Diagonal resolutions for metacyclic groups

FEA Johnson and JJ Remez

Abstract

We show the finite metacyclic groups $G(p,q)$ admit a class of projective resolutions which are periodic of period $2q$ and which in addition possess the properties that a) the differentials are 2×2 *diagonal* matrices; b) the Swan-Wall finiteness obstruction (cf [21], [22]) vanishes. We obtain thereby a purely algebraic proof of Petrie's Theorem ([16]) that $G(p,q)$ has free period $2q$.

Keywords: Diagonal resolution; metacyclic group.

Mathematics Subject Classification (AMS 2010):

Primary 16E05; 20C10: Secondary 18E30

§0 : Introduction:

The metacyclic group $G(p,q) = C_p \rtimes C_q$ is the semi-direct product of cyclic groups where p is an odd prime, q is a divisor of $p-1$ and where C_q acts on C_p via the natural imbedding $C_q \hookrightarrow \mathrm{Aut}(C_p)$. It is known that $G(p,q)$ has cohomological period $2q$ and hence (cf [21], [22]) the trivial module $\mathbb{Z}$ has a finitely generated projective resolution of period $2q$ over the integral group ring $\Lambda = \mathbb{Z}[G(p,q)]$. In this paper we show that each $G(p,q)$ admits a projective resolution

$$\Delta_* = (\cdots \to \Delta_{2n+1} \xrightarrow{\partial_{2n+1}} \Delta_{2n} \xrightarrow{\partial_{2n}} \Delta_{2n-1} \xrightarrow{\partial_{2n-1}} \cdots\cdots \xrightarrow{\partial_2} \Delta_1 \xrightarrow{\partial_1} \Delta_0 \to \mathbb{Z} \to 0)$$

of *diagonal type* described by the following conditions (i) - (iii):

(i) $\Delta_0 = \Lambda$;

(ii) for each $k \geq 1$ $\Delta_{2k-1} = \Lambda \oplus \Lambda$ and $\Delta_{2k} = P(k) \oplus \Lambda$ where $P(k)$ is a projective module of rank 1 over Λ;

(iii) for each $k \geq 2$ the differential ∂_k has the diagonal form $\partial_k = \begin{pmatrix} \partial_k^+ & 0 \\ 0 & \partial_k^- \end{pmatrix}$.

Such a resolution is *periodic of period* $2q$ when $P(k+mq) = P(k)$ and $\partial^{\pm}_{k+2mq} = \partial^{\pm}_k$ for all $k, m \geq 1$; in addition it is said to be *almost free* when

$$\bigoplus_{r=1}^{q-1} P(r) \cong \Lambda^{(q-1)} \quad \text{and} \quad P(q) \cong \Lambda.$$

Theorem A: For any odd prime p and any divisor q of $p-1$, the trivial module $\mathbb{Z}$ admits an almost free resolution of diagonal type and period $2q$ over $\Lambda = \mathbb{Z}[G(p,q)]$.

In general, if the finite group G has cohomological period $2q$ then its free period is $2\delta q$ where δ is a positive integer which divides the order of the projective class group $\widetilde{K}_0(\mathbb{Z}[G])$. Moreover, there are cases known in which $\delta > 1$; for example, certain generalised quaternionic groups $Q(8;p,q)$ (cf [1], [13], [14]). However, Theorem A implies that in the present case $\delta = 1$; that is:

Theorem B : The group $G(p,q)$ has free period $2q$.

The conclusion of Theorem B follows implicitly from the main theorem of Petrie's paper [16], where it is proved in a topological context by showing that a certain surgery obstruction vanishes. By contrast, our proof is purely module theoretic.

In the proof of Theorem A the lower strand of the resolution is easily constructed, being induced up from the standard resolution of C_q thus:

$$\ldots \Lambda \xrightarrow{y-1} \Lambda \xrightarrow{\Sigma_y} \Lambda \xrightarrow{y-1} \Lambda \xrightarrow{\Sigma_y} \Lambda \xrightarrow{y-1} \Lambda \xrightarrow{\Sigma_y} \Lambda \xrightarrow{y-1} \Lambda \xrightarrow{\Sigma_y} \ldots$$

By contrast, far more work is required to construct the upper strand

$$\cdots \xrightarrow{\partial^+_{2n+2}} \Lambda \xrightarrow{\partial^+_{2n+1}} P(n) \xrightarrow{\partial^+_{2n}} \Lambda \xrightarrow{\partial^+_{2n-1}} P(n-1) \xrightarrow{\partial^+_{2n-2}} \Lambda \xrightarrow{\partial^+_{2n-3}} \ldots$$

To do this we first describe Λ as a fibre product

$$\begin{tikzcd}
\Lambda \arrow[r] \arrow[d] & \mathcal{T}_q(A,\pi) \arrow[d] \\
\mathbb{Z}[C_q] \arrow[r] & \mathbb{F}_p[C_q].
\end{tikzcd}$$

Here A is a ring of cyclotomic integers which ramifies completely over p ; $\pi \in A$ is the unique prime over p ; $\mathcal{T}_q(A,\pi)$ is the following *quasi-triangular* subring of $M_q(A)$

$$\mathcal{T}_q(A,\pi) \;=\; \{X = (x_{rs})_{1\le r,s\le n} \in M_q(A) \mid x_{rs} \in (\pi) \text{ if } r > s\}.$$

We denote by $R(i)$ the i^{th} row of $\mathcal{T}_q(A,\pi)$ considered as a right Λ-module so that

$$\mathcal{T}_q(A,\pi) \cong R(1) \oplus R(2) \oplus \cdots \oplus R(q).$$

The obvious projections $\Lambda \to \mathcal{T}_q(A,\pi)$ and $\mathcal{T}_q(A,\pi) \to R(i)$ compose to give a surjection $p_i : \Lambda \to R(i)$. In particular, each $R(i)$ is *monogenic*[†]; that is, generated by a single element over Λ. Defining $K(i) = \mathrm{Ker}(p_i : \Lambda \to R(i))$ we first show:

Theorem C : There exists an exact sequence of the following form

$$\begin{tikzcd}
 & & & & & K(q) \arrow[dr] & & & \\
\mathfrak{S}(q) & = & (\ 0 \arrow[r] & R(1) \arrow[r] & \Lambda \arrow[rr] \arrow[ur] & & \Lambda \arrow[r] & R(q) \arrow[r] & 0\ )
\end{tikzcd}$$

We refer to $\mathfrak{S}(q)$ as a *basic sequence*; it demonstrates the non-obvious fact that $K(q)$ is also monogenic. From the existence of $\mathfrak{S}(q)$ we proceed to deduce:

Theorem D : For $1 \le i \le q-1$ there are exact sequences over Λ of the form

$$\begin{tikzcd}
 & & & & & K(i) \arrow[dr] & & & \\
\mathfrak{S}(i) & = & (\ 0 \arrow[r] & R(i+1) \arrow[r] & P(i) \arrow[rr] \arrow[ur] & & \Lambda \arrow[r] & R(i) \arrow[r] & 0\ )
\end{tikzcd}$$

where $P(2), \ldots, P(q)$ are projective modules of rank 1 such that $\bigoplus_{i=2}^{q} P(i) \cong \Lambda^{q-1}$.

[†] The referee points out that *monogenic modules* are frequently called *cyclic modules.*

Splicing the segments $\mathfrak{S}(i)$ together with $\mathfrak{S}(q)$ gives the exact sequence which constitutes the upper strand in Theorem A, namely:

$$\begin{tikzcd}
 & & & K(q) \arrow[dr] & & & & K(q-1) \arrow[dr] & & K(2) \arrow[dr] & & & & K(1) \arrow[dr] & & & \\
0 \arrow[r] & R(1) \arrow[r] & \Lambda \arrow[rr] \arrow[ur] & & \Lambda \arrow[rr] \arrow[dr] & & P(q\text{-}1) \arrow[r] \arrow[ur] & & \cdots\ \cdots \arrow[ur] \arrow[rr] & & \Lambda \arrow[rr] \arrow[dr] & & P(1) \arrow[rr] \arrow[ur] & & \Lambda \arrow[r] & R(1) \arrow[r] & 0. \\
 & & & & & R(q) \arrow[ur] & & & & & & R(2) \arrow[ur] & & & & &
\end{tikzcd}$$

The possibility of constructing such diagonal resolutions originates from the fact that the augmentation ideal I_G of $G = G(p,q)$ decomposes as a direct sum

$$I_G \;\cong\; \overline{I_C} \,\oplus\, [y-1).$$

Here y is a generator of C_q and $[y-1)$ is the right ideal of Λ generated by $y-1$ whilst $\overline{I_C}$ is the Galois module obtained from the action of C_q on the augmentation ideal I_C of C_p; as we shall see, $\overline{I_C}$ is isomorphic to $R(1)$. The existence of such a direct sum decomposition has been known for many years (cf. the paper of Gruenberg and Roggenkamp [7]). However, in the interests of clarity and completeness we give a direct proof (see §5 below).

