, by the lemma, is s^M so $s^t = s^u$, $u \in M_2$ so tu^{-1} centralizes s. The picture



Next, suppose a maximal subgroup looks like this, say, for example, M is the central product of a p-group of maximal class and a cyclic group of order p^2, generated by z, with the group of maximal class having elements $x_0, x_1, x_2, \ldots$ and so on (and assume of positive degree of commutativity e.g. as well. Let $t \in P - M$ of order p with $C_P(t) = \langle t \rangle \times$ cyclic. Picture:



If t centralizes M/M' then we can get $C_P(x_0)$ having $\mathbb{Z}_1 \times \mathbb{Z}_1 \times \mathbb{Z}_p$ as an image, so this would be a contradiction. So how does t act? On M, the elements of order p and p^2 with the "good" small centralizers are in the cosets of M' containing $x_0^a x_1^b z^c$ where

$0 < a < p$, $0 \le b < p$, $0 \le c < p$. For each a, b there is a unique c with $X_0^a X_1^b Z^c$ of order p. So can this be? The subgroup $\langle Z \rangle$ is the center of M so invariant under conjugation by t. So is $\langle X_1, X_2, \ldots, Z \rangle$ which is the centralizer of $Z_2(M)$ as is easy to see. Some cases should be examined!

In any case, we hope that the p-groups G with $\mathcal{E}(G) = G$ are close to being of maximal class and that this suffices for the obtaining of bounds. For example, suppose we can show that for a fixed prime p the coclass of such groups is uniformly bounded. Then by Conjecture A (p. 129, L-M) such a group G has a normal subgroup N of bounded index with N uniserially embedded and N of class at most two. Let us analyze what this implies for the case of p odd.

First, replacing N by $\mathcal{U}^1(N)$ is no loss general. For the number generators of any subgroup is at most (p) by Thompson's result and since N is a regular p-group. But, if $x \in \Omega_2(N)$, $y \in N$ then $[x, y^{p^c}] = [x^{p^c}, y] = 1$ so we now have, in addition, that we can assume that $\Omega_2(N)$ is abelian.

Let $t \in G$ with $\langle t, Z(G) \rangle \in \mathcal{E}(G)$ so $\Omega_1(N)$ is a simple Jordan block under the action of t, so $\Omega_2(N)/\Omega_1(N)$ is as well. Let $H/\Omega_1(N)$ be the "socle" and $\Omega_1(N)/K$ the "top". The uniseriality then implies that some element to with the same properties is not trivial on H/K.

$\Omega_2(N)$
H
$\Omega_1(N)$
K
1

Suppose now that s is another element of order p such $\langle s, Z(b)\rangle \in \mathcal{P}(B)$ and that s is trivial on H/K. Hence, if $a \in H - \Omega_1(N)$ then $s^{-1}as = ax$, $x \in K$. Then $x = [b, s]$ for some $b \in \Omega_1(N)$ by the Jordan block structure. Hence

$$s: ab^{-1} \to ax.\ s^{-1}b^{-1}s = ax[b,1]b^{-1} = ab^{-1}$$

so there is an actual fixed point for s in $H - \Omega_1(N)$.

Now what we would like is that there is $c \in \Omega_2(N)$ with $s: c \to cf$, $f = ab^{-1}$ the fixed point of order p^2. For then s^p does not fix c, a contradiction. Then every element like s is not trivial on H/K so has only p fixed points on $\Omega_2(N)$. Thus, such s has no fixed point of order $\geq p^2$ in N so the fixed point set is of order p. This means the conjugacy class of s, which lies in sG' is large, so we get a bound on the number of conjugacy classes like s lying in this coset. Hence, we have the desired bound.

Now if $\Omega_2(N)/\Omega_1(N)$ has order p then by regularity of N we get $N/\Omega_1(N)$ cyclic so either the order of N is bounded or there is a cyclic subgroup of order p^2 of N normal in G, a contradiction. Hence, we may assume otherwise that $\Omega_2(N)/\Omega_1(N)$ has order at least p^2. Let $M/\Omega_1(N)$ be normal in G with $M/\Omega_1(N) \simeq Z_p \times Z_p$, so $M \geq H \geq \Omega_1(N) \geq K$. Hence $M \simeq Z_{p^2} \times Z_{p^2} \times \overbrace{Z_p \cdots Z_p}^{sp-2}$ with s acting by two Jordan blocks $(M/\Omega_1(M),\ \Omega_1(M))$ with a fixed point of order p^2 as above. Does this lead to the elements c, f as above so we will be done?

First note that the number of factors $\mathbb{Z}_p$ in the decomposition of M is at most $p-3$, since $\langle S, H \rangle$ is of maximal class and we can quote Blackburn's structure result.

Before working at this, an aside. Suppose we have $N \triangleleft G$, N abelian but did not have the uniseriality. Could we proceed. The question we just posed would be a typical problem facing us. Albert suggests using a reduction to N primary (a generalization of abelian) that is available by Thompson's theorem (see Dixon et al, p 48, 2.13)

Now back to the remaining point about M and s. It is a little more complicated than stated above. The picture of M is

where the number of factors is at most $p-1$ since $\langle M, t \rangle$ is of maximal class. Then $s^{-1} m s = t m x_1$ where $x_1 \in \Omega_1(M)$. Defining recursively, $x_i . x_{i+1} = s^{-1} x_i s$ we then have

$$m = s^{-p} m s^p$$
$$= t^p m x_1^{(p_1)} x_2^{(p_2)} \cdots x_r^{(p_r)}$$

where $r < p$ so

$$m = s^{-p} m s^p = t^p m$$

and t^{p-1}, which is a contradiction

Would be interesting now to study the case of N abelian and normal of bounded index as a step towards the principal case.

Want to close with some remarks. Let $e(P)$ now be the set of elements x of P such that $\langle x, \Omega_1(Z(P)) \rangle \in \mathcal{E}(P)$.

Lemma Let H be a proper subgroup of P generated by elements of $e(P)$ contained in it. There exists a maximal subgroup M of P containing H which is also generated by the elements of $e(P)$ contained in it.

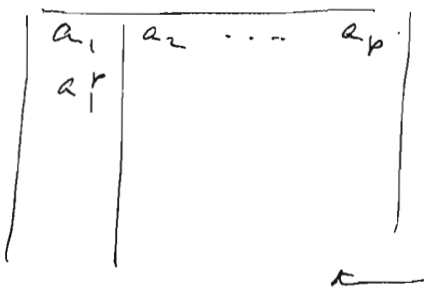
This is easy to see, just generalize the case $H=1$ using the images in $P/\Phi(P)$ of the elements of $e(P)$ which lie in H.

