Research Notes

Volume XIII

Contents

Commutators

Theorem 1 If K is a conjugacy class of a finite group G then the number of pairs (x,y) of elements of G with $[x,y] \in K$ is divisible by $|G|$.

Remark: If $K = \{1\}$ then the number is $= |G|$, the class number as is well-known. A way to restate the result is that the probability that a commutator lies in K is an integer divided by $|G|$, as there are $|G|^2$ pairs of elements.

Proof. Enough to show that if $g \in G$ then the number of commutators equal to g is divisible by $|C_G(g)|$. Hence, for each $y \in G$ it suffices to prove that the number of $x \in G$ with $[x,y] = g$ is divisible by $|C(g) \cap C(y)|$: for y lies in an orbit of size $|C(g) : C(g) \cap C(y)|$ under conjugation by $C(g)$ and each element of the orbit is the second term of a commutator giving g in the same number of ways. But $C(y) \cap C(g)$ acts on all pairs (x,y) with $[x,y] = g$ by $c \in C(y) \cap C(g)$ sending (x,y) to (xc,y) as $(xc,y) = [x,y]^c [c,y] = g^c \cdot 1 = g$. This orbit is regular of course, so we are done.

This integral numerator has a character-theoretic interpretation as well.

Theorem 2 The probability that a commutator of G lies in K is

$$\sum_{\omega} \omega(K) / |G|$$

where ω runs over the central characters.

Proof. If $g \in K$ then the number of ways S is a commutator is $|G| \sum_\chi \frac{\chi(S)}{\chi(1)}$ so the number of ways a commutator lies in K is

$$|G : C(S)| \cdot |G| \cdot \sum_\chi \frac{\chi(S)}{\chi(1)}$$

so the probability is as is divided by $|G|^2$, which is

$$1/|C(S)| \sum_\chi \frac{\chi(g)}{\chi(1)}$$

which is

$$1/|G| \sum_\chi \frac{|G : C(S)|\, \chi(S)}{\chi(1)}$$

as claimed.

How to calculate these probabilities? There is the character and combinatorial approach found in Stanley for the case of n-cycles in Σ_n, but are there direct methods? In general, if $g = x^{-1} y x y^{-1}$, i.e. $Sy = y^x$ so we are looking at "translates" by S which stay in the same conjugacy class. In Σ_n this may be a method?

An identity connected with commutators

K. Anderson has used the Zeilberger "A = B" machine to prove the identity on alternating sums of reciprocals of binomial coefficients that arises in computing the "j" function for symmetric groups. Here is the information:

Let $F(n,k) = (-1)^n / \binom{n}{k}$, $0 \le k \le n$. Miracle:

Let $G(n,k) = \dfrac{(-1)^{k+1} \cdot k! \cdot (n+1-k)!}{(n+2)\ n!}$, $0 \le k \le n+1$.

Then $G(n,k+1) - G(n,k) = F(n,k)$ (check directly) so

$$\sum_{k>0}^{n} F(n,k) = G(n,n+1) - G(n,0) = \frac{((-1)^n + 1) \cdot n+1}{n+2}$$

Cropped rings

We are interested in submatrices of decomposition matrices and how they arise as decomposition matrices for rings "cropped" from the original one. We have the usual modular set-up: K, R, F.

Hypothesis A is an algebra over R (i.e. finitely generated and free over R) with $A_K = K \otimes_R A$ split semisimple and with $A_F = F \otimes_R A$ split semisimple modulo its radical.

This condition guarantees that the usual facts about decomposition matrices and Cartan matrices hold for such algebras, not just group algebras. Suppose now that A is as stated, that D is its decomposition matrix and E is a submatrix of D which has no row or column of zeros. Let e be the central idempotent of A_K corresponding with the rows of E (so e is the sum of the primitive central idempotents of the simple A_K-modules for the rows of E) and let f be an idempotent of A so that Af is a direct sum of indecomposable projective modules which cover the simple A_F-modules belonging with the columns of E, all of them and no others.

Proposition The ring eAf satisfies the hypothesis and has decomposition matrix E.

This breaks down into two steps. Let E_R be

the submatrix of D corresponding with the rows of E and all the columns of D and let E_C be similarly defined for columns. The two steps are as follows (the first is simple and known):

Lemma 1. The ring eA satisfies the hypothesis and has decomposition matrix E_R.

Lemma 2. The ring fAf satisfies the hypothesis and has decomposition matrix E_C.

The proposition follows by applying Lemma 2 to eA using the idempotent ef (as $ef(eA)ef = efAf$). Let's turn to the proofs of these lemmas. We start with Lemma 1. Since Ae is a direct summand of A it is also a free module over R. Now Ae tensored with K is isomorphic with a direct summand of A_K so is split semisimple. The linear transformations induced by A and Ae on Ae are the same so any simple subquotient of Ae as an A-module is the same as an Ae-module so has the same endomorphism ring. In particular, $F \otimes Ae$ modulo its radical is split semisimple.