Beyond Theorem A it is tempting to conjecture that each $G(p,q)$ admits a diagonal resolution with the additional property that each $P(i) \cong \Lambda$. Such a resolution is called *strongly diagonal* ; in fact our proof of Theorem D shows that the p-adic completion $\widehat{\Lambda}$ admits such a strongly diagonal resolution. In [10] the first named author showed the existence of strongly diagonal resolutions in all the cases $G(p,2)$; that is, for the dihedral groups of order $2p$. For $q \geq 3$, the task of constructing resolutions of this stronger type is less straightforward. If the sequences $\mathfrak{S}(1), \ldots, \mathfrak{S}(q\text{-}1)$ could be modified to the form

$$\mathfrak{S}(i)' \quad = \quad \Big(\begin{tikzcd}
 & & & K(i) \arrow[dr] & & & \\
0 \arrow[r] & R(i+1) \arrow[r] & \Lambda \arrow[rr] \arrow[ur] & & \Lambda \arrow[r] & R(i) \arrow[r] & 0
\end{tikzcd} \Big)$$

we could splice them together with $\mathfrak{S}(q)$ to give an exact sequence of period $2q$

$$\begin{tikzcd}
 & & & K(q) \arrow[dr] & & & & K(q-1) \arrow[dr] & & & & K(2) \arrow[dr] & & & & K(1) \arrow[dr] & & & \\
0 \arrow[r] & R(1) \arrow[r] & \Lambda \arrow[rr] \arrow[ur] & & \Lambda \arrow[rr] \arrow[dr] & & \Lambda \arrow[rr] \arrow[ur] & & \Lambda & \cdots & \Lambda \arrow[rr] \arrow[ur] & & \Lambda \arrow[rr] \arrow[dr] & & \Lambda \arrow[rr] \arrow[ur] & & \Lambda \arrow[r] & R(1) \arrow[r] & 0 \\
 & & & & & R(q) \arrow[ur] & & & & & & & & R(2) \arrow[ur] & & & & &
\end{tikzcd}$$

to form the upper strand in a strongly diagonal resolution. This in turn would imply that each $K(i)$ is monogenic, a fact which is yet to be established in general.

Apart from the dihedral groups, strongly diagonal resolutions were previously known to exist only for the groups $G(5,4)$ and $G(7,3)$, ([15], [19]), both cases being established by direct calculation. Elsewhere [11] we shall establish the existence of $\mathfrak{S}(1)', \ldots, \mathfrak{S}(q-1)'$ for certain small values of p and q. In particular, we are able to show the existence of strongly diagonal resolutions in the cases;

$G(5,4)$; $G(7,3)$, $G(7,6)$; $G(11,5)$, $G(11,10)$; $G(13,3)$, $G(13,4)$, $G(13,6)$;

$G(17,4)$; $G(19,3)$, $G(19,6)$, $G(19,9)$.

The authors wish to thank the referee whose careful attention to detail revealed a number of notational inconsistencies.

§1 : Some standard modules over $\mathbb{Z}[G(p,q)]$

For each integer $n \geq 2$ we denote by C_n the cyclic group $C_n = \langle x \mid x^n = 1 \rangle$. For the remainder of this paper we fix an odd prime p, an integral divisor q of $p-1$ and write $d = (p-1)/q$. Recalling that $\mathrm{Aut}(C_p) \cong C_{p-1}$ then there exists an element $\theta \in \mathrm{Aut}(C_p)$ such that $\mathrm{ord}(\theta) = q$. Taking y to be a generator of C_q and making a once and for all choice of θ with order q, we construct the semi-direct product $G(p,q) = C_p \rtimes_h C_q$ where $h : C_q \to \mathrm{Aut}(C_p)$ is the homomorphism $h(y) = \theta$. There is then a unique integer a in the range $1 \leq a \leq p-1$ such that $\theta(x) = x^a$ and $G(p,q)$ then has the presentation

$$G(p,q) = \langle x, y \mid x^p = y^q = 1 \, ; \, yxy^{-1} = x^a \rangle.$$

The integer a will have a fixed meaning in what follows. We denote by Λ the integral group ring $\Lambda = \mathbb{Z}[G(p,q)]$ and by $i : \mathbb{Z}[C_p] \hookrightarrow \Lambda$ and $j : \mathbb{Z}[C_q] \hookrightarrow \Lambda$ the respective inclusions. Indecomposable lattices over Λ have been classified up to genus, though not up to isomorphism, by Pu [17]. Here we shall need only a small selection from Pu's list. Depending on context, $\mathbb{Z}$ may denote the trivial module over any of the group rings Λ, $\mathbb{Z}[C_p]$ or $\mathbb{Z}[C_q]$. Moreover I_C will denote the augmentation ideal of $\mathbb{Z}[C_p]$ and I_Q the augmentation ideal of $\mathbb{Z}[C_q]$. Clearly I_C is defined by the exact sequence of $\mathbb{Z}[C_p]$-modules

$$0 \to I_C \overset{\iota}{\hookrightarrow} \mathbb{Z}[C_p] \xrightarrow{\epsilon} \mathbb{Z} \to 0.$$

On dualising we get an exact sequence $0 \to \mathbb{Z} \xrightarrow{\epsilon^*} \mathbb{Z}[C_p] \xrightarrow{\iota^*} I_C^* \to 0$ where $\epsilon^*(1) = \Sigma_x = 1 + x + x^2 + \cdots + x^{p-1}$. It is a standard and easily verified fact that

(1.1) I_C^* and I_C are isomorphic as $\mathbb{Z}[C_p]$-modules.

If $i_*(-)$ denotes 'extension of scalars' from $\mathbb{Z}[C_p]$-modules to Λ-modules then:

(1.2) $i_*(I_C)$ and $i_*(I_C^*)$ are isomorphic as Λ-modules.

As I_C^* and I_C are not actually identical we find it convenient to distinguish between them. We identify the dual I_C^* with the quotient $\mathbb{Z}[C_p]/(\Sigma_x)$. As (Σ_x) is a two-sided ideal in $\mathbb{Z}[C_p]$ then I_C^* is naturally a ring; indeed, putting $\zeta = \exp(2\pi i/p)$ then:

(1.3) There is a ring isomorphism $I_C^* \cong \mathbb{Z}[\zeta]$.

If M is a module over $\mathbb{Z}[C_p]$ then by a *Galois structure* on M we mean an additive automorphism $\Theta : M \to M$ such that $\Theta^q = \mathrm{Id}_M$ and $\Theta(m \cdot x) = \Theta(m) \cdot \theta(x)$ for all $m \in M$ where θ is our chosen automorphism of C_p. By a *Galois lattice* we shall mean a pair (M, Θ) where M is a lattice over $\mathbb{Z}[C_p]$ and Θ is a Galois structure on M. The Galois lattice (M, Θ) becomes a (right) lattice over Λ via the action

$$m \cdot x^r y^s b = \Theta^{-s}(m \cdot x^r).$$

Significant examples of Galois lattices arise from ideals of $\mathbb{Z}[C_p]$ which satisfy $\theta(J) = J$. For such an ideal J we put $\overline{J} = (J, \Theta_J)$ where Θ_J is the restriction of θ to J. Thus we obtain Galois lattices $\overline{\mathbb{Z}[C_p]}$, $\overline{I_C}$ and $\overline{(x-1)^k I_C}$ $(k \geq 1)$. Similarly we denote by $\overline{I_C^*}$ the Galois lattice obtained from the dual of the augmentation ideal. Evidently $\overline{I_C^*}$ is a quotient $\overline{I_C^*} = \overline{\mathbb{Z}[C_p]}/(\Sigma_x)$. This last module is fundamental in what follows and we note the following properties which characterise it amongst Λ-modules.

Proposition 1.4: Let M be a Λ-lattice satisfying the following three conditions:

(i) there exists $\mu \in M$ such that $\mu \cdot y = \mu$ and $M = \mathrm{span}_{\mathbb{Z}}\{\mu \cdot x^r \mid 0 \leq r \leq p-1\}$;

(ii) $\mathrm{rk}_{\mathbb{Z}}(M) = p-1$.

(iii) $m \cdot \Sigma_x = 0$ for each $m \in M$;

Then $M \cong_\Lambda \overline{I_C^*}$ and $\{\mu \cdot x^r \mid 0 \leq r \leq p-2\}$ is a $\mathbb{Z}$-basis for M.

Proof : We note that conditions (ii) and (iii) above are satisfied for $\overline{I_C^*}$. Let $\natural : \overline{\mathbb{Z}}[C_p] \to \overline{I_C^*}$ be the natural mapping and put $\eta = \natural(1)$. Then $\eta \cdot y = \eta$ and $\{\eta \cdot x^r \mid 0 \leq r \leq p-2\}$ is a $\mathbb{Z}$-basis for $\overline{I_C^*}$. Now suppose that M is a Λ-lattice satisfying conditions (i), (ii) and (iii) and consider the homomorphism of abelian groups $\Psi : \overline{I_C^*} \to M$ defined on the basis $\{\eta \cdot x^r \mid 0 \leq r \leq p-1\}$ by $\Psi(\eta \cdot x^r) = \mu \cdot x^r$. As $M = \mathrm{span}_{\mathbb{Z}}\{\mu \cdot x^r \mid 0 \leq r \leq p-1\}$ then Ψ is necessarily surjective and as $\mathrm{rk}_{\mathbb{Z}}(\overline{I_C^*}) = \mathrm{rk}_{\mathbb{Z}}(M) = p-1$ then Ψ is bijective and $\{\mu \cdot x^r \mid 0 \leq r \leq p-2\}$ is a $\mathbb{Z}$-basis for M. Evidently Ψ is now an isomorphism of $\mathbb{Z}[C_p]$-modules. Moreover from the identities $\eta \cdot y = \eta$ and $\mu \cdot y = \mu$ it follows easily that Ψ is also an isomorphism over Λ. □

For any Galois lattice (M, Θ) there is an isomorphism of abelian groups

$$\Psi : \mathbb{Z}[C_q] \otimes (M, \Theta) \xrightarrow{\simeq} i_*(M) \quad (= M \otimes_{\mathbb{Z}[C_p]} \Lambda)$$

defined by taking $\Psi(y^b \otimes m) = \Theta^{-b}(m) \otimes y^b$. It is straightforward to check that Ψ is also a homomorphism of (right) Λ-modules. We obtain:

Proposition 1.5: $\mathbb{Z}[C_q] \otimes (M, \Theta) \cong i_*(M)$ for any Galois lattice (M, Θ).