Finally, another look at $Z_{p+2} \supset Z_p = B \cdot \langle t \rangle$. A "basis" for B/B^p will then pull back to a basis of B, using any pull back. Hence, then a basis $a_1, \dots, a_p$ of B with $t^{-1}(a_i)t = a_i a_{i+1}$, $1 \le i \le p$ (and using $a_{p+1} = [a_i, t]$). So what is a_{p+1}? But

$$t^p : a_1 \to a_1 a_2 \to a_1 a_2^2 a_3 \to \dots \to a_1^{\binom{p}{0}} a_2^{\binom{p}{1}} \dots a_{p-1}^{\binom{p}{p-1}} a_p^{\binom{p}{p}} a_{p+1}$$

which must be a_1 so $a_{p+1} = a_2^{-\binom{p}{1}} a_3^{-\binom{p}{2}} \dots a_p^{-\binom{p}{p-1}}$.

Picture



← maximal class "part"

What generates the center? Is the product

$$a_1 \cdot a_1 a_2 \cdot a_1 a_2^2 a_3 \cdots$$
$$= \left(a_1^p a_2^{1+2+\dots+\binom{p-1}{1}} \cdots\right) a_p$$

Power products

We observe a strange identity

Proposition Let x, y, z be elements of the group G with xy and yz in a normal abelian subgroup. If n is a positive integer then

$$(xyz)^n = x^n y^n z^n$$

Proof. In the following lemma set $a = yx$, $b = yz$, $t = y^{-1}$ (and observe that yx and xy are conjugate in G).

Lemma If t is an element of the group G while a, b lie in a normal abelian subgroup of G then $(tab)^n = (ta)^n t^{-n} (tb)^n$ for any $n > 0$.

Proof We have

$$\begin{aligned}
(tab)^n &= tab.\ tab.\ \dots\ .\ tab \\
&= t^n (ab)^{t^{n-1}} (ab)^{t^{n-2}} \cdots (ab)^t ab \\
&= t^n a^{t^{n-1}} a^{t^{n-2}} \cdots a^t a\ b^{t^{n-1}} b^{t^{n-2}} \cdots b^t b \\
&= t^n a^{t^{n-1}} \cdots a.\ t^{-n}.\ t^n b^{t^{n-1}} \cdots b^t b \\
&= (ta)^n t^{-n} (tb)^n
\end{aligned}$$

as desired.

Small centralizers, p>2

Let P be a p-group, $\mathcal{E}(P)$ the set of elements t of P of order p such that $\langle t, \Omega_1(Z(P)) \rangle$ is elementary of order p^2 and in $\mathcal{E}(P)$. We assume $\mathcal{E}(P) \neq \emptyset$, $p > 2$ and want to analyze the structure of P. We also assume that P is generated by the elements of $\mathcal{E}(P)$ though this hardly comes in. The focus is on abelian normal subgroups of exponent p^2, which also play a central role in Carlson's analysis for the case $p = 2$.

Here's a first result which we won't actually need but sets the stage.

Lemma There is a unique largest normal elementary abelian subgroup of P and its order is at most p^p.

Proof. The order restriction follows from letting $t \in \mathcal{E}(P)$, one of the generators, act on the largest such subgroup, since there can be only one Jordan block.

Let E and F be normal and elementary abelian subgroups neither containing the other, say. Choose subgroups E_1 and F_1 of E and F, respectively, with $E \geq E_1 > E \cap F$, $F \geq F_1 > E \cap F$, $|E_1 : E \cap F| = |F_1 : E \cap F| = p$, and E_1, F_1 t-invariant. Then $H = \langle E_1, F_1 \rangle$ is of exponent p and class at most 2 plus $H/E \cap F$ is elementary of order p^2 and centralized by t. If K is of index p in $E \cap F$, normal in H and t-invariant then t must centralize an elementary abelian subgroup of order p^2 of H/K or we get such a quotient on a smaller group. Continue to "go further down" and we get a contradiction.

Lemma Suppose that E is a normal elementary abelian subgroup of order p^k and $\bar{P} = P/E$. If $t \in c(P)$ then $\bar{t} \in c(\bar{P})$. Moreover, if $t_1, t_2 \in c(P)$ and $\bar{t}_1, \bar{t}_2$ are conjugate in $\bar{P}$ then t_1, t_2 are conjugate in P.

Proof. We now have that t acts as an Jordan block on E so let $e_1, \ldots, e_p$ be a basis of E showing that $t^{-1} e_i t = e_i e_{i+1}$ (where $e_{p+1} = 1$). To prove the first statement we have to deal with the situation of a subgroup H containing E, $H/E \cong Z_p \times Z_p$, $t \notin H$, t centralizing H/E; we need to derive a contradiction. It suffices to show that if $x \in H - E$ then there is an element of xE fixed by t, as then $C(t)$ has a section isomorphic with $Z_p \times Z_p \times Z_p$, certainly a contradiction. But $t^x \in \langle t, E \rangle$ so $\langle t^x \rangle$ and $\langle t \rangle$ are complements to E in $\langle E, t \rangle$. Since E is a free module for $\langle t \rangle$ we deduce that there exists $e \in E$ with $t^x = t^e$ so $xe^{-1} \in C(t)$, as we needed.

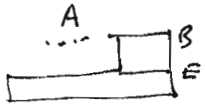
The second statement is quite easy too. We may assume, without loss of generality, that $\bar{t}_1 = \bar{t}_2$. Now the conjugacy of complements applies once again and the lemma is proved.

Now suppose we can get bounds in the case that the largest normal elementary abelian subgroup is of order less than p^r. Then this bound applies in all cases, by induction using this lemma!

Next, let A be maximal subject to being normal, abelian and of exponent p^2 and assume the rank is less than p so that A contains every element of order at most p^2 which centralizes it, by our theorem as p is odd - see hypothesis. Let $E = \Omega_1(A)$. We divide our analysis into three cases according as $A = E$, $|A:E| = p$, $|A:E| \geq p^2$. The first case is trivial as then A must be maximal normal abelian so $|P|$ is bounded by a function of p. The remaining two cases will be treated separately.