We turn to the decomposition numbers. Let X be a simple A_K-module corresponding with a row of E. Let S be a simple A_F-module and let f be a primitive idempotent of A so that the indecomposable projective module Af is a cover of S. The decomposition number d belonging to the row of X and column of S

is the multiplicity of X as a summand of $K \otimes_R Af$. (This is where the hypothesis is used.) We want to compare this calculation with the number one for the algebra eA.

The idempotent ef is either a primitive idempotent of eA or it is zero. For the endomorphism ring of $(eA)ef$ is anti-isomorphic with $ef(eA)ef = efAf$ which is an epimorphic image of fAf which, in turn, is local. We are interested in $A_K e.\ Af$ which is thus zero if $ef = 0$ and $(A_K e)f$ otherwise, which is just the direct sum of the correct number of copies of the simple modules corresponding with $A_K e$. If $ef = 0$ then $ef' = 0$ for any conjugate f' of f and if $ef \neq 0$ then $ef' \neq 0$. If we express 1 as a sum of orthogonal primitive idempotents then the multiplication by e gives rise a sum for the identity element e of eA so we have the central idempotents and primitive idempotents at hand ready to be studied with Lemma 2.

We now turn to the proof of Lemma 2. First, let's verify that fAf satisfies the hypothesis. Indeed, fAf is a summand of A as R-module so is a finitely generated free R-module. Moreover, $K \otimes fAf \simeq fA_K f$ so this is just a direct sum of matrix algebras over K since A_K has this structure and f is an idempotent. It remains to deal with the structure of $fAf/\mathrm{rad}(fAf)$.

If $f = f_1 + \dots + f_n$ is an orthogonal sum of primitive idempotents of A then it is the same in fAf (since $f_i = f f_i f$). Hence, we need to study the endomorphism ring of the fAf-module $(fAf)f_i$ and compare it with the endomorphism ring of the A-module Af_i. They are, respectively, anti-isomorphic with $f_i fAf f_i = f_i A f_i$ and $f_i A f_i$. Hence, they have the same radical quotient which we already have, by the hypothesis, is F for the second of these. Thus, fAf satisfies the hypothesis.

Next, we claim the A-modules Af_i and Af_j are isomorphic if, and only if, the fAf-modules $fAf f_i$ and $fAf f_j$ are isomorphic. The identity endomorphism are given by right multiplication by f_i and f_j for both maps. The homomorphisms of the A-module Af_i to the A-module f_j are given by the right multiplications by $f_i A f_j$ and the homomorphisms of the fAf-module $fAf f_i$ to the fAf-module $fAf f_j$ are given by the right multiplication by $f_i fAf f_j = f_i A f_j$. Hence, the A-modules Af_i and Af_j are isomorphic if, and only if, the fAf-modules $fAf f_i$ and $fAf f_j$ are isomorphic. Thus, the simple modules over F for fAf correspond naturally with the selected columns of D in the statement of the lemma. It remains to deal with multiplicities of simple modules over K, a comparison.

Since f is an idempotent, the algebra fA_Kf ($\simeq K \otimes_R fAf$) is a direct sum of matrix subalgebras of the matrix summands of fA_Kf. Hence, the simple modules for fA_Kf are just the non-zero products of f and the simple A-modules. Let E be a primitive central idempotent of A so EA is one of the matrix summands of A. Let S be a simple EA-module. We wish to decompose

$$EA_Kf_1 \simeq \oplus S$$

$$E(fA_Kf)f_1 \simeq \oplus fS$$

and show that the two multiplicities agree. Suppose that Ef_1 is an idempotent of rank r so we can picture

$$Ef_1 = \begin{pmatrix} \overbrace{1 \;\; \cdots \;\; 1}^{r} & \\ & \ddots \\ & 1 \end{pmatrix}^{r}$$

with all other entries zero. Suppose Ef has rank s, so $s \geq r$ and we can picture

$$Ef = \begin{pmatrix} \overbrace{1 \;\; \cdots \;\; 1}^{s} & \\ & \ddots \\ & 1 \end{pmatrix}^{s}$$

Then EA_Kf_1 consists of matrices whose entries outside the first r columns are zero, so, the multiplicity is r in the first case. Also $E(fA_Kf)f_1$ consists of the matrices that are zero outside the $s \times r$ block in the upper left corner, so the second decomposition gives r columns truncated to the first s entries, such columns isomorphic with fS, so we are done.

Finally, we come to the main result which is an immediate consequence of the Proposition.

Theorem. Let A be an algebra over R satisfying the Hypothesis. Let E be a matrix, with no row or column of zeros, of the decomposition matrix D of A. Then is a canonical Morita equivalence class of algebras over R which satisfy the Hypothesis and have E as their decomposition matrix.

The various algebras eAf are Morita equivalent as is well known (write this as $f(eA)f$ which is the endomorphism ring of a projective module with certain indecomposable summands determined.). It remains to see that if B is a ring Morita equivalent to A (and apply this to eAf) then B satisfies the Hypothesis and has the same decomposition matrix as A. Hence, B is isomorphic with the endomorphism ring of a projective A module so B is an algebra over R. Given a Morita context (the two bimodules) between A and B (two modules projective on each side in particular) we then have Morita contexts between $A_{\mathfrak{p}}$ and $B_{\mathfrak{p}}$, and $A_{\mathfrak{p}}$ and $B_{\mathfrak{p}}$ so all is clear.