Taking $J = \mathbb{Z}[C_p]$ and noting that $i_*(\mathbb{Z}[C_p]) = \Lambda$ we now see from (1.5) that :

(1.6) $$\mathbb{Z}[C_q] \otimes \overline{\mathbb{Z}[C_p]} \cong \Lambda.$$

In contrast to (1.1), $\overline{I_C^*}$ is *not isomorphic to* $\overline{I_C}$ and $\overline{(x-1)^k I_C}$ is *not, in general, isomorphic* to either $\overline{I_C^*}$ or $\overline{I_C}$.

Let Z be a set with $|Z| = q$ on which $\widehat{C_q} = \{1, \theta, \ldots, \theta^{q-1}\}$ acts transitively on the left; for each $z \in Z$ let $F(z)$ be the free $\mathbb{Z}[C_p]$-module of rank 1 with basis element $[z]$ and put $F(Z) = \bigoplus_{z \in Z} F(z)$. Then $F(Z)$ is a Galois module with Galois structure Θ where

$$\Theta([z] \cdot x^r) = [\theta_*(z)] \cdot \theta(x^r)$$

and it is straightforward to see that, as Λ-modules, $F(Z) \cong \Lambda$. More generally, suppose that Z is a finite set on which $\widehat{C_q}$ acts freely on the left and denote by $Z = Z_1 \coprod \ldots \cdots \coprod Z_m$ the partition of Z into disjoint orbits where each $|Z_i| = q$. By the above, $F(Z_i) \cong \Lambda$ for each i so that $F(Z) = \bigoplus_{i=1}^m F(Z_i) \cong \Lambda^m$; that is:

(1.7) If Z is a finite set on which $\widehat{C_q}$ acts freely with m orbits then $F(Z) \cong \Lambda^m$.

We first prove:

Proposition 1.8 : $\overline{I_C} \otimes [\Sigma_y) \cong \Lambda^d$.

Proof : Note that $i^*(\overline{I_C} \otimes [\Sigma_y)) \cong I_C \otimes \mathbb{Z}[C_p] \cong \bigoplus_{e=1}^{p-1} F(e)$ where $F(e)$ is the free module of rank 1 over $\mathbb{Z}[C_p]$ on the basis element $(x^e$ -$1) \otimes \Sigma_y$. Now $\widehat{C_q} = \{\mathrm{Id}, \theta, \theta^2, \ldots, \theta^{q-1}\}$ acts freely on $Z = \{(x^e - 1) \otimes \Sigma_y \mid \ 1 \leq e \leq p-1\}$. via the action

$$\theta_*((x^e - 1) \otimes \Sigma_y) = (\theta(x^e) - 1) \otimes \Sigma_y$$

under which Z decomposes as a disjoint union $Z_1 \coprod .... \coprod Z_d$ of $d = \frac{(p-1)}{q}$ cyclic orbits. In the above notation, $\overline{I_C} \otimes [\Sigma_y) \cong \bigoplus_{r=1}^{d} F(Z_r) \cong \Lambda^d$. □

Corollary 1.9 : $\overline{I_C} \otimes [y-1) \cong \Lambda^{d(q-1)}$.

Proof : The exact sequence $0 \to [y-1) \to \Lambda \to [\Sigma_y) \to 0$ gives an exact sequence

$$0 \to \overline{I_C} \otimes [y-1) \to \overline{I_C} \otimes \Lambda \to \overline{I_C} \otimes [\Sigma_y) \to 0.$$

As $\overline{I_C} \otimes [\Sigma_y) \cong \Lambda^d$ this latter sequence splits. Hence $\overline{I_C} \otimes [y-1) \oplus \Lambda^d \cong \Lambda^{p-1}$ so that $\overline{I_C} \otimes [y-1)$ is stably free of rank $p-d-1$. As Λ satisfies the Eichler condition then, by the Swan-Jacobinski Theorem $\overline{I_C} \otimes [y-1) \cong \Lambda^{p-d-1}$. However $p-d-1 = d(q-1)$ and so $\overline{I_C} \otimes [y-1) \cong \Lambda^{d(q-1)}$ as claimed □

For any Λ-lattices A, B, $(A \otimes B)^* \cong A^* \otimes B^*$. As Λ and $[y-1)$ are self-dual then:

Corollary 1.10: $\overline{I^*_C} \otimes [y-1) \cong \Lambda^{d(q-1)}$.

It is a standard consequence of Frobenius reciprocity that $M \otimes \Lambda \cong \Lambda^m$ whenever M is a Λ-lattice with $\mathrm{rk}_{\mathbb{Z}}(M) = m$. In particular:

(1.11) $\overline{I^*_C} \otimes \Lambda \cong \Lambda^{(p-1)}$.

§2 : A fibre product decomposition for $\mathbb{Z}[G(p,q)]$:

As is well known, $\mathbb{Z}[C_p]$ has a canonical fibre product decomposition

(2.1)

$$\begin{tikzcd}
\mathbb{Z}[C_p] \arrow[r] \arrow[d, "\epsilon"'] & I^*_C \arrow[d] \\
\mathbb{Z} \arrow[r] & \mathbb{F}_p
\end{tikzcd}$$

where $\epsilon : \mathbb{Z}[C_p] \to \mathbb{Z}$ is the augmentation map and $\mathbb{F}_p$ is the field with p elements. To proceed, we briefly recall the cyclic algebra construction. Thus let S denote a commutative ring and $\theta : S \to S$ a ring automorphism of finite order dividing q; in particular, θ satisfies the identity $\theta^q = \mathrm{Id}$. The *cyclic ring* $\mathcal{C}_q(S,\theta)$ is then the (two-sided) free S-module

$$\mathcal{C}_q(S,\theta) = S\,\mathbf{1} \dot{+} S\mathbf{y} \ldots \dot{+} S\mathbf{y}^{n-1}$$

of rank q with basis $\{\mathbf{1}, \mathbf{y}, \ldots \mathbf{y}^{q-1}\}$ and with multiplication determined by the relations

$$\mathbf{y}^q = \mathbf{1} \quad ; \quad \mathbf{y}\xi = \theta(\xi)\mathbf{y} \quad (\xi \in S).$$

So defined, $\mathcal{C}_q(S,\theta)$ is an extension ring of S. In the fibre product (2.1) θ induces a ring automorphism of order q on $\mathbb{Z}[C_p]$. As θ fixes Σ_x then θ induces a ring automorphism on the quotient $I^*_C = \mathbb{Z}[C_p]/(\Sigma_x)$. Likewise the augmentation ideal I_C is stable under θ and θ induces the identity automorphism both on the quotient $\mathbb{Z} = \mathbb{Z}[C_p]/I_C$ and $\mathbb{F}_p$. As the homomorphisms in (2.1) are equivariant with respect to these ring automorphisms we may apply the cyclic algebra construction $\mathcal{C}_q(-,\theta)$ to (2.1). Identifying $\mathcal{C}_q(\mathbb{Z}[C_p] = \mathbb{Z}(G(p,q)$,

$\mathcal{C}_q(\mathbb{Z}) \;=\; \mathbb{Z}[C_q]$, $\mathcal{C}_q(\mathbb{F}_p) \;=\; \mathbb{F}_p[C_q]$ we obtain a fibre product

(2.2)
$$\begin{tikzcd}
\mathbb{Z}[G(p,q)] \arrow[r] \arrow[d] & \mathcal{C}_q(I_C^*,\theta) \arrow[d] \\
\mathbb{Z}[C_q] \arrow[r] & \mathbb{F}_p[C_q].
\end{tikzcd}$$

To proceed to a more tractable description of $\mathcal{C}_q(I^*,\theta)$ we first make the identification $\mathcal{C}_q(I^*,\theta)\otimes\mathbb{Q} \cong \mathcal{C}_q(\mathbb{Q}(\zeta),\theta)$ where, as above, ζ is a primitive p^{th} root of unity. We note ([2], Lemma 3) that $p \;=\; (\zeta-1)^{p-1}u$ for some unit $u \in \mathbb{Z}(\zeta)^*$. In particular:

(2.3) p ramifies completely in $\mathbb{Z}(\zeta)$.