First, assume $|A:E| = p$. Let $\hat{A}$ be a maximal normal abelian subgroup of P containing A so $\hat{A} = E \times C$ where C is cyclic and $|E \cap C| = p$. Hence, $t \in e(P)$ centralizes $\mho^2(C)$ so $\mho^1(C) = \mho^1(\hat{A})$ is invariant and t has order p which is odd. Since P is generated by such elements, we have that P centralizes $\mho^2(C)$ so the order of the group of automorphisms induced on $\hat{A}$ by P is bounded. But this is isomorphic with $P/\hat{A}$. (continued next page)

Second, assume $|A:E| > p$ and let $|B:E| = p^2$ where B is normal in P, $B \leq A$. Now E is a proper subgroup of B so B/E is as well, using the pth power map. Hence, there are $b_1, b_2 \in B$ so that $\bar{b}_1, \bar{b}_2$ is a basis of $\bar{B} = B/E$ with $t^{-1}b_1 t = b_1 b_2$. Let $t^{-1}b_2 t = b_2 b_3$ define b_3, which lies in E, and $b_4, b_5 \cdots$ and so on. Then



$$b_1 = t^{-p} b_1 t^p = b_1^{\binom{p}{0}} b_2^{\binom{p}{1}} \cdots b_p^{\binom{p}{p-1}} b_{p+1}^{\binom{p}{p}} = b_1 b_2^p b_{p+1}$$

so $b_{p+1} = b_2^{-p}$ so $b_{p+1} \neq 1$. Hence, $b_3, \ldots, b_{p+1}$ must be a basis of E, in particular, $|E| = p^{p-1}$. Thus, in addition

we have that t acts uniserially on B so $|C(t) \cap B| = p$. But A/E, by the p-th power map, is uniserial for t, so $|C(t) \cap A| = p$. Hence, by our theorem on $C(A)$, in Huppert, $|C(t) \cap C(A)| = p$ so $|P : C(t)|$ is bounded by a function of p only so each coset of $\Phi(P)$ in P can have only a bounded number of classes of elements from $e(P)$. But $|P : \Phi(P)|$ is bounded by Thompson's theorem, see Huppert. Hence, we are done.

Continuation from page 80: Hence there are only finitely many cosets of $\hat{A}$ in P which contain elements of $e(P)$. In any such coset there are only finitely many elements of order p. For if $t \in e(P)$ then t is the unit in a cyclic quotient module a subgroup of bounded order so not many elements of order p.

Small centralizers, $p=2$

Let's turn to the case $p=2$ and see whether, with our inductive idea, we can give a complete classification of the 2-groups G with $E(G)=G$. Assume M is a maximal subgroup, $M=E(M)$ and $t\in G-M$ with $\langle t, S_1 Z(G)\rangle \in \mathcal{E}(G)$.

Lemma 1 If M is a dihedral group then G is either dihedral or isomorphic with the central product $M\circ Z_4$.

Proof. If t induces an inner automorphism then it is easy to see this leads to the second case, otherwise t will not centralize $M/\Phi(M)$ so there is a generating involution s of M such that $M=\langle s, t^{-1}st\rangle$ and G is now dihedral.

Lemma 2 Suppose that M is the central product of a dihedral group and a cyclic group of order four. Then G is of the same structure as the central product of a dihedral group of order eight and the quaternion group of order eight.

Proof. Write $M=D\circ Z_4$, the central product where D is dihedral. Let $t\in G-M$ as above. If t normalizes D then the previous argument readily generalizes. If t does not normalize D then $|D|=8$. Indeed, if $|D|\geq 16$ then exactly two cosets of $\Phi(M)$ in M consist entirely of involutions so we are in the case already dealt with. So assume $|D|=8$, $D=\langle s_1, s_2\rangle$, s_1, s_2 involutions. Let $1\neq z\in Z(G)$ generate $Z(G)$. Then there are just three cosets of $\Phi(M)$ in M consisting of involutions, with representatives $s_1, s_2, s_1 s_2 z$. So t must permute these cosets. Hence, after relabeling, we have that conjugation by t

gives the following (using that t does not normalize D again):

$$t : s_1 \to s_1 z^2 \text{ or } s_1$$
$$z \to z^{\pm 1}$$
$$s_2 \to s_1 s_2 z^{\pm 1}$$

But by hypothesis on t, it can't fix s_1 as it certainly fixes z^2 (and $\langle s_1, z^2 \rangle \simeq Z_2 \times Z_2$). So there are $\epsilon = \pm 1$, $\delta = \pm 1$ with

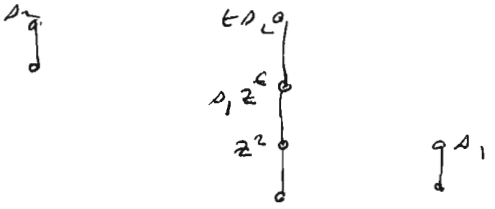
$$t : s_1 \to s_1 z^2, \quad s_2 \to s_1 s_2 z^{\epsilon}, \quad z \to z^{\delta}$$

$\therefore (ts_2)^2 = ts_2 ts_2 = s_1 s_2 z^{\epsilon} s_2 = s_1 z^{\epsilon}$, $(ts_2)^4 = z^2$, $(ts_2)^8 = 1$. Also $t : s_1 \to s_1 z^2$, $s_2 : s_1 \to s_1 z^2$ so ts_2 and s_1 generate a group isomorphic with $Z_2 \times Z_2$. Moreover,

$$(ts_2)^{s_2} = s_2 t = s_2^{-1} t^{-1} = (ts_2)^{-1}$$
$$s_1^{s_2} = s_1 z^2$$

so in the $Z_8 \times Z_2$ we have that s_2 inverts the Z_8 and "skews" the Z_2

The picture:



But then s_2 centralizes $s_1 z^{\epsilon}$. $s_1 = z^{\epsilon}$ and $\langle s_1, z^{\epsilon} \rangle \simeq Z_4$ so we now have that $G \simeq D_{16} \circ Z_4$ a central product as desired.

The case left to analyze, we think: $M \simeq D_8 \circ Q$ where Q is a quaternion or generalized quaternion group, hopefully leading to the same sort of structure for G.

Let's just make some comments on this case as it does not, perhaps, seem to be worth the effort as Carlson has handled the case $p=2$ by direct methods rather than our inductive approach.