Decomposition numbers and the Navarro correspondence

We have the usual p-modular system K, R, F and finite group G.

Theorem If G is p-solvable with a self-normalizing Sylow p-subgroup then the entries in the first column of the decomposition matrix of G in the rows indexed by irreducible characters of degree prime to p are all "1."

Proof Let H be a p-complement so the permutation module $R[G/H]$ has dimension p^n, where $|G|_p = p^n$ and is projective as H has order prime to p. Therefore, this module is the indecomposable projective RG-module corresponding with the trivial FG-module F. We shall prove that the inner product of an irreducible character of degree prime to p with the character of $K[G/H]$ is always equal to 1, establishing the theorem.

We shall use the Navarro correspondence. If λ is a linear character of a Sylow p-subgroup P then $\lambda^G = \chi_\lambda + \dots$ where χ_λ is an irreducible character of degree prime to p and the dots represent a sum of characters of degree divisible by p, and $\lambda \to \chi_\lambda$ sets up a one-to-one correspondence between linear characters of P and irreducible characters of degree not divisible by p. Let π be the character of $K[G/H]$ so $(\lambda^G, \pi)_G = ((\lambda^G)_H, 1_H)_H = (\rho_H, 1_H) = 1$, where ρ_H is the regular character of H, by Mackey's theorem since $G = PH$, $P \cap H = 1$. Hence, it suffices to prove that

$(\chi_\lambda, \pi) \neq 0$, i.e. $((\chi_\lambda)_H, 1_H) \neq 0$.

This we shall now do by induction. If $O_{p'}(G) \neq 1$ then all the χ_λ, as above, are characters of $G/O_{p'}(G)$ (e.g. apply Navarro's correspondence to $G/O_{p'}(G)$) so we are done in this case. Hence, $Q = O_p(G) \neq 1$. Let $\mu = \lambda_Q$ so μ is a linear character of Q. Let T be the stabilizer of μ in G so $P \leq T \leq G$.

If $T = G$ then let R be the kernel of μ so $R \trianglelefteq G$. We apply induction to G/R to the linear character corresponding to λ and to the character corresponding with χ_λ (χ_λ "lies over" μ so is a character of G/R) and we are done.

Finally, suppose $T < G$. By Navarro's correspondence, applied to T, $\lambda^T = \alpha_\lambda + \dots$ where α_λ is an irreducible character of T of degree prime to p and the dots represent characters of T of degree divisible by p. Since all these characters all "lie over μ" further induction to G preserves irreducibility. Also $P \leq T$ so $|G:T|$ is prime to p. Now, without loss of generality, we may assume that $H \cap T$ is a p-complement of T so, by induction, $(\alpha_\lambda)_{T \cap H}$ contains the principal character so $((\alpha_\lambda)_{T\cap H})^H$ contains 1_H. But, by Mackey's theorem $(\chi_\lambda)_H$ "contains" $(\alpha_\lambda)^H_{T\cap H}$ so we are done.

Let's look at one example, $G = \Sigma_4$, $p = 2$. The character table and decomposition matrix are well known. We are interested in the cuspidal unipotent character corresponding to the character of odd degree and the first column. This is the Steinberg

of G with respect to H. The decomposition matrix suggests this Hecke algebra is isomorphic with $R[Z_2 \times Z_2]$. This is not so. Here are the character table and class-count table:

(1)	(12)(34)	(123)	(12)	(1234)
1	1	1	1	1
1	1	1	−1	−1
2	2	−1	0	0
3	−1	0	1	−1
3	−1	0	−1	1

$\langle (123) \rangle$	$\begin{matrix}(12)\\(13)\\(23)\end{matrix}$	$A_4 - \langle (123) \rangle$	
D_1	D_2	D_3	D_4
1	0	0	0
0	0	3	0
2	0	6	0
0	3	0	3
6	0	0	6

Hence, the character table of the Hecke algebra is (removing a row of zeros):

D_1	D_2	D_3	D_4
1	1	3	3
1	−1	3	−3
1	1	−1	−1
1	−1	−1	1

This is commutative so the Hecke algebra is contained in a unique ring isomorphic to $R \oplus R \oplus R \oplus R$ inside the Hecke algebra over K. The quotient is described by the elementary divisors of this last table. They are 8, 4, 2, 1 as is easy to calculate. This appears from $R[Z_2 \times Z_2]$.

The Navarro correspondence revisited

We have a self-normalizing Sylow p-subgroup P of the finite group G and the one-to-one correspondence between linear characters of P and p'-characters of G (e.g. when G is p-solvable or when $p=2$ and $G=\Sigma_{2^n}$). We are interested in the Hecke algebra corresponding to G/P'. We have the usual modular system K, R, F. So the linear characters of $H_K(G/P')$ correspond one-to-one with the p'-characters of G and the submatrix of the character table for $H_K(G/P')$ corresponding to the linear characters and cosets of P' in P is just the character table of P/P'. What we want to know is whether the columns of the character table of $H_K(G/P')$ truncated to the rows for linear characters are all R-linear combinations of the columns of the embedded character table we just spoke of. This is clearly a question of calculating dot products and seeing them congruent to zero modulo $|P:P'|$ in R.