Applying $-\otimes\mathbb{Q}$ to (2.2) we see that $\mathbb{Q}[G(p,q)] \;\cong\; \mathbb{Q}[C_q] \times \mathcal{C}_q(\mathbb{Q}(\zeta),\theta)$ as $\mathbb{F}_p[C_q]\otimes\mathbb{Q} = 0$. Thus $\mathcal{C}_q(\mathbb{Q}(\zeta),\theta)$ is a semisimple $\mathbb{Q}$-algebra. Moreover the centre $\mathcal{Z}(\mathcal{C}_q(\mathbb{Q}(\zeta),\theta))$ is a field, namely the subfield $\mathbb{Q}(\zeta)^\theta$ of $\mathbb{Q}(\zeta)$ fixed by θ; hence:

(2.4) $\mathcal{C}_q(\mathbb{Q}(\zeta),\theta)$ is a simple $\mathbb{Q}$-algebra.

§3 : A quasi-triangular representation of $G(p,q)$:

If B is commutative ring and $I \lhd B$ is an ideal we denote by

$$\mathcal{T}_q(B,I) \;=\; \{X = (x_{rs})_{1\le r,s\le n} \in M_q(B) \mid x_{rs} \in I \text{ if } r > s\}$$

the ring of *upper quasi-triangular* matrices over B relative to I; when $I \;=\; \{0\}$ then $\mathcal{T}_q(B,\{0\}) \;=\; \mathcal{T}_q(B)$ is simply the ring of *upper triangular* matrices over B. We denote by $\mathcal{U}_q(B,I)$, $\mathcal{U}_q(B)$ the corresponding unit groups. Under the induced homomorphism $\natural : M_q(B) \to M_q(B/I)$ we have

(3.1) $$\mathcal{T}_q(B,I) \;=\; \natural^{-1}(\mathcal{T}_q((B/I))$$

Likewise from the induced map on unit groups $\natural : \mathrm{GL}_q(B) \to \mathrm{GL}_q(B/I)$ we see

(3.2) $$\mathcal{U}_q(B,I) \;=\; \natural^{-1}(\mathcal{U}_q(B/I)).$$

Note that θ acts on $\mathbb{Z}(\zeta)$ via the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \;\cong\; C_{p-1}$. Let $A \;=\; \mathbb{Z}[\zeta]^\theta$ denote the subring fixed by θ. Putting $\pi = (\zeta-1)^q$, it follows from (2.3) that:

(3.3) p ramifies completely in A and π is the unique prime in A over p.

We shall show that $\mathcal{C}_q(I^*,\theta) \;\cong\; \mathcal{T}_q(A,\pi)$. This may be regarded as a concrete form of Rosen's Theorem [20]. Whilst this isomorphism is known in principle (cf p.358 of [18]), for the purpose of calculation it is necessary to give an explicit description. To this end observe that $\{1,\zeta,\ldots,\zeta^{q-1}\}$ is an A-basis for $\mathbb{Z}(\zeta)$. On writing successively

$$\begin{array}{rclclcl}
\zeta & = & (\zeta-1) & + & 1 & & \\
\zeta^2 & = & (\zeta-1)^2 & + & 2(\zeta-1) & + & 1 \\
\zeta^r & = & (\zeta-1)^r & - & \sum_{k=0}^{r-1}(-1)^{r-k}\binom{r}{k}\zeta^k & &
\end{array}$$

we may make a sequence of elementary basis transformations to show that:

(3.4) $$\{(\zeta-1)^{q-1}, (\zeta-1)^{q-2}, \ldots, (\zeta-1), 1\} \quad \text{is an } A\text{-basis for } \mathbb{Z}(\zeta).$$

$G(p,q)$ acts on the right of $\mathbb{Z}(\zeta)$ by $\mathbb{Z}\cdot(x^r y^s) = \theta^{-s}(\mathbb{Z}\cdot\zeta^{-r})$. Via the basis of (3.4), this action gives a representation $\lambda : G(p,q) \to \mathrm{GL}_q(A)$ where $\lambda(x^{-1})$ is given by

$$\lambda(x^{-1})[(\zeta-1)^r] = \begin{cases} (\zeta-1)^{r+1} + (\zeta-1)^r & 1 \le r \le q-2 \\ \pi + (\zeta-1)^{q-1} & r = q-1. \end{cases}$$

Hence the matrix of $\lambda(x^{-1})$ takes the quasi-triangular form

$$\lambda(x^{-1}) = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 & 0 \\ & & & \ddots & & & \\ & & & & \ddots & & \\ & & & & & \ddots & \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 \\ \pi & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

As x^{-1} generates C_p, the restriction of λ to C_p is also quasi-triangular; that is:

(3.5) $\lambda(C_p) \subset \mathcal{U}_q(A,\pi)$.

It follows that the full representation $\lambda : G(p,q) \to GL_q(A)$ is also quasi-triangular. To see this, let $X \in M_q(A)$ be an upper triangular matrix; we say that X is *unitriangular* when in addition $X_{ii} = 1$ for all i. A unitriangular matrix X will be called a *generalized Jordan block* when in addition $X_{ij} \neq 0 \iff j = i$ or $j = i+1$. The following is straightforward.

Proposition 3.6 : Let A be a commutative integral domain, let $X, Z \in M_q(A)$ be unitriangular matrices and suppose that $Y \in M_q(A)$ satisfies $XY = YZ$; if X is a generalized Jordan block then Y is upper triangular.

Let $\natural : GL_q(A) \to GL_q(A/\pi)$ denote the canonical homomorphism. The above expression for $\lambda(x^{-1})$ shows that $\natural\circ\lambda(x^{-1})$ is a generalized Jordan block. Hence for all r, $\natural\circ\lambda(x^r)$ is unitriangular. Writing $\theta(x) = x^t$ then $x\cdot y^{-1} = y^{-1}x^t$ so that

$$\natural\circ\lambda(x)\,\natural\circ\lambda(y^{-1}) = \natural\circ\lambda(y^{-1})\,\natural\circ\lambda(x^t).$$

Taking $X = \natural\circ\lambda(x)$, $Y = \natural\circ\lambda(y^{-1})$ and $Z = \natural\circ\lambda(x^t)$ in (3.6) shows that $\natural\circ\lambda(y^{-1})$ is upper triangular. As y^{-1} generates C_q then $\mathrm{Im}(\natural\circ\lambda) \subset \mathcal{U}_q(A/\pi) = \natural^{-1}(\mathcal{U}_q(A/\pi))$; thus:

Theorem 3.7 : $\lambda(G(p,q) \subset \mathcal{U}_q(A,\pi)$.

Consequently λ induces a ring homomorphism $\lambda_* : \mathbb{Z}[G(p,q)] \longrightarrow \mathcal{T}_q(A,\pi)$. Noting that $\lambda_*(\Sigma_x) = 0$ then λ_* induces ring homomorphisms

$$\widehat{\lambda}_* : \mathcal{C}_q(I^*,\theta) \to \mathcal{T}_q(A,\pi) \quad ; \quad \widehat{\lambda}_*\otimes\mathrm{Id} : \mathcal{C}_q(\mathbb{Q}(\zeta),\theta) \to M_q(A\otimes\mathbb{Q}).$$

As $\mathcal{C}_q(\mathbb{Q}(\zeta),\theta)$ is a simple $\mathbb{Q}$-algebra then $\widehat{\lambda}_*\otimes\mathrm{Id} : \mathcal{C}_q(\mathbb{Q}(\zeta),\theta) \to M_q(A\otimes\mathbb{Q})$ is injective and hence also:

(3.8) $\widehat{\lambda}_* : \mathcal{C}_q(I^*,\theta) \to \mathcal{T}_q(A,\pi)$ is injective.

In fact λ_* is also surjective. To see this, suppose that $\mathcal{C}$, $\mathcal{T}$ are both orders in the same finite dimensional semisimple $\mathbb{Q}$-algebra and that $\lambda : \mathcal{C} \to \mathcal{T}$ is an injective ring homomorphism. As $\mathcal{C}$, $\mathcal{T}$ both have the same $\mathbb{Z}$-rank it follows that $\lambda(\mathcal{C})$ has finite index δ in $\mathcal{T}$. Furthermore δ is determined by the relation $\mathcal{D}\mathrm{isc}(\mathcal{T}) = \delta^2\mathcal{D}\mathrm{isc}(\mathcal{C})$ between discriminants. In our case, taking $\mathcal{C} = \mathcal{C}_q(I^*, \theta)$ and $\mathcal{T} = \mathcal{T}_q(A, \pi)$, one may calculate (cf [18] Chapter 2) that:

(3.9) $\quad \mathcal{D}\mathrm{isc}(\mathcal{C}_q(I^*, \theta)) = \pm\, \mathcal{D}\mathrm{isc}(\mathcal{T}_q(A, \pi)) = \pm\, \pi^{q(q-1)}q^{q^2}.$

In consequence, $\delta = 1$. Thus as previously claimed $\widehat{\lambda}_*$ is surjective; hence:

Theorem 3.10 : $\widehat{\lambda}_* : \mathcal{C}_q(I^*, \theta) \to \mathcal{T}_q(A, \pi)$ is a ring isomorphism.