First, assume that $M = D \cdot Q$ where $D = \langle s_1, s_2 \rangle$ is dihedral of order eight, $Q = \langle u, c \rangle$ is generalized quaternion of order 2^n, $n \geq 4$ where $u^2 = c^{2^{n-2}} = z$, $c^{2^{n-1}} = 1$, $ucu^{-1} = c^{-1}$ and so on. Then there are just four cosets of $\Phi(M) = \langle c^2 \rangle$ in M which contain involutions, each such coset containing an involution and its product with z. Representatives are

$$s_1, \quad s_2, \quad s_1 s_2 u, \quad s_1 s_2 uc$$

By calculating the orders of the products we get that $t \in C_M(A)$ as above, must stabilize the last coset (i.e. leave each fixed or switch) so the same applies to $s_1 s_2$ so D is invariant and then Q, its centralizer is too.

Next: consider the cases as t is known or not on D, Q.

The last case will be $M = D \cdot Q$, $D = D_4$, $Q = Q_8$, $Q = \langle u_1, u_2 \rangle$ $D = \langle s_1, s_2 \rangle$. The cosets of $\Phi(M) = \langle z \rangle$ containing involutions have representatives

$$s_1, \quad s_2, \quad s_1 s_2 u, \quad s_1 s_2 u_2, \quad s_1 s_2 u_1 u_2$$

and since $\mathrm{Cent}(M)$ is transitive on these four cosets we can assume t leaves $s_1 \langle z \rangle$ fixed. By hypothesis on t we must have it acting non-trivially on $\langle s_1, z \rangle$ so $t s_1 t = s_1 z$.

Much more work needs to be carried out.

Small centralizers revisited

As before, P is a p-group, $t \in \mathcal{C}(P)$, $t \in P - \Phi(P)$, $p > 2$. Let N be a normal subgroup of exponent p.

Proposition 1 If $t \in N$ then N is of maximal class and $|P : C(t)N| \leq p$.

Proof. Since N is of exponent p we have $|C_N(t)| \leq p^2$ so N is of maximal class. Now $t \notin \Phi(N)$ as $t \notin \Phi(P)$ so, by counting, $t^N = tN_2$ (as all conjugates of t in N lie in tN_2 and $|t^N| \geq |tN_2|$. The number of conjugates of $t^N = tN_2$ in G is thus at most p, as it is a power of p, so the stabilizer of t^N is of order at most p. But this stabilizer is $C(t)N$, so we are done.

Henceforth, assume $t \notin N$ (without repeating this).

Proposition 2 $|N| \leq p^p$.

Proof. If this fails then we may assume that $|N| = p^{p+1}$ so $G = \langle t, N \rangle$ is of order p^{p+2} and of maximal class. Then, by 3.3.6 on page 61 of L-M, $S_1(G_2) \neq G_2$ contradicting $G_2 \leq N$.

Proposition 3 If $|N| = p^p$ and N is of maximal class then $C(N)$ is cyclic.

Proof If $E = Z_p \times Z_p \leq C(N)$ then EN is of exponent p and order p^{p+1} violating the previous result in $\langle t, EN \rangle$.

Proposition 4 If $|N| = p^p$ and N is of maximal class then $\bar{t} \in e(\bar{P})$, $\bar{P} = P/N$.

Proof. Let $G = \langle t, N \rangle$ and let $N = N_0 > N_1 > \cdots > N_p = 1$ be the t-invariant normal subgroups of N. (Recall that G is of maximal class; hence $N_1 = G'$). In analogy with the case where N is abelian we have to deal with $m \in P$ with $t^m \equiv t$ modulo N and deduce that t^m is conjugate to t by an element of N. But $t^N \subseteq tN_1$, as $N_1 = G'$, so $t^N = tN_1$ since these two sets have the same cardinality (as $|C_N(t)| = p$). Now m certainly leaves N invariant under conjugation so it permutes the other p maximal subgroups of G. One of them, namely G_1 in Blackburn's notation, is not of maximal class, while $\langle t, N_1 \rangle$ is of maximal class. Hence, m leaves invariant each maximal subgroup of G, so $t^m \in tN_1 = t^N$ and we are done.

Remarks: We are not claiming that if $t_1, t_2 \in e(P)$ with $\bar{t}_1, \bar{t}_2$ conjugate in $\bar{P} = P/N$ then t_1, t_2 are conjugate in P. The analysis above shows each $\bar{t}$ may "contain" up to $p-1$ elements like t, so the counting is under some control. More has to be done. Presumably the normal subgroups of P/N are more restricted or, if not, we get further information on N, perhaps even that it is abelian in the right circumstances.

Let's turn to the case where N is not of maximal class when we have the same situation by an altered argument.

Lemma 1 If G is a p-group of maximal class and order p^{p+1} then G is not of exponent p.

Proof. With the usual notation, let $s \in G$ be in not 2-step centralizer and let $s_1 \in G_1 - G_2$. Hence $[s_1, \overbrace{s, \ldots, s}^{p}]$ is a non-identity element of G_p which forces the exponent to be greater than p.

Proposition 5 If $|N| = p^p$ and N is not of maximal class then $\bar{t} \in c(\bar{P})$, $\bar{P} = P/N$.

Proof. Same notation as in the previous proposition. We are done unless the p maximal subgroups of G, other than N, are isomorphic. But $\langle t, N_1 \rangle$ is one of these and is of exponent p (as is generated by elements of order p and has class less than p. Also N is of exponent p. Thus, if we are not done then G is of exponent p and order p^{p+1}, contradicting the lemma just proved.

Again the situation as to comparing counts in P and $\bar{P}$ is the same as in the previous case. We now turn to normal subgroups of exponent p which have orders strictly smaller than p^p, keeping in mind the abelian case for comparisons.

Lemma 2. Let α be an automorphism of order p of the p group G which has exponent p. If G has a quotient which is elementary abelian of order p^2 and trivial action of α then it has a subgroup which is elementary abelian of order p^2 on which α acts trivially.

Proof By induction on $|G|$. Let $N \lhd G$, $G/N \simeq Z_p \times Z_p$ with trivial action. Let $K \lhd G$, $|N:K| = p$ so G/K is of order p^3 so, by induction there is a subgroup H of G, $G > H > K$, H/K isomorphic with $Z_p \times Z_p$ and α acting trivially. (use homomorphism of G/K to H/K determined by α.) If we are done by induction.