We claim that we just need to check inner products with the first column of the embedded character table, that is a column of all ones. Suppose D is a double P', P' coset. Suppose we are interested in the dot product of its (truncated) column with the column of the embedded character table for the element xP' of P/P'. Say $D = P'gP'$ and set $E = P' \times gP'$. We assert that the dot product of the column for E with the first column (of all ones) equals the calculation that we just expressed interest about. This will establish our claim.

It suffices to prove that

$$\frac{1}{|P'|}\sum_{h\in P'} \chi h \cdot \frac{1}{|P'|}\sum_{C\in C} C = \frac{1}{|P'|}\sum_{d\in D} d$$

since then we can apply the linear characters (which are representations) and then sum the expression over the linear characters to get the desired dot products. (Have to actually take some conjugates, using inverse elements). But

$$\chi h \cdot C = \chi h\, P' g\, P' = \chi\, P' g\, P' = P' \chi g\, P'$$

and all the factors $|P'|$ are alright as the number of terms h is $|P'|$.

To recap, we want to have

$$\Lambda(D) \equiv 0 \text{ modulo } P$$

where Λ is the sum of the p'-characters, D is a P', P' double coset, P is a Sylow p-subgroup and $\Lambda(D)$ means $\sum_{d\in D} \Lambda(d)$.
When $p=2$, $G = \Sigma_n$, $n = 2^a$ then Λ is the sum of the knots. We get the following from Hemmer, in this case

Lemma (Hemmer) Λ vanishes on elements of even order and $\Lambda(g)$, for g of odd order, equals $2^{(\#\text{cycles of } g) - 1}$.
(Count cycles of length 1).

Paul Fong tells us this follows directly from the Murnaghan - Nakayama theorem readily.

Corollary $\Lambda(gP) = |P|$ for any $g \in \Sigma_n$.

Proof We must to calculate

$$\Lambda\left(g \cdot \sum_{x \in P} x\right) = \Lambda(|P| ge) = |P| \Lambda(ge)$$

where $e = \frac{1}{|P|} \sum_{x \in P} x$ is an idempotent. Also for any $\mathbb{C}\Sigma_n$ module M, eM is the space of fixed points of P. By the Navarro correspondence, we both save the principal character has any fixed points of P other than zero, so the same as those of ge, i.e. ge also annihilates every non-principal character module. On the principal module, ge is the identity since g & e are both. Hence, $\Lambda(ge) = 1$ which is what we need.

Ring split group extensions

Suppose we have a group extension, a normal subgroup N of the finite group G. Let R be a commutative ring. We say R splits the group extension if the epimorphism of RG to $R[G/N]$ is split, that is we have a semi-direct products of rings. Basic question: What does this mean? When can we find a backwards map from G/N not just to G but to linear combinations of elements of G? Of course if $R = k$ a field of characteristic prime to the order of G then kG is a semi-simple algebra and so every ideal, not just the kernel of the map from kG to $k[G/N]$, is a direct summand so the group extension is always k-split.

A little stronger result is as follows, preserving the notation.

Proposition 1. If k is a field of characteristic coprime with $|G/N|$ or $|N|$ then the extension is k-split.

Proof. It suffices to deal with the case of prime fields so that we may assume k is perfect. If the characteristic is p and $(p, |G/N|) = 1$ then $kG \supseteq K \supseteq \mathrm{rad}(kG)$, where K is the kernel of the map to $k[G/N]$. By the Wedderburn Principal Theorem, as k is perfect, kG is a semidirect product of $\mathrm{rad}(kG)$ and an algebra A. But $A \simeq kG/\mathrm{rad}\, kG$ and A is semisimple so our first claim is valid.

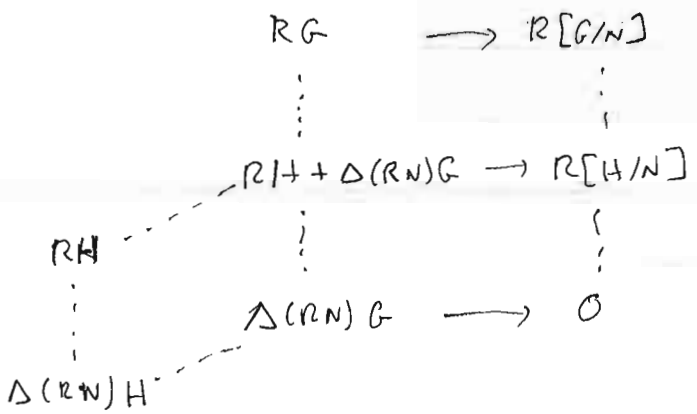
Suppose now that $p \nmid |N|$. Let $e = \frac{1}{|N|} \sum_{y \in N} y$ so e is a central idempotent of kG and $kG = kGe \oplus kG(1-e)$. By calculation, the image of e in $k[G/N]$ is the identity element so $1-e$ is mapped to zero and so is $kG(1-e)$. But if x, y are elements of G in the same coset of N then $xe = ye$, by an easy computation. Hence, $\dim_k kGe \leq |G:N|$ so we must have $kGe \simeq k[G/N]$ and $kG(1-e)$ equaling the kernel of the map $kG \to k[G/N]$.