We may now re-interpret (2.2) as a fibre square of the form

(3.11)

$$\begin{tikzcd}
\mathbb{Z}[G(p,q)] \arrow[r] \arrow[d] & \mathcal{T}_q(A, \pi) \arrow[d] \\
\mathbb{Z}[C_q] \arrow[r] & \mathbb{F}_p[C_q]
\end{tikzcd}$$

We note that $\mathcal{C}_q(I^*_C, \theta)$ is simply another description of the induced module $i_*(I^*_C)$. As $\mathcal{T}_q(A, \pi) \cong \mathcal{C}_q(I^*_C, \theta)$ it follows from (1.2) that:

(3.12) $\quad i_*(I_C) \cong i_*(I^*_C) \cong \mathcal{T}_q(A, \pi).$

Whilst the quasi-triangularity of $\lambda_*(x^{-1})$ is evident by construction, that of $\lambda_*(y^{-1})$ is known only implicitly from (3.7). To complete our account we elicit some explicit information on the form of $\lambda_*(y^{-1})$. For $0 \le k \le q-2$ define

$$U(k) = \mathrm{span}_A\{(\zeta - 1)^r \mid k+1 \le r \le q-1\}$$

and put $U(k) = 0$ for $q - 1 \le k$. Recalling that $(\zeta - 1)^q \in (\pi)$ it is straightforward to check that :

(3.13) $\qquad U(k)U(l) \subset U(k+l+1) + (\pi).$

We now consider the Galois action given by $\Theta(\zeta) = \zeta^a$.

Proposition 3.14 : For each k , $1 \le k \le q-1$ there are elements $\upsilon(k) \in U(k)$ and $\pi(k) \in (\pi)$ such that $\Theta[(\zeta - 1)^k] = a^k(\zeta - 1)^k + \upsilon(k) + \pi(k)$.

Proof : Observe that $\Theta(\zeta - 1) = \Theta(\zeta) - 1 = \zeta^a - 1$ and that

$$\begin{aligned} \zeta^a - 1 &= ((\zeta - 1) + 1)^a - 1 \\ &= a(\zeta - 1) + \sum_{s=2}^{a} \binom{a}{s} (\zeta - 1)^s. \end{aligned}$$

Let $\mathcal{P}(k)$ be the statement for $\Theta[(\zeta - 1)^k]$. Then $\mathcal{P}(1)$ is verified on putting

$$\upsilon(1) = \sum_{s=2}^{a} \binom{a}{s} (\zeta - 1)^s \ \text{ and } \ \pi(1) = 0.$$

Suppose $\mathcal{P}(r)$ is true for $1 \le r \le k$ where $k < q-1$. As Θ is a ring homomorphism then

$$\begin{aligned}\Theta[(\zeta-1)^{k+1}] \;&=\; \Theta(\zeta-1)\cdot\Theta[(\zeta-1)^{k}]\\ &=\; [a(\zeta-1)+\upsilon(1)]\cdot\left[a^{k}(\zeta-1)^{k}+\upsilon(k)+\pi(k)\right]\\ &=\; a^{k+1}(\zeta-1)^{k+1} \;+\; \Upsilon \;+\; \Psi\end{aligned}$$

where $$\begin{cases}\Upsilon \;=\; a^{k}\upsilon(1)(\zeta-1)^{k}+a(\zeta-1)\upsilon(k)+\upsilon(1)\upsilon(k)\\ \Psi \;=\; [a(\zeta-1)+\upsilon(1)]\,\pi(k).\end{cases}$$

Clearly $\Psi\in(\pi)$ whilst $\Upsilon\in U(k+1)\;+\;(\pi)$ by (3.13). Thus for some $\upsilon(k+1)\in U(k+1)$ and $\pi(k+1)\in(\pi)$ we have

$$\Upsilon+\Psi \;=\; \upsilon(k+1) \;+\; \pi(k+1).$$

Hence $\Theta[(\zeta-1)^{k+1}] \;=\; a^{k+1}(\zeta-1)^{k+1}+\upsilon(k+1)+\pi(k+1)$ verifying $\mathcal{P}(k+1)$. $\square$

Any $Y\in M_q(A,\pi)$ can be written uniquely as a sum

(3.15) $$Y \;=\; \Delta(Y) \;+\; U(Y) \;+\; L(Y)$$

where $\Delta(Y)$ is diagonal, $U(Y)$ is strictly upper triangular and $L(Y)$ is strictly lower triangular. Moreover, as $Y\in\mathcal{T}_q(A,\pi)$ then $L(Y)\;=\pi L'(Y)$ for some strictly lower triangular matrix $L'(Y)$. If $\mu_0,\mu_1,\cdots\mu_{q-1}\in A$ we denote by $\Delta(\mu_{q-1},\dots,\mu_0)$ the diagonal $q\times q$ matrix

$$\Delta(\mu_{q-1},\dots,\mu_0) \;=\; \begin{pmatrix}\mu_{q-1} & & & & \\ & \mu_{q-2} & & & \\ & & \ddots & & \\ & & & \mu_1 & \\ & & & & \mu_0\end{pmatrix}$$

It follows from (3.15) that, with respect to the basis $\{(\zeta-1)^{q-k}\}_{1\le k\le q}$for I_C^*, the matrix $M(\Theta)$ of Θ takes the form $M(\Theta) \;=\; \Delta(a^{q-1},a^{q-2},\dots,a,1)\;+\;U\;+\;\Pi$ where U is a strictly upper triangular and $\Pi\;=\;\pi\cdot X$ for some $X\in M_q(A)$. Let $X\;=\;\Delta'+U'+L'$ be the decomposition of X given in (3.15) and write $\Delta'\;=\;\Delta(\xi_{q-1},\xi_{q-2},\dots,\xi_1,\xi_0)$ for some $\xi_i\in A$. Writing $U(\Theta)\;=\;U+\pi U'$ and $L(\Theta)\;=\pi L'$ we see that with respect to the basis $\{(\zeta-1)^{q-k}\}_{1\le k\le q}$ for I_C^*, the matrix $M(\Theta)$ takes the form

(3.16) $$M(\Theta) \;=\; \Delta(a^{q-1}+\pi\xi_{q-1},\, a^{q-2}+\pi\xi_{q-2},\dots,a+\pi\xi_1,\, 1+\pi\xi_0) \;+\; U(\Theta) \;+\; L(\Theta)$$

where $U(\Theta)$ is strictly upper triangular and $L(\Theta)$ is strictly lower triangular. Denoting by $\overline{M}(\Theta)$ the reduction of $M(\Theta)$ mod π we see that:

$$\overline{M}(\theta) \;=\; \begin{pmatrix}a^{q-1} & * & * & * & * & *\\ & a^{q-2} & * & * & * & *\\ & & \ddots & & & \\ & & & & a^{1} & *\\ & & & & & 1\end{pmatrix}.$$

As $a^{-r} \ = \ a^{q-r} \mod q$ then:

$$\overline{M}(\theta^{-1}) \ = \ \begin{pmatrix} a & * & * & * & * & * \\ & a^2 & * & * & * & * \\ & & & \ddots & & \\ & & & & a^{q-1} & * \\ & & & & & 1 \end{pmatrix}. \tag{3.17}$$

§4 : Properties of the modules $R(i)$:

We decompose $\mathcal{T}_q(A,\pi)$ as direct sum of right Λ-modules thus

$$\mathcal{T}_q(A,\pi) \ \cong \ R(1) \oplus R(2) \oplus \cdots \oplus R(q) \tag{4.1}$$

where $R(i)$ is the i^{th} row of $\mathcal{T}_q(A,\pi)$. Each $R(i)$ is free over A with $\mathrm{rk}_A(R(i)) \ = \ q$. However there is an isomorphism

$$\mathcal{T}_q(A,\pi) \otimes_A A/\pi \ \ \cong \ \ \mathcal{T}_q(A/\pi) \tag{4.2}$$

under which $R(i)$ descends to $\breve{R}(i)$, the i^{th}-row of $\mathcal{T}_q(A/\pi)$. The modules $\breve{R}(i)$ are pairwise isomorphically distinct over $\mathcal{T}_q(A/\pi)$ as $\mathrm{rk}_{A/\pi}[\breve{R}(i)] \ = \ q+1-i$. Hence:

$$R(i) \ \cong_\Lambda \ R(j) \ \iff \ i \ = \ j. \tag{4.3}$$

We proceed to study the duality properties of the $R(i)$. Fix the following notation

$$\mathcal{T}_q \ = \ \mathcal{T}_q(A,\pi) \quad ; \quad R(i) \ = \ i^{th} \text{ row of } \mathcal{T}_q \quad ; \quad C(j) \ = \ j^{th} \text{ column of } \mathcal{T}_q.$$

Then $R(i)$, $C(j)$ are respectively right and left ideals in $\mathcal{T}_q$. Define $Q = (q_{ij}) \in M_q(A)$ by

$$q_{ij} \ = \ \begin{cases} 1 & i+j \ = \ q+1 \\ & \\ 0 & \text{otherwise} \end{cases}$$

Clearly $Q \ = \ Q^t \ = \ Q^{-1}$. Define $\theta : \mathcal{T}_q \to \mathcal{T}_q$ by $\theta(A) \ = \ QA^tQ$. Then θ is an anti-involution on $\mathcal{T}_q$ which takes a left ideal J to a right ideal $\theta(J)$; in particular:

(4.4) $\theta(C(k)) \ = \ R(q+1-k)$.

If M is a right $\mathcal{T}_q$-module then $\mathrm{Hom}_{\mathcal{T}_q}(M, \mathcal{T}_q)$ is a left $\mathcal{T}_q$-module. In particular:

(4.5) $\mathrm{Hom}_{\mathcal{T}_q}(R(k), \mathcal{T}_q) \cong C(k)$.