Proposition 6 If $0 < r < p$ then there is at most one normal subgroup of P which is of exponent p and order p^r.

Proof. Suppose that N_1 and N_2 are unequal but satisfy the conditions. Let K_1, K_2 be normal subgroups of N_1, N_2 respectively each containing $N_1 \cap N_2$ as a subgroup of index p. Then $K = \langle K_1, K_2 \rangle$ has order at most p^r, is generated by elements of order p so has exponent p. Furthermore, it is trivial on $K_i/N_1 \cap N_2$ so is on $K/N_1 \cap N_2$ so the lemma applies and we have a contradiction.

Now let N be as above but of maximal order, say p^r. Let us analyze the case where $r < p-1$. (We have studied the case $r = p$, so we are leaving aside $r = p-1$ for now. The technique is a bit more general and we shall apply it to the one remaining case $r = p-1$.)

Let K be a normal subgroup of P containing N and not containing t with $K/N \cong Z_p \times Z_p$. Hence $|K| \leq p^p$ so it is regular so K/N as a module for $\langle t \rangle$ is isomorphic with $Z^1(K) \leq N$ of order p^2 so K/N is a single Jordan block of dimension two. Now $\langle t, K \rangle$ cannot be of maximal class, by 3.3.2 of L-M, since then $\langle t, K \rangle_2$ would properly contain N and not be of exponent p. Hence, there is $f \in C(t)$, $f \in K - N$. Hence if $b \in K$, not fixed modulo N by t then $b^t \equiv bf$ modulo N, where we replace t by a power if needed, keeping $t \notin N$. Then $b^t = y b f$, $y \in N$. Then $b t^2 = y^t . y b f . f = y^t y b f^2$ and, continuing in this way,

$$\begin{aligned} b = b^{t^p} &= y^{t^{p-1}} y^{t^{p-2}} \cdots y^t y . b . f^p \\ &= t^{-p} (ty)^p . b . f^p \\ &= b . f^p \end{aligned}$$

so $f^p = 1$, a contradiction, using $n < p-1$, to see that $\langle t, N \rangle$ is of exponent p. So there is no such subgroup K at all.

Let $L \lhd P$, $|P : L| = p$, $t \notin L$, $L \geq N$. Hence there is no "K" as above contained in L, in particular. Looking at a subgroup of L normal subject to containing N, with L/N not cyclic we get a contradiction (using the subgroup of elements of order p).

Proposition 7 Suppose N is maximal among normal subgroups of exponent p not containing t. Suppose further that $|N| < p^{p-1}$. Then there is a normal subgroup L of P of

index p not containing t such that L/N is cyclic.

This summarizes what we just have proved.

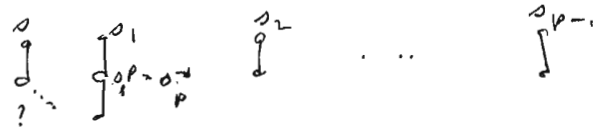
Now let N be normal of exponent p as above with $|N| = p^{p+1}$ and not such subgroup of order p^p. Again assume that $K \lhd P$, $K \geq N$, $K/N \simeq Z_p \times Z_p$, $t \notin K$. We must consider the case that t is trivial on K/N or not trivial and in the latter case whether $\langle K, t \rangle$ is of maximal class or is not. Now, the maximal class case exists so we are left with the remaining two cases to be analyzed. First, consider the case with non-trivial action on K/N and $\langle K, t \rangle$ not of maximal class. The above argument we had for $n \leq p+1$ carries over. This leaves one situation to be analyzed: t trivial on K/N. (Note: by the maximal class case we mean $|C_K(t)| > p$.)

In the case of trivial action on K if K has class less than p then we can proceed just as above since then K is regular. So assume K has class p so it is of maximal class being of order p^{p+1}. This case definitely seems to exist. Suppose that K has degree of commutativity 0 so there are two 2-step centralizers. Hence P induces the identity only on K/N and all the maximal subgroups of K are normal in P, so, as a result, all elements of $K-N$ are of order p. Assume the degree is positive so K_1 (usual notation) is the common 2-step centralizer. Then, either all elements of $K-N$ are, again, of order p or the p maximal subgroups of K, other than K_1, are all conjugate by an automorphism given by conjugation in P, in which case all

the elements of $K - K_1$ have the same order.

Let's give an example of this. Set $G = \langle s, s_1, \dots s_{p-1}, \delta_p \rangle$ where $\langle s_1, \dots s_{p-1} \rangle$ is normal abelian, $s_p = s_1^{-p}$, $s^{-1} s_i s = s_i s_{i+1}$. $s_2, \dots, s_{p-1}$ have order p, s_p has order p, s_1 has order p^2, s has order p or p^2.

Picture:



So $s^p = 1$ or $s^p = s_p$ say. Have to satisfy by conjugation by s, another automorphism sends s to ss_1 and so on. Easy and standard calculations apply. (Can use results on page 71 now).

What should come next? Analysis of M when M/N is maximal normal of exponent p in P/N is a good guess. Keep track of $c(t)$!

Let's do one case.

Proposition 8 Suppose N is normal of exponent p and order p^p and that M/N is normal of exponent p and order p^p. It follows that N is abelian, if $p > 3$.

We need a preliminary result:

Lemma 3. Suppose that Q is a normal subgroup of the p-group P that Q and P/Q are of exponent p and $|Q| \leq p^p$. Then $[U_1(P), Q] = 1$

Proof. It suffices to prove that $[x^p, y] = 1$ whenever $x \in P$, $y \in Q$

But (see Dixon et al, 2nd edition, p 274)

$$[X^p, y] \equiv [X, y]^p \bmod \gamma_2(\langle X, [X,y]\rangle)^p \gamma_p(\langle X, [X,y]\rangle)$$

But $\gamma_2(-) \subseteq Q$ a group of exponent p so the first factor is the identity. Next, look at a central series for P running from Q to 1 which therefore takes at most p steps. Call such a series $Q = Q_1 \geq Q_2 \geq \cdots 1$. Hence $[X, [X,y]] \in Q_3$ as $[X,y] \in Q_2$ so $\gamma_p(\langle X, [X,y]\rangle) = 1$ and we are done.

Proof (of Proposition) Let now $G = \langle t, M\rangle$. Consider G_2 so $G_2 N/N$ is of order p^{p-1} and $G_2 \geq [N,t]$ which is of order p in N. Hence, there are two possibilities: $G_2 \geq N$ and $|G_2| = p^{2p-1}$, $G_2 \cap N = [N,t]$ and $|G_2| = p^{2p-2}$.