What about $\mathbb{Z}$-split extensions? We do not know any that are not split. We can prove a special result, for p-groups, that there are none. In fact, we can do better and work over $\mathbb{Z}_p$. The result is, as we shall see, an immediate consequence of a deep theorem from integral representation theory.

Proposition 2 If N is a normal subgroup of the p-group G then this extension splits iff it is $\mathbb{Z}_p$-split.

Proof. Let $V = V(\mathbb{Z}_pG)$ be the group of units in the multiplicative group of $\mathbb{Z}_pG$ of augmentation one. If β is a "backwards" map then its image H is in V (as composing with the natural map is the identity so an element of H has augmentation one iff its image in $\mathbb{Z}_p[G/N]$ has the same property. Hence, by Alfred Weiss' "Sylow" theorem (Annals of Math. 127, p 317) H is conjugate to a subgroup of G by an element of V. But this conjugate is also mapped one-to-one to $\mathbb{Z}_p[G/N]$ so it intersects N in 1. By order considerations, we have a split extension.

It is natural to ask if we can get the same result assuming N is a p-group but letting G/N be arbitrary. One problem is that using splitting does not seem to automatically extend to subgroups. So suppose N is a normal subgroup of the group G and $N \leq H \leq G$. Assume R, a ring, splits the extension of N by G/N. What about the extension of N by H/N? The kernel of the map of RG to $R[G/N]$ is easily seen to be $\Delta(RN)G$ so we have the following picture:



where $\Delta(RN)H = RH \cap \Delta(RN)G$ (as $\Delta(RN)G$ is the direct sum of terms $\Delta(RN)t$, as t runs over a set of coset representatives for N in G. So we have a "backwards" map

$$R[H/N] \longrightarrow RH + \Delta(RN)G$$

but not necessarily to RH.

However, if H is a Sylow p-subgroup of G (so N is a p-group) then we can't, when $R = \mathbb{Z}_p$, automatically reduce to looking at H.

We now turn to fields of characteristic p for our rings.

<u>Theorem 1</u> If N is a central subgroup of the p-group P and R is a field of characteristic p then the extension splits if, and only if, it is R-split.

First, we want to observe that splitting by R (or any ring) passes to quotients. That is, if $N_1 \leq N$ are normal subgroups of the group G and R splits G over N then it splits G/N_1 over N/N_1. Consider the set-up

$$\begin{array}{ccccc} R[G/N_1] & \longleftarrow & RG & \longrightarrow & R[G/N] \\ \vdots & & \vdots & & \vdots \\ \Delta(N/N_1)\cdot G/N_1 & \longleftarrow & \Delta(RN)G & \longrightarrow & 0 \\ \vdots & & \vdots & & \\ 0 & \longleftarrow & \Delta(RN_1)G & & \end{array}$$

where we are assuming a complement to $\Delta(RN)G$ in RG so certainly we get one for $\Delta(N/N_1)\cdot G/N_1$ in $R[G/N_1]$.

This means that we can assume, in the above theorem, that N is cyclic if need be. For just look at it as a cyclic problem and be S-clear.

We now proceed with the proof of Theorem 1. By hypothesis, there is a subalgebra A of RP, isomorphic with $R[P/N]$ under the natural homomorphism, such that

$$\Delta RP = \Delta(RN)P + A$$

is a semidirect "product," that is a splitting. Now

then A contains a subset whose images in $kP/\Delta(kN)P$ are a vector space basis. Since kN is a local ring and kP is a free kN-module, such a basis must be generators for the kN-module kP. In particular, $(kN)A = kP$. But N is central, so, by dimension counting

$$kP \cong kN \otimes k[P/N]$$
$$\cong k[N \times P/N].$$

We aim to use this to deduce that N is a direct factor of P.

First, a general observation. If G is any finite group then kG abelianized is isomorphic with $k[G/G']$. Indeed, if $x, y \in G$,

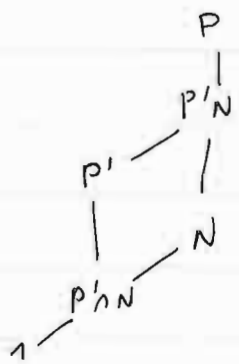
$$x^{-1}y^{-1}xy - 1 = x^{-1}y^{-1}(xy - yx)$$

so $\Delta(kG')$, and hence the ideal generated by it, namely $\Delta(kG')kG$, is in the ideal generated by $[kG, kG]$. But $kG/(\Delta G')kG$ is abelian so the claim is valid.