We use θ to convert a left $\mathcal{T}_q$-module M to a right $\mathcal{T}_q$-module ${}^{\theta}M$ by means of

$$m * \alpha \ = \ \theta(\alpha)m$$

where $m \in M$ and $\alpha \in \mathcal{T}_q$. Note that if J is a left ideal in $\mathcal{T}_q$ then $\theta(J)$ is a right ideal in $\mathcal{T}_q$; moreover, we see that θ induces an isomorphism of right $\mathcal{T}_q$-modules

$$\theta : \ {}^{\theta}J \ \xrightarrow{\simeq} \ \theta(J).$$

If M is a right module its *dual module* M^*, defined by $M^* \ = \ {}^{\theta}\mathrm{Hom}_{\mathcal{T}_q}(M, \mathcal{T}_q)$, is also a right module. It follows from (4.4) and (4.5) that:

(4.6) $R(k)^* \cong \ R(q+1-k)$.

Choose $\overline{a} \in \{1, 2, \ldots, p-1\}$ to satisfy $\theta(x) \ = \ x^{\overline{a}} \ (= \ \ yxy^{-1})$. Then $y^q - 1$ factorises completely over $\mathbb{F}_p$ as $y^q - 1 \ = \ (y-1)(y-\overline{a})(y-\overline{a}^2)\ldots(y-\overline{a}^{q-1})$. Hence

(4.7) $$\mathbb{F}_p[C_q] \;\cong\; \mathbb{F}_p(\overline{a}) \times \mathbb{F}_p(\overline{a}^2) \times \cdots \times \mathbb{F}_p(\overline{a}^{q-1}) \times \mathbb{F}_p(1)$$

where $\mathbb{F}_p(\overline{a}^k)$ is the 1-dimensional $\mathbb{F}_p[C_q]$-module on which y acts by $y \cdot \mathbf{z} \;=\; \overline{a}^k\mathbf{z}$..

Proposition 4.8: There is an exact sequence $0 \to R(1) \hookrightarrow R(q) \to \mathbb{F}_p(1) \to 0$.

Proof : Consider the $q \times q$ matrix $\Gamma \;=\; \lambda(x^{-1} - 1)$ so that

$$\Gamma \;=\; \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ \pi & 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

Then $\Gamma^q \;=\; \pi \cdot \mathrm{I}_q$. Define $\Gamma_* : \mathcal{T}_q(A,\pi) \to \mathcal{T}_q(A,\pi)$ by $\Gamma_*(\beta) \;=\; \Gamma \cdot \beta$. Then Γ_* is a homomorphism of right $\mathcal{T}_q(A,\pi)$ modules and is evidently injective as π is a nonzero element of the integral domain I_C^*. Write a typical element $\beta \in R(1)$ as

$$\beta \;=\; \begin{pmatrix} b_1 & b_2 & \dots & b_{q-1} & b_q \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix} \quad \text{so that} \quad \Gamma_*(\beta) \;=\; \begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \pi b_1 & \pi b_2 & \dots & \pi b_{q-1} & \pi b_q \end{pmatrix}.$$

Thus $R(1) \;\cong\; \Gamma_*(R(1)) \;\subset\; R(q)$. However, a typical element $\gamma \in R(q)$ has the form

$$\gamma \;=\; \begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 \\ \pi c_1 & \pi c_2 & \dots & \pi c_{q-1} & c_q \end{pmatrix} \;\in\; R(q)$$

which differs from an element of $\Gamma_*(R(1))$ only in the $(q,q)^{th}$ entry. As abelian groups, $R(q)/\Gamma_*(R(1)) \;\cong\; A/\pi \;\cong\; \mathbb{F}_p$. Finally, from the form of $\lambda(y^{-1}) \in \mathcal{T}_q(A/\pi)$,

$$\lambda(y^{-1}) \;=\; \begin{pmatrix} \overline{a} & * & * & * & * & * \\ & \overline{a}^2 & * & * & * & * \\ & & \overline{a}^3 & * & * & * \\ & & & \ddots & & \\ & & & & \overline{a}^{q-1} & * \\ & & & & & 1 \end{pmatrix}$$

y acts *trivially* on the *right* of the $(q,q)^{th}$ entry. Thus, $R(q)/\Gamma_*(R(1)) \;\cong_\Lambda\; \mathbb{F}_p(1)$. Hence, as claimed, we have an exact sequence of Λ-modules $0 \to R(1) \overset{\Gamma_*}{\hookrightarrow} R(q) \to \mathbb{F}_p(1) \to 0$. □

In the remaining cases we have :

Proposition 4.9: For $1 \leq k \leq q-1$ there are exact sequences of Λ-modules

$$0 \to R(k+1) \hookrightarrow R(k) \to \mathbb{F}_p(\overline{a}^k) \to 0.$$

Proof : First note that $\quad \Gamma_*(R(k+1)) \ \subset \ R(k) \quad$ for $\ 1 \leq k \leq q-1$.

To make this statement precise consider a typical element

$$\beta \ = \ \begin{pmatrix} 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \pi b_1 & \dots & \pi b_{k-1} & \pi b_k & b_{k+1} & b_{k+2} & \dots & b_q \\ \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix} \ \in \ R(k+1).$$

Then

$$\Gamma_*(\beta) \ = \ \begin{pmatrix} 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \pi b_1 & \dots & \pi b_{k-1} & \pi b_k & b_{k+1} & b_{k+2} & \dots & b_q \\ 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix} \ \in \ R(k).$$

Thus $R(k+1) \ \cong \ \Gamma_*(R(k+1)) \ \subset \ R(k)$. A typical element $\gamma \in R(k)$ has the form

$$\gamma \ = \ \begin{pmatrix} 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \pi c_1 & \dots & \pi c_{k-1} & c_k & c_{k+1} & c_{k+2} & \dots & c_q \\ 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix} \ \in \ R(k)$$

which differs from a typical element of $\Gamma_*(R(k+1))$ only in the $(k,k)^{th}$ entry, showing that, as abelian groups, $R(k)/\Gamma_*(R(k+1)) \ \cong \ A/\pi \ \cong \ \mathbb{F}_p$. Finally, from (3.17) the reduction $\lambda(y^{-1}) \in \mathcal{T}_q(A/\pi)$ takes the form

$$\lambda(y^{-1}) \ = \ \begin{pmatrix} \overline{a} & * & * & * & * & * & * & * & * \\ & \overline{a}^2 & * & * & * & * & * & * & * \\ & & \ddots & & & & & & \\ & & & & \overline{a}^k & * & * & * & * \\ & & & & & & \ddots & & \\ & & & & & & & \overline{a}^{q-1} & * \\ & & & & & & & & 1 \end{pmatrix}$$

Hence in the *right action* in the quotient, y acts on the $(k,k)^{th}$ entry as multiplication by $\overline{a}^k$. Thus, as Λ-modules, $R(k)/\Gamma_*(R(k+1)) \cong \mathbb{F}_p(\overline{a}^k)$ so, as claimed, we get an exact sequence $0 \to R(k+1) \overset{\Gamma_*}{\hookrightarrow} R(k) \to \mathbb{F}_p(\overline{a}^k) \to 0$. □

It is useful to describe $R(1)$ and $R(q)$ as Galois modules. One first checks that $R(q)$ satisfies conditions (i), (ii) and (iii) of (1.4). In particular $\mu = (0, 0, \ldots, 0, 1) \in R(q)$ satisfies $\mu \cdot y = \mu$. Thus it follows from (1.4) that:

Proposition 4.10 : $R(q) \cong \overline{I_C^*}$.

It is straightforward to see that $\overline{I_C^*} \cong (\overline{I_C})^*$. From (4.6) and (4.10) it follows that:

(4.11) $R(1) \cong \overline{I_C}$.

§5: Decomposing the augmentation ideal of Λ :

The collection $\{E_r\}_{1 \le r \le pq-1}$ is an integral basis for I_G where

$$\left\{ \begin{array}{lcll} E_{(k-1)p+s} & = & y^k x^s - 1 & \text{for } 1 \le k \le q-1 \quad \text{and} \quad 1 \le s \le p. \\ E_{(q-1)p+s} & = & x^s - 1 & \text{for } 1 \le s \le p-1. \end{array} \right.$$

Make the change of basis to $\{\Phi_r\}_{1 \le r \le pq-1}$ where

$$\left\{ \begin{array}{lcll} \Phi_{(k-1)p+s} & = & E_{(k-1)p+s} - E_{(q-1)p+s} & \text{for } 1 \le k \le q-1 \quad \text{and} \quad 1 \le s \le p-1; \\ \Phi_{kp} & = & E_{kp} & \text{for } 1 \le k \le q-1; \\ \Phi_{(q-1)p+s} & = & E_{(q-1)p+s} & \text{for } 1 \le s \le p-1. \end{array} \right.$$

Then $\{\Phi_r\}_{1 \le r \le p(q-1)}$ is an integral basis for the right ideal $[y-1)$ as

$$\left\{ \begin{array}{lcll} \Phi_{(k-1)p+s} & = & (y^k - 1)x^s & \text{for } 1 \le k \le q-1 \quad \text{and} \quad 1 \le s \le p-1 \\ \Phi_{kp} & = & y^k - 1 & \text{for } 1 \le k \le q-1. \end{array} \right.$$

As this extends to an integral basis for I_G is follows that $I_G/[y-1)$ is free over $\mathbb{Z}$. Moreover if $\natural : I_G \to I_G/[y-1)$ is the identification map then

(5.1) $\natural(\Phi_{(q-1)p+s})_{1 \le s \le p-1}$ is an integral basis for $I_G/[y-1)$.