Consider the first case. Let $\bar{G} = G/N$ so $|\bar{G}_2 / \bar{G}_3| = p$ so $[\bar{G}_2, \bar{G}_2] = [\bar{G}_2, \bar{G}_3]$ is of order p^3 at least in $\bar{G}_2$ as $p \geq 5$. Hence $|[G_2, G_2]| \leq p^{2p-4}$. Hence $|[G_2, G_2, G_2]| \leq p^{2p-6}$ (as get two 2_p's cancelled as G as normal and G_2 is normal of action) so $[\overbrace{G_2, \ldots G_2}^{p}] = 1$ and G_2 is, in particular, regular. Thus $N = \Omega_1(G_2)$, so $|\mathcal{U}^1(G_2)| = p^{p-1}$ so, by the lemma, N has a central subgroup of order p, and so is abelian.

Consider the second case. There we have $|[G_2, G_2]| \leq p^{2p-4}$ and so on and again G_2 is regular, but, this is even more work as then $\Omega_1(G_2)$ will be of order p^{p-1} and p^p of it possibly contains $N \cap G_2$. So we must be more careful!

Hence, set $H = NC_2$ so $|H| = p^{2p-1}$ as in the previous case. But we need a different argument. We still want $H_p = 1$ as then we can proceed as in the previous case using H and $\mathcal{V}^1(H)$. We need to prove that

$$[\underbrace{N, N, \dots, N}_{a}, \underbrace{C_2, \dots, C_2}_{p-a}] = 1$$

where $0 \le a \le p$. But if there are two or more N's, $1 \le a \ge 2$ then $|[N,N]| \le p^{p-2}$ and the remaining terms suffice. If there are no N's then $|C_2| = p^{2p-2}$ so $|[C_2, C_2]| \le p^{2p-4}$ as in the previous case so we are alright. Finally, assume there is just one N. But $|N : [N, C_2]| \le p^2$ and so on.

Proposition 9. With the above notation, assume $p > 3$ and M/N is abelian. Then $N = \mathcal{V}^1 M$,

Rk: In particular, M is powerful.

Proof. Keep the above notation, $G = \langle t, M \rangle$. Let H be the subgroup of index p in M either C_2 or $C_2 N$ so H is regular and $\mathcal{V}^1 H$ is of order p^{p-1} and normal in G so must equal $[N, G]$ the one subgroup with these two properties. But M centralizes $H/N = H/\mathcal{R}_1 H$ so it centralizes $\mathcal{V}^1 H = [N, G]$. But $M_2 \le N$, so M/N is abelian, so $M_3 \le [N, G]$ and thus $M_4 = [M, G] \le [[N, G], M] = 1$ and M is regular. Hence, the claim follows.

We close this section with some remarks on the "top down" inductive approach. Recall the situation when H is of maximal class and index p in G, $H = \langle t, H_1 \rangle$ with the usual notation so H_1 is the first two step centralizer so t is of order p, $|C_{H_1}(t)| = p$. Say $s \in c(G)$, $s \in G - H$ so $t^s = t^k$ for some $k \in H$ and $sk^{-1} \in c(t)$ so sk^{-1} is order p^2 so $k \in H - H_1$ or else s and sk would be conjugate. This situation can occur when $G = H\langle w \rangle$, $w \in Z(G)$ of order p^2, $w^p \in Z(H)$, a central product, when $s = tkw$, $k \in H$ when sk is of order p^2 and s has order p.

Can this continue, with $G < X$ of index p, $X = \langle G, u \rangle$ as you might expect? What about $s^u = t = s \cdot s^{-1}t$? Seems hard to rule out.

We want to point out that, in the above situation with $H < G$, we must have $|H| > p^p$. For suppose that $|H| \leq p^p$. Now H_2 is of exponent p (see L-M) because of the order. If $k \in H_1$ then $(tk)^p = k^p$ by collection, as $t^p = 1$. Since H is generated by t and another element $tk \in c(G)$, $k \in H_1 - H_2$, then as $k \in H_1 - H_2$ of order p so H_1 is of exponent p, being of class less than p. Then $sk^{-1} \in \langle s, H_1 \rangle$ which is then also of exponent p, by generators and order, contradicting that sk^{-1} has order bigger than p.

Suppose that there's no normal subgroup of exponent p and order p^p but N is such of order p^{p-1}. Want to investigate what can go on top of N. Idea: we can build "layers" of order p^{p-1} which "avoid" $C(t)$ except for $C(t) \cap N$ so we sort of have a "maximal class" notion. Presumably, the index of the biggest of these is bounded by a function of p. So we would have, in the general case, a structure made up of three pieces, the "p^p layers", the "p^{p-1} layers" and a finite part.

So we let M/N be a maximal normal subgroup of exponent p and study its structure. Presumably the ideas will generalize to further layers on top. We only provide sketches of our ideas. Since $C_N(t)$ is of order p we have $C_{M/N}(t)$ of order at most p^2 there being at most one "real" fixed point coming from $C_N(t)$ and one "fake", a new, fixed point. First, suppose $|C_{M/N}(t)| = p$. If eN is a "real" fixed point then $|M/N| = p$ by previous argument (no "block" of size greater than "one-dimensional"). The fake case means $\langle t, M \rangle$ is of maximal class so $|M/N| \leq p^{p-1}$ as usual. So all is O.K. in the case $C_{M/N}(t)$ has order p.

Let $e, f \in M$ with $\langle fN \rangle$ a "real" fixed point of t and $\langle eN \rangle$ a "fake" one so $C_{M/N}(t) = \langle eN, fN \rangle$ is elementary of order p^2 (must have a central element of M/N in it). Choose H/N maximal in M/N being t-invariant and intersecting $\langle fN \rangle$ in 1, so, with change of notation, $C_{H/N}(t) = \langle eN \rangle$. Want: M/N is the direct product of H/N and $\langle fN \rangle$.

Indeed, let $F = \langle f N \rangle$ and suppose we have this decomposition. We would also like H normal in G (or replace H if necessary) as then H/N is the desired "layer" on top of N. But if H is not normal in G then there is $g \in G$ which maps H to H^* a "diagonal" subgroup corresponding to a homomorphism of H/N to F/N. This must be obtained by an element s, "like t," as these generate G. But then we have a "2-dimensional" stack for s on top of N. So need that $F - N$ contains a fixed point for s.