Hence, returning to the proof, we have that

$$k[P/P'] \cong k[N \times P/P'N]$$

But we have the diagram



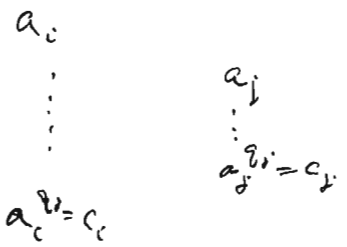
By comparing orders, we deduce that $P' \cap N = 1$. Hence,

$Q = P/P'$ has a subgroup $\tilde{N}$ isomorphic with N and $Q/\tilde{N} \simeq P/P'N$ with $kQ \simeq k[\tilde{N} \times Q/\tilde{N}]$. If we can deduce that $\tilde{N}$ is a direct factor then $P'N$ is a direct factor of P and, since $P' \cap N = 1$, we would have N a direct factor of P. Thus, we are reduced to the following: P is an abelian p-group, N is a subgroup, $k[P] \simeq k[N \times P/N]$ and we wish to deduce that N is a direct factor of P.

The next step is to reduce that $P \simeq N \times P/N$. This is a special case of the modular group ring isomorphism problem, which is unsolved. But in the abelian case it is, see W. E. Deskins, "Finite abelian groups with isomorphic group algebras," Duke Math. J. 23 (1956), 35-40. (Presumably, Jennings' theorem is in play here.)

Let's study a cyclic subgroup C of a finite abelian p-group A, in general. If $A = A_1 \times \cdots \times A_n$ is a direct decomposition with cyclic factors and $a \in A$ let $s(a)$ be the number of non-identity "coordinates" so for generators of C, s is constant. Fix a decomposition where this value is minimized. Let $c = c_1 \cdots c_n$ be a generator of C and its coordinates. Suppose $i \neq j$, $c_i \neq 1$, $c_j \neq 1$ and $|A_i| \geq |A_j|$. Then we claim that $|c_i| > |c_j|$, a strict inequality. Assume that $|c_i| \leq |c_j|$ and we need to derive a contradiction. By change of generators we may assume $a_i^{q_0} = c_i$, $a_j^{q_j} = c_j$ where $A_i = \langle a_i \rangle$, $A_j = \langle a_j \rangle$ and q_0 and q_j are powers of p.

We must have $q_i \geq q_j$ (that is $q_j \mid q_0$) as a_i has the order of at least the order of a_j and c_i has the order at most the order of c_j. Picture:

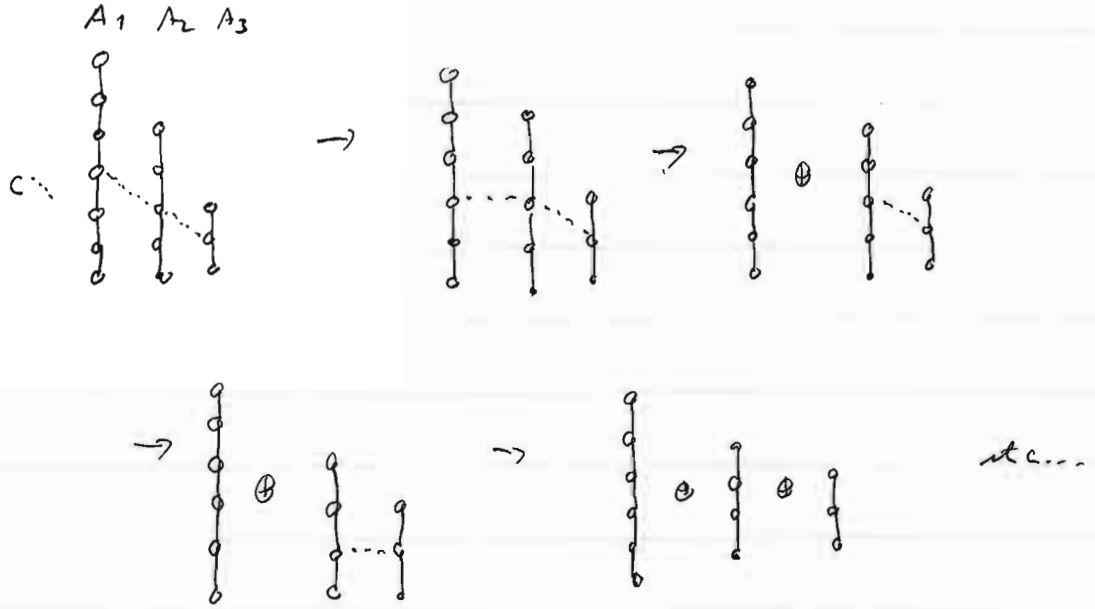


Hence, $a_i^{q_0/q_j} \cdot a_j$ has the same order as a_j and its q_0/q_j th power is $c_i c_j$. Hence, replace $\langle a_j \rangle$ by $\langle a_i^{q_0/q_j} a_j \rangle$ in the decomposition and we contradict the minimality of s, as above.