However $\natural(\Phi_{(q-1)p+s}) = \natural(x^s - 1)$ from which we see easily that $I_G/[y-1)$ is isomorphic to I_C as a module over $\mathbb{Z}[C_p]$. Computing the action of y^{-1} on I_G we find

$$\begin{array}{rcl} (x^s - 1) \cdot y^{-1} & = & x^s y^{-1} - y^{-1} \\ & = & y^{q-1}(x^{\theta_*(s)} - 1) \\ & = & (y^{q-1} - 1)(x^{\theta_*(s)} - 1) \; + \; (x^{\theta_*(s)} - 1) \end{array}$$

Write $X^s - 1 = \natural(x^s - 1)$ so that $(X^s - 1)_{1 \le s \le p-1}$ is an integral basis for $I_G/[y-1)$. Observing that $(y^{q-1} - 1)(x^{\theta_*(s)} - 1) \in [y-1)$ the above calculation thereby shows

$$(X^s - 1) \cdot y^{-1} = X^{\theta_*(s)} - 1$$

which coincides with the Galois action on $\overline{I_C}$. Thus $I_G/[y-1] \cong \overline{I_C}$ and we have shown

(5.2) There exists an exact sequence $0 \to [y-1) \to I_G \to \overline{I_C} \to 0$.

We proceed to show that the exact sequence of (5.2) splits. To economise on notation we use boldface symbols **Hom**, $\mathbf{Ext}^k$ when describing homomorphisms and extensions of Λ-modules and standard Roman font, Hom and Ext^k, when referring to homomorphisms and extensions of modules over $\mathbb{Z}[C_p]$. First note that

$$\textbf{(5.3)} \qquad \mathrm{Ext}^k(\mathbb{Z}, I_C) \qquad \cong \qquad \begin{cases} \mathbb{Z}/p & k=1 \\ \\ 0 & k=2. \end{cases}$$

Any $\mathbb{Z}[C_q]$-module becomes a module over Λ via the projection $\Lambda \to \mathbb{Z}[C_q]$. Thus:

Proposition 5.4: $\mathbf{Ext}^1(\mathbb{Z}[C_q], R(k)) \cong \mathbb{Z}/p$ for all k $(1 \le k \le q)$.

Proof : Let i denote the inclusion $i : \mathbb{Z}[C_p] \hookrightarrow \Lambda$. Applying the induced representation functor i_* to the exact sequence $0 \to I_C \to \mathbb{Z}[C_p] \to \mathbb{Z} \to 0$ gives an exact sequence

$$\textbf{(*)} \qquad 0 \to i_*(I_C) \to \Lambda \to \mathbb{Z}[C_q] \to 0.$$

Now $i_*(I_C) \cong \bigoplus_{t=1}^q R(t)$ so that **(*)** can be re-written as an extension

$$\textbf{(**)} \qquad 0 \to \bigoplus_{t=1}^q R(t) \to \Lambda \to \mathbb{Z}[C_q] \to 0$$

which is classified by cohomology classes $c = (c_t)_{1 \le t \le q}$ where $c_t \in \mathbf{Ext}^1(\mathbb{Z}[C_q], R(t))$. If $\mathbf{Ext}^1(\mathbb{Z}[C_q], R(k)) = 0$ then Λ decomposes as a direct sum $\Lambda \cong R(k) \oplus X$ where the module X occurs in the extension

$$0 \to \bigoplus_{t \ne k} R(t) \to X \to \mathbb{Z}[C_q] \to 0$$

classified by the sequence $(c_t)_{t \ne k}$. However Λ, being the integral group ring of a finite group, is indecomposable (cf [4] p.678). Consequently each $c_k \ne 0$ and hence each $\mathbf{Ext}^1(\mathbb{Z}[C_q], R(k)) \ne 0$. Now note that $i^*(\mathbb{Z}[C_q]) \cong \mathbb{Z}^q$; from the Eckmann-Shapiro isomorphism $\mathbf{Ext}^1(\mathbb{Z}[C_q], i_*(I_C)) \cong \mathrm{Ext}^1(i^*(\mathbb{Z}[C_q]), I_C)$ and (5.3) we see that

$$\mathbf{Ext}^1(\mathbb{Z}[C_q], i_*(I_C)) \cong \mathrm{Ext}^1(\mathbb{Z}, I_C)^q \cong \underbrace{\mathbb{Z}/p \oplus \cdots \oplus \mathbb{Z}/p}_{q}.$$

As above, $i_*(I_C) \cong \bigoplus_{k=1}^q R(k)$. Hence $\bigoplus_{k=1}^q \mathbf{Ext}^1(\mathbb{Z}[C_q], R(k)) \cong \underbrace{\mathbb{Z}/p \oplus \cdots \oplus \mathbb{Z}/p}_{q}$. As $\mathbf{Ext}^1(\mathbb{Z}[C_q], R(k)) \ne 0$ then each $\mathbf{Ext}^1(\mathbb{Z}[C_q], R(k)) \cong \mathbb{Z}/p$ as claimed. □

From the Eckmann-Shapiro isomorphism $\mathbf{Ext}^2(\mathbb{Z}, i_*(I_C)) \cong \mathrm{Ext}^2(\mathbb{Z}, I_C)$ we see from (5.3) that $\mathbf{Ext}^2(\mathbb{Z}, i_*(I_C)) = 0$. However

$$\bigoplus_{k=1}^q \mathbf{Ext}^2(\mathbb{Z}, R(k)) \cong \mathbf{Ext}^2(\mathbb{Z}, \bigoplus_{k=1}^q R(k)) \cong \mathbf{Ext}^2(\mathbb{Z}, i_*(I_C))$$

from which it follows that:

$$\textbf{(5.5)} \qquad \mathbf{Ext}^2(\mathbb{Z}, R(k)) = 0 \quad \text{for all } k \quad (1 \le k \le q).$$

Now $\mathrm{Hom}(i^*(I_Q), I_C) \cong \mathrm{Hom}(\mathbb{Z}, I_C)^{(q)} = 0$. From the Eckmann-Shapiro isomorphism

$\mathbf{Hom}(I_Q, i_*(I_C)) \cong \mathrm{Hom}(i^*(I_Q), I_C)$ we see that $\mathbf{Hom}(I_Q, i_*(I_C)) \cong 0$. Hence

(5.6) $\mathbf{Hom}(I_Q, R(k)) = 0$ for all k $(1 \le k \le q)$.

As $\mathbb{Z}[C_p]$ is indecomposable, from the exact sequence $0 \to \overline{I_C} \to \overline{\mathbb{Z}[C_p]} \to \mathbb{Z} \to 0$ it follows that $\mathbf{Ext}^1(\mathbb{Z}, \overline{I_C})) \neq 0$. As $\overline{I_C} \cong R(1)$ then $\mathbf{Ext}^1(\mathbb{Z}, R(1)) \neq 0$. However, $\mathbf{Ext}^1(\mathbb{Z}, i_*(I_C)) \cong \mathrm{Ext}^1(i^*(\mathbb{Z}), I_C) \cong \mathrm{Ext}^1(\mathbb{Z}, I_C) \cong \mathbb{Z}/p$ so that

$$\bigoplus_{k=1}^{q} \mathbf{Ext}^1(\mathbb{Z}, R(k)) \cong \mathbb{Z}/p.$$

As $\mathbf{Ext}^1(\mathbb{Z}, R(1)) \neq 0$ it follows that:

$$\textbf{(5.7)} \qquad \mathbf{Ext}^1(\mathbb{Z}, R(k)) \cong \begin{cases} \mathbb{Z}/p & k = 1 \\ 0 & k \neq 1. \end{cases}$$

Applying $\mathbf{Hom}(-, R(k))$ to the exact sequence $0 \to I_Q \to \mathbb{Z}[C_q] \to \mathbb{Z} \to 0$ we obtain a long exact sequence in cohomology, from which, in conjunction with (5.4), (5.5) and (5.6), we extract the following portion:

$$\begin{tikzcd}
\mathbf{Hom}(I_Q, R(k)) \arrow[r] \arrow[d, equal] & \mathbf{Ext}^1(\mathbb{Z}, R(k)) \arrow[r] \arrow[d, equal] & \mathbf{Ext}^1(\mathbb{Z}[C_q], R(k)) \arrow[r] \arrow[d, equal] & \mathbf{Ext}^1(I_Q, R(k)) \arrow[r] \arrow[d, equal] & \mathbf{Ext}^2(\mathbb{Z}, R(k)) \arrow[d, equal] \\
0 \arrow[r] & \mathbf{Ext}^1(\mathbb{Z}, R(k)) \arrow[r] & \mathbb{Z}/p \arrow[r] & \mathbf{Ext}^1(I_Q, R(k)) \arrow[r] & 0.
\end{tikzcd}$$

In the case $k = 1$ then $\mathbf{Ext}^1(\mathbb{Z}, R(1)) \cong \mathbb{Z}/p$ so that $\mathbf{Ext}^1(I_Q, R(1)) = 0$ whilst if $k \neq 1$ then $\mathbf{Ext}^1(\mathbb{Z}, R(k)) = 0$ so that $\mathbf{Ext}^1(I_Q, R(k)) \cong \mathbb{Z}/p$; that is:

$$\textbf{(5.8)} \qquad \mathbf{Ext}^1(I_Q, R(k)) \cong \begin{cases} 0 & k = 1 \\ \mathbb{Z}/p & k \neq 1. \end{cases}$$

Theorem 5.9 : I_G decomposes as a direct sum $I_G \cong \overline{I_C} \oplus Y$ for some Λ-module Y.