So there are issues to resolve. Also need $HF = M$ which looks doable by usual Jordan form arguments.

Small centralizers, $p=2$, cont'd

Our goal is to establish the following result?

Theorem? If G is a 2-groups generated by the subgroups belonging to $\mathcal{E}(G)$ then G is one of the following:

1. Dihedral
2. Central product of a dihedral group and a cyclic group of order four
3. Central product of a dihedral group of order eight and a quaternion or generalized quaternion group.

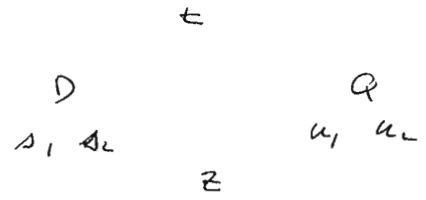
We shall use an inductive approach so assume M is a normal subgroup of G generated by the subgroups in $\mathcal{E}(G)$ which lie in M. We assume M is one of the three types and must prove that G is also one of the three types. If M is one of the first two types then we have dealt with that case in Lemmas 1 and 2 on page 42. Hence, we assume M is of type 3 and now subdivide according to the quaternion or generalized quaternion cases.

We start with the "easier" case where there is a generalized quaternion group of order at least sixteen. We have $M = D \circ Q$ as on page 84, $D = \langle S_1, S_2 \rangle$, $Q = \langle u, C \rangle$. As there, we have four cosets of $\Phi(M) = \langle C^2 \rangle$ containing involutions, two or more in each coset, with representatives $S_1, S_2, S_1 S_2 u, S_1 S_2 uC$ where t normalizes $D = \langle S_1, S_2 \rangle$ so Q is as well, its centralizer.

First, suppose that t induces an inner automorphism on D. Since $C_D(t)$ contains no Fours subgroup, we may assume, after relabeling if needed, that t and $s_1 s_2$ induce the same automorphism of D so $ts_1s_2 \in C(D)$. But $(ts_1s_2)^2$ is a non-identity element of $Z(D)$, by calculation, there is this cyclic group of order four centralizing s_1. But Q contains another so there is a Four group, not containing s_1, which centralizes it. The "parity" of involutions in M forces $\langle s_1, Z(D)\rangle \in \mathcal{E}(G)$ so we have a contradiction

Second, suppose that t induces an outer automorphism, so without loss of generality, t "switches" s_1 and s_2. Hence, if t should invert an element v in Q of order 4 so $tvt = vz$, $ts_1s_2t = s_1s_2z$, we would have t centralizing the involution s_1s_2v as well as z, a contradiction. So how does t act on Q then? But t leaves Q invariant, as it leaves D invariant, as we said above. Let v_1 be an element of order 4 in Q. If t normalizes $\langle v_1\rangle$ then it must centralize it. Suppose otherwise so $v_2 = tv_1t$ generates a different cyclic group of order 4. Hence, $\langle v_1, v_2\rangle$ generates a quaternion or Fourier quaternion group. In the first case, t normalizes $\langle v_1 v_2\rangle$, a contradiction. In the second, it normalizes $\langle [v_1, v_2]\rangle$ which has order at least four. Hence, t centralizes Q so we seem to have to extend the answers in the statement of the supposed result to include $D \cdot Q$, D extended of arbitrary order.

So this leaves the last case $M = D_8 \circ Q_8$ as on page 84, at the bottom. We continue using the same notation and information. The picture:



Involutions: $s_1, s_2, s_1s_2u_1, s_1s_2u_2, s_1s_2u_1u_2$ + conjugates. Since t permutes the pair classes of involutions and t has order 2 there is a subset of 2 left invariant. Hence, after relabeling we can assume D is t-invariant so Q, its centralizer, is as well. We now have to consider whether t acts on D by an inner automorphism or by an outer automorphism.

In the inner case, we must have $t: s_1 \to s_1 z$, $s_2 \to s_2 z$ or we have a contradiction, so t agrees with s_1s_2 on D. Since s_1s_2 is fixed by t and has order four there is no cyclic subgroup of order four in Q on which t acts trivially. But t acts on Q so it must leave a subgroup of index two invariant, so now, after relabeling, we may assume $t: u_1 \to u_1 z = u_1^{-1}$. If $u_2 \to u_2 z$ then $u_1u_2 \to u_1u_2$, a contradiction so $u_2 \to \begin{cases} u_1u_2 \\ u_1u_2z \end{cases}$. Relabel u_1 if needed so $t: u_2 \to u_1u_2$, $u_1 \to u_1z$. Let $\tau = s_1s_2t$ so this centralizes D and has some action on Q, $\tau^2 = z$ as $\tau^2 = s_1s_2ts_1s_2t = (s_1s_2)^2 z$. What is $\langle Q, \tau \rangle$? We have

$$(\tau u_2)^2 = \tau u_2 \tau u_2 = \tau^2 \cdot \tau^{-1} u_2 \tau \cdot u_2 = \tau u_1 u_2 u_2 = u_1$$

so τu_2 is of order eight. Furthermore,

$$\tau^{-1}(\tau u_2)\tau = u_2 \tau = \tau(\tau^{-1} u_2 \tau) = \tau u_1 u_2$$

$$= \tau u_2 \cdot u_1 \tau = \tau u_2 (\tau u_2)^{-2} = (\tau u_2)^{-1}$$

so $\langle \tau, Q \rangle$ is generalized quaternion and the "inner" case is complete.

Now assume that t acts as an outer automorphism of D so, without loss of generality, t "switches" s_1, s_2. But we have faced this before. t inverts $s_1 s_2$ so there can be no cyclic subgroup of order power in Q inverted by t or else t centralizes Q and get $G = D_{16} \circ Q_8$.

What is left to do now, in fact, is to handle $M = D \circ Q$ when D is dihedral of order at least sixteen and Q is either quaternion or generalized quaternion. First, suppose that Q is of order 8. Let r be an element of order 4 in D, $D = \langle s_1, s_2 \rangle$ as usual, $Q = \langle u_1, u_2 \rangle$ and u_3 as before. Hence, representatives of the classes of involutions of M outside $\Phi(M)$ are given by $s_1, s_2, r u_1, r u_2, r u_3$. By counting the numbers in each class we get that t must stabilize D so it also stabilizes Q the centralizer of D. If t induces an outer automorphism of D then it is non-trivial on $D/\Phi(D)$ so, without loss of generality t "switches" s_1 and s_2. If t induces an inner automorphism then it must be non-trivial on all power subgroups so, again relabeling, t acts the same as r on D.