Notice, that as a consequence, after interchanging i and j we cannot have $|A_i| = |A_j|$. Thus, the orders of the factors of A giving the non-identity coordinates of C are all distinct. Hence, we can renumber so that $A = A_1 \times \dots \times A_m \times \cdots$ where $|A_1| > \dots > |A_m|$, $A_1, \dots, A_m$ are the factors giving non-identity coordinates $c_1, \dots, c_m$ so $|c_1| > \cdots > |c_m|$ as well. In particular, it follows directly that the subgroup of order p in A_1 is contained in C so the exponent of $A_1 \times \dots \times A_m / C$ is less than the exponent of $A_1 \times \dots \times A_m$, that is, of A_1. Hence, the number of factors of order $|A_1|$ in $A = A_1 \times \dots \times A_n$ is one plus the number in A/C. But if it happens that $A \simeq A/C \times C$ then this is a contradiction unless $|C| = |A_1|$, in which case it is immediate that C is a direct factor of A. Notice that we have now completed the proof of the theorem that we were working on.

We want to make, as an aside, one more observation about cyclic subgroups, keeping the same notation as above. If $|A_i| > |A_j|$ then $|A_i|/|C_i| > |A_j|/|C_j|$. Otherwise, $A_j/\langle C_j \rangle$ has a subgroup isomorphic with $A_i/\langle C_i \rangle$ and we can "clean" to replace A_i by another factor and then contradict the minimality.

We guess that the conditions we have give the classification of cyclic subgroups of A, up to the action of $\mathrm{Aut}(A)$. The method would be to look for the largest subgroup of C which lies in a cyclic direct factor, factor this out, continue this way, keep track of various orders, this should do it. Here is an example.



Theorem 2 If N is a central and elementary p-subgroup of the finite groups G and k is a field of characteristic p then the extension splits if, and only if, it is k-split.

As before this reduces us to the case of N of order p and central. Presumably the theorem holds when N is not elementary but we have no proof. By abuse of notation, we shall let $g, h, l, \ldots$ be elements of G/N, choosing coset representatives $x_g, x_h, x_l, \ldots$. Hence, $x_g x_h = \alpha(g,h) x_{gh}$, $\alpha(g,h) \in N$ so $\alpha(g,h) = y^{a(g,h)}$ where $N = \langle y \rangle$. Let $\epsilon = y - 1$ so $y = 1 + \epsilon$. We now view kG as an algebra over kN so since $kN = k[\epsilon]$, $\epsilon^p = 0$ we are viewing kG as a deformation of degree $p-1$ of $k[G/N]$. We wish to calculate the corresponding Hochschild 2-cocycle in terms of α. Hence, we wish to "calculate modulo ϵ^2."

But $y^{a(g,h)} = (1+\epsilon)^{a(g,h)} \equiv 1 + a(g,h)\epsilon$. Hence,

$$x_g x_h = y^{a(g,h)} x_{gh} \equiv (1 + a(g,h)\epsilon) x_{gh}$$
$$= x_{gh} + (a(g,h) x_{gh})\epsilon.$$

Let $f(g,h) = a(g,h) x_{gh}$. We wish to verify that α is a Hochschild 2-cocycle, as it has to be. Multiplying the above equation by x_l on the right we get

$$(x_g x_h) x_l = x_{gh} x_l + a(g,h) x_{gh} x_l \epsilon$$
$$= x_{ghl} + a(gh,l) x_{ghl} \epsilon$$
$$+ a(g,h)\{ x_{ghl} + a(gh,l) x_{ghl} \epsilon \} \epsilon$$
$$= x_{ghl} + \{ a(gh,l) x_{ghl} \epsilon + a(g,h) x_{ghl} \} \epsilon$$
$$= x_{ghl} + \{ f(gh,l) + f(g,h) x_{gh}^{-1} x_{ghl} \} \epsilon$$

$$= X_{gkl} + \{ f(gk,l) + f(g,k) X_l \} \epsilon$$

as $X_{gk}^{-1} X_{gkl} \equiv X_l \mod \epsilon$ so ϵ^2 gives a 2-cocycle congruence. Hence, we have one side of a Hochschild 2-cocycle equation. The other case is left to the reader. The formula, from α to f is a homomorphism as is clear. Hence, to prove the theorem, it remains only to show that if f is a coboundary then so is α. (The other way is immediate as group splitting gives ring splitting.)

We change notation, so f has values in kG: we have $f(g,k) = a(g,k) gk$. Suppose that f is a Hochschild 2-coboundary so

$$f(g,k) = g\,\gamma(k) - \gamma(gk) + \gamma(g)\,k$$

where $\gamma : G \to kG$. Hence,

$$a(g,k)\,gk = g\,\gamma(k) - \gamma(gk) + \gamma(g)\,k$$

$$a(g,k) = g\,\gamma(k) k^{-1} g^{-1} - \gamma(gk) k^{-1} g^{-1} + \gamma(g) g^{-1}$$

$$= {}^{g}\gamma(k) k^{-1} - \gamma(gk)(gk)^{-1} + \gamma(g) g^{-1}$$

$$= {}^{g}b(k) - b(gk) + b(g)$$

where $b(g) = \gamma(g) g^{-1}$ etc. Taking the identity component of the right-hand side gives what we need. For the identity component has values in k and if $a(g,k)$ is a coboundary over k it is over $\mathbb{F}_p$ which is what we need.

This argument fails in the non-elementary case as we can have "partial" splitting. Also keeping track of all higher deformations looks messy.

Questions.

1. Does our map of cohomology to Hochschild coho. agree with the usual one?
2. Can we do a B_∞ version using Buchholmann?
3. Other blocks?
4. Start with local information for a block? Stability.
5. Connection with Smith-Tyan for blocks?

Let's now return to the topic of a cyclic subgroup C of a finite abelian p group A. We used to see that the form we had is a canonical one in that it classifies C up to the action of $\mathrm{Aut}(A)$. We have parts

$$\lambda_1 \geq \cdots \geq \lambda_r$$

of the partition that classifies A. We have other positive integers

$$\mu_1 \geq \cdots \geq \mu_r$$

where $\mu_i \leq \lambda_i$ and

$$\lambda_1 - \mu_1 \geq \cdots \geq \lambda_r - \mu_r.$$

We have elements a_i, $1 \leq i \leq r$, of A of order p^{λ_i} from a direct decomposition (i.e. a_i is a generator of one factor, for all i, from one decomposition). We have $c_i = a_i^{p^{\lambda_i - \mu_i}}$ of order p^{μ_i} in $\langle a_i \rangle$ and

$$C = c_1 c_2 \cdots c_r$$

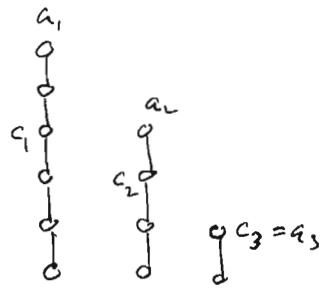
where $C = \langle c \rangle$. We want to see all these λ_i, μ_i are determined by C in a structural way so that we have a classification up to the action of $\mathrm{Aut}(A)$.

The idea is as follows. $C_1 = \langle c_1 p^{\mu_2} \rangle$ has order $p^{\mu_1 - \mu_2}$ and is the largest subgroup of C contained in a cyclic direct factor of A. When we factor it out we are looking at a situation where we have deleted λ_1 and μ_1 (and added a direct factor). The order of this cyclic factor containing C_1 is p^{λ_1}. We now check carry this out.

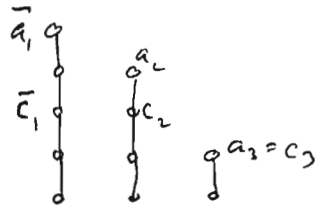
First, a remark. We are just using the nature of the form, not using the minimality that gave rise to it! Hence, we need only do as we just said. Really from above we include other direct factors of A when C has trivial projection.

We need some preliminary facts. With the above notation, $c^p = c_1^p \cdots c_r^p$ is also canonical (allowing for identity components). And so on for other powers p^e, $e \geq 0$. Another observation: if $r > 1$ then c is not an element of a cyclic direct factor of A. For in this case, c_r is a $p^{\lambda_r - \mu_r}$ power as are $c_2, \ldots, c_{r-1}$ since $\lambda_i - \mu_i \geq \lambda_r - \mu_r$, but no higher power. But the same holds for C but in a homomorphic image, namely $\langle c_1 \rangle$ there are further roots, a contradiction.

Hence, to calculate which powers c^{p^α} are in cyclic direct factors, calculate these and so when the canonical part has $r = 1$. We get a element in C and $\langle a_1 \rangle$ of order $p^{\mu_1 - \mu_2}$. Here's the picture!



and $c_1^{p^2} = c^{p^2} = a_1^{p^4}$ is what we are after. If we factor it out then get a similar picture with the $a_2, \ldots a_n$, $c_2 \ldots c_n$ the same but a_1, c_1 of smaller order. New orders are $p^{\lambda_1 - (\mu_1 - \mu_2)} = p^{\lambda_1 - \mu_1 + \mu_2}$; $p^{\mu_1 - (\mu_1 - \mu_2)} = p^{\mu_2}$. In the example



Since $\bar{c}_1, c_2$ have same order, $\bar{a}_1$ has order larger than a_2, can get new a_2 and be reduced to a smaller case, "shearing" as above. Hence, done.

Note: There is a reference, as follows:

H. Birkhoff, Subgroups of abelian groups, Proc. L.M.S. (2) 38 (1934), 385-401.

Furthermore, with an assist from Said Sidki, there are references for the problem of an abelian group G, finitely generated, with subgroup N with $G \simeq N \times G/N$. It is always true that this forces N to be a direct factor.

This is due to H. Toda and the simple proof is to be found in the paper: T. Mijata, Note on direct summands of modules, J. Math. Kyoto Univ. 7 (1967), 65-69. The analogous theorem for finite groups is to be found as follows: J. Ayoub, The direct extension theorem, J. Groups Theory 9 (2006), no. 3, 307-316. A general module result is as follows: R. M. Bumagnick, Roth's theorem and decomposition of modules, Linear Algebra Appl. 39 (1981), 155-165.