First, suppose that t switches s_1 and s_2 so inverts $s_1 s_2$ and, consequently, inverts r. Hence, t inverts no element of order four in Q so, as before, is the identity on Q so $G = \langle D, t \rangle \circ Q$, $\langle D, t \rangle$ a nilpotent group.

Second, suppose that t acts by conjugation by r on D so $\tau = tr^{-1}$ centralizes D. Now $\tau^2 = tr^{-1}tr^{-1} = r^{-2} = z$. (For t acts by conjugation by r so fixes R.) Now the argument on the bottom of page 99 and top of 100 applies here so $G = D \circ \hat{Q}$, $\hat{Q}$ generalized quaternion of order 16.

Finally, assume $M = D \circ Q$, where D is dihedral of order at least sixteen, Q is generalized quaternion (of order at least sixteen). Notation as usual, $D = \langle s_1, s_2 \rangle$, $Q = \langle u, c \rangle$. Representatives of the classes of involutions outside $\mathfrak{F}(M)$ being s_1, s_2, ru, ruc, where r is an element of order four in D. Now $C_M(s_1) \geq Q$ so $C_M(s_1) = C_D(s_1)Q = \langle s_1, z \rangle Q = \langle s_1 \rangle \times Q$. And $C_M(ru)$ contains $C_D(ru)\, C_Q(ru)$ of order at least two (since DQ is a homomorphic image of $D \times Q$ and centralizers never get bigger in homomorphic images). But $C_D(ru) = C_D(r) = \langle s_1 s_2 \rangle$, $C_Q(ru) = C_Q(u) = \langle u \rangle$. Let v be an element of order four in Q which inverts u so then $s_1 v$ inverts ru, i.e. centralizes it. Hence $C_M(ru) = \langle s_1 v, \langle s_1 s_2 \rangle, \langle u \rangle \rangle$. But $\langle s_1 v, w \rangle = \langle s_1 v \rangle \times \langle ru \rangle$ since $u^2 = r^2 = z$, a direct product of a cyclic group and a group of order two. Now $s_1 v$ inverts $s_1 s_2$ while it centralizes ru, as it inverts r and u as above, so $C_M(ru) \cong D \times Z_2$. By the Kurosh–Schmidt theorem, t centralizes the two classes

in D and the two classes in Q. Hence, t normalizes D and so also normalizes Q. Again we are now reduced to two cases, as t induces an inner automorphism on D or an outer automorphism on D.

If t is outer then we may assume, as before, that t switches s_1 and s_2 so $\langle D, t\rangle$ is dihedral. Again, t cannot invert any element of order four in Q. Say u is an element of order four and $t^{-1}vt = tvt \neq u$ so it is not u^{-1} so $\langle u, v\rangle$ is a quaternion group or generalized quaternion so t inverts uv (as $vu.uv = v^2u v = z^2 = 1$) and we are done, as $G \cong \langle D, t\rangle$ Q.

Hence, t is inner, so, since it is non-trivial on each four subgroup, we can assume, without loss of generality that the automorphism induced by t coincides with the inner automorphism given by r, in particular, t fixes r. We shall now take up an argument on the bottom of page 99 which continues on page 100. The idea is that $\tau = r^{-1}t$ centralizes D so $G \cong D \circ \langle \tau, Q\rangle$.

So how does τ act on Q? And remember that $\tau^2 = z$ as well. Since τ centralizes Q/C, $C = \langle c\rangle$ the maximal subgroup of Q which is cyclic, $\tau: u_i \to u_i c^e$ where $e \in C$ and $\tau: c \to c^{-1}$ or $c^{-1}z$, where c is a generator of C, as τ induces an involutory automorphism of order two not trivial on $\Omega_2(C) \cong Z_4$. For since τ centralizes $\langle r\rangle$ we would otherwise get t acting trivially on a four subgroup.

But $\tau^{-1}u\tau = uc^e$ implies $e \in U^1(C)$; in other G has a quotient isomorphic with Σ_2^5 (coming from t, s_1, s_2, u, c) which can't be when the normal 2-rank is two. Hence

$\tau : u \to uc$, c a generator of C, so without loss of generality, $\tau^{-1} u \tau = uc$. Then

$$\tau^2 : u \to uc \to \begin{cases} uc \cdot c^{-1} \\ uc \cdot c^{-1} z \end{cases} = \begin{cases} u \\ uz \end{cases}$$

so we are in the first case when τ inverts C. Now calculate

$$(\tau u)^2 = \tau u \tau u = \tau^2 (\tau^{-1} u \tau) u = z uc u$$

$$= z u^2 u^{-1} c u = z^2 c^{-1} = c^{-1}$$

so τu has twice the order of c. Moreover,

$$u^{-1} (\tau u) u = z u \tau z = u \tau = \tau \cdot \tau^{-1} u \tau = \tau u c$$

$$= \tau u (\tau u)^{-2} = (\tau u)^{-1}$$

so $\langle \tau, Q \rangle$ is a generalized quaternion group.

We have the

<u>Theorem</u> If G is a 2-group generated by the subgroups belonging to $\mathcal{E}(G)$ then G is dihedral or the central product of a dihedral group and a cyclic group of order four, a quaternion group or a generalized quaternion group.

We turn to consequences, just one and we don't carry out the full argument, perhaps should do so in a paper. Let G be a 2-group, t a "good" involution, so $t \notin \Phi(G)$, $\langle t, Z(t)\rangle$ is a proper subgroup and maximal elementary abelian. Let $K = \langle t^G\rangle$ so now our theorem applies. But moreover, we have that K is generated by classes of good involutions, the number of these is a power of 2 and these classes are all conjugate under a 2-group of automorphisms. For example, $K \simeq D_8 \circ Z_4$ is out as the number of good involution (classes, that is) is three and the group is a 3-generator group. $K \simeq D_8 \circ Q_8$ is OK since there are four classes and four of them generate. So we can make a list of possible structures for K. Then $|G : K C_G(t)|$ is the power of two which is the number of classes that t^G breaks up in K, so it is 1, 2, or 4. $C_G(t)$ is also cyclic, quaternion or generalized quaternion.