Proof : First consider the exact sequence $0 \to I_C \to \mathbb{Z}[C_p] \to \mathbb{Z} \to 0$. By taking induced representations we obtain an exact sequence $0 \to i_*(I_C) \longrightarrow \Lambda \xrightarrow{p} \mathbb{Z}[C_q] \to 0$. As $i_*(I_C) \cong \bigoplus_{k=1}^{q} R(k)$ and $p^{-1}(I_Q) = I_G$ we obtain an exact sequence

$$0 \longrightarrow \bigoplus_{k=1}^{q} R(k) \longrightarrow I_G \xrightarrow{p} I_Q \longrightarrow 0$$

classified by a sequence of cohomology classes $\mathbf{c} = (c_1, c_2, \dots, c_q)$ where $c_k \in \mathbf{Ext}^1(I_Q, R(k))$. As $c_1 \in \mathbf{Ext}^1(I_Q, R(1)) = 0$ then $I_G \cong R(1) \oplus Y$ where Y is given as the extension

$$0 \longrightarrow \bigoplus_{k \neq 1} R(k) \longrightarrow Y \xrightarrow{p} I_Q \longrightarrow 0$$

classified by $(c_2, \dots, c_q)$. The conclusion follows as $R(1) \cong \overline{I_C}$. □

As above we continue to use boldface symbols **Hom**, $\mathbf{Ext}^a$ when describing homomorphisms and extensions of Λ-modules but we now use italics *Hom*, Ext^a when referring to homomorphisms and extensions of modules over $\mathbb{Z}[C_q]$. Let $j : \mathbb{Z}[C_q] \hookrightarrow \Lambda$ denote the inclusion; we note that $[y-1) = j_*(I_Q)$ and $j^*(\overline{I_C}) \cong \mathbb{Z}^{p-1}$; thus $\mathbf{Hom}([y-1), \overline{I_C})) \cong \mathit{Hom}(I_Q, \mathbb{Z}^{p-1})$ However $\mathit{Hom}(I_Q, \mathbb{Z}) = 0$ so that we have:

(5.10) $\mathbf{Hom}([y-1), \overline{I_C})) \;=\; 0$

Corollary 5.11: The exact sequence of (5.2) splits.

Proof : It suffices to construct a right splitting of (5.2); that is, a Λ-homomorphism $s : I_G/[y-1) \to I_G$ such that $\natural \circ s \;=\; \mathrm{Id}$ where, as above, $\natural : I_G \to I_G/[y-1)$ is the identification map. We first show that the isomorphism $I_G \;\cong\; Y \;\oplus\; \overline{I_C}$ of (5.9) implies that $Y \cong [y-1)$. Thus let $\varphi : I_G \to Y \oplus \overline{I_C}$ be the isomorphism of (5.9) and let ψ denote the projection $\psi : \;\; [y-1) \;\oplus\; \overline{I_C} \;\to\; \overline{I_C}$. The restriction $\psi \circ \varphi_{|\,[y-1)} : [y-1) \to \overline{I_C}$ is necessarily zero by (5.10). Hence φ restricts to an injection

$$\varphi_{|\,[y-1)} : [y-1) \;\to\; Y$$

and induces an isomorphism $\varphi_* : I_G/[y-1) \to (Y/\varphi([y-1)) \oplus \overline{I_C}$. Clearly we have $\mathrm{rk}_{\mathbb{Z}}([y-1)) \;=\; \mathrm{rk}_{\mathbb{Z}}(Y)) \;=\; p(q-1)$, from which it follows that $Y/\varphi([y-1))$ is finite. However, $I_G/[y-1)$ is torsion free so that $Y/\varphi([y-1)) \;=\; 0$ and $\varphi : [y-1) \xrightarrow{\simeq} Y$ is the required isomorphism. Consequently $[y-1) \oplus \overline{I_C} \;\cong\; I_G$. As $\overline{I_C} \;\cong\; I_G/[y-1)$ it follows that there is an isomorphism $h : [y-1) \;\oplus\; I_G/[y-1) \to I_G$. As $\mathrm{Coker}(\natural) \cong \overline{I_C}$, it follows, again from (5.10), that $h([y-1)) \subset \mathrm{Ker}(\natural) \;=\; [y-1)$. As h injective then $\mathrm{Ker}(\natural)/h([y-1))$ is finite. However, the quotient $\left([y-1) \;\oplus\; I_G/[y-1)\right)/[y-1) \;\;\cong\;\; \overline{I_C}$ is torsion free, so that $h([y-1)) \;=\; \mathrm{Ker}(\natural)$. Thus I_G decomposes as the internal direct sum $I_G \;=\; \mathrm{Ker}(\natural) \;\dot{+}\; h(I_G/[y-1))$. Take σ to be the restriction of $\natural \circ h$ to $I_G/[y-1)$. Then $\sigma \;=\; \natural \circ h : I_G/[y-1) \xrightarrow{\simeq} I_G/[y-1)$ is an isomorphism and $s = h \circ \sigma^{-1} : I_G/[y-1) \to I_G$ is the required right splitting of (5.2). □

Corollary 5.12: I_G decomposes as a direct sum $I_G \;\cong\; [y-1) \oplus \overline{I_C}$.

§6 : Proof of Theorem C :

It follows from (5.12) that there is an exact sequence $0 \to \overline{I_C} \oplus [y-1) \to \Lambda \to \mathbb{Z} \to 0$. Applying $\overline{I^*_C} \otimes -$ we obtain an exact sequence

$$0 \to\; (\overline{I^*_C} \otimes \overline{I_C}) \oplus (\overline{I^*_C} \otimes [y-1)) \;\to\; \overline{I^*_C} \otimes \Lambda \;\to\; \overline{I^*_C} \otimes \mathbb{Z} \;\to 0$$

which, by (1.10), (1.11) we may write more conveniently as

(6.1) $$0 \to\;\; (\overline{I^*_C} \otimes \overline{I_C}) \oplus \Lambda^{d(q-1)} \;\;\to\;\; \Lambda^{p-1} \;\;\to\;\; \overline{I^*_C} \;\;\to 0.$$

As $\Lambda^{d(q-1)}$ and $\overline{I^*_C} \otimes \overline{I_C}$ are self-dual, then dualisation of (6.1) gives an exact sequence

(6.2) $$0 \to \overline{I_C} \;\;\to \Lambda^{p-1} \;\;\to\;\; (\overline{I^*_C} \otimes \overline{I_C}) \oplus \Lambda^{d(q-1)} \;\;\to 0.$$

Splicing (6.1) and (6.2) together gives an exact sequence

(6.3) $$0 \to \overline{I_C} \longrightarrow \Lambda^{(p-1)} \longrightarrow \Lambda^{(p-1)} \longrightarrow \overline{I^*_C} \to 0$$

However, $\overline{I^*_C}$ is monogenic and finitely presented so there is an exact sequence

(6.4) $$0 \to K \longrightarrow \Lambda^b \longrightarrow \Lambda \longrightarrow \overline{I^*_C} \to 0$$

Comparison of (6.3) and (6.4) via the generalised form of Schanuel's Lemma (cf [21]) gives

(6.5) $$\overline{I_C} \oplus \Lambda^{p+b-1} \;\;\cong\;\; K \oplus \Lambda^p$$

We may modify (6.4) successively, first to an exact sequence

(6.6) $$0 \to K \oplus \Lambda^p \longrightarrow \Lambda^{p+b} \longrightarrow \Lambda \longrightarrow \overline{I^*_C} \to 0$$

Then, using (6.5), to an exact sequence

(6.7) $$0 \to \overline{I_C} \oplus \Lambda^{p+b-1} \xrightarrow{j} \Lambda^{p+b} \longrightarrow \Lambda \longrightarrow \overline{I_C^*} \to 0$$

Finally to an exact sequence

(6.8) $$0 \to \overline{I_C} \longrightarrow S \longrightarrow \Lambda \longrightarrow \overline{I_C^*} \to 0$$

where $S = \Lambda^{p+b}/j(\Lambda^{p+b-1})$. It follows from the 'de-stabilisation theorem' of [9] (Prop. 5.17, p. 97) that S is projective. Moreover, from the exact sequence

$$0 \to \Lambda^{p+b-1} \xrightarrow{j} \Lambda^{p+b} \to S \to 0$$

we see that $S \oplus \Lambda^{p+b-1} \cong \Lambda^{p+b}$. That is, S is stably free of rank 1. However, Λ satisfies the Eichler condition so that, by the Swan-Jacobinski Theorem ([5] §51),

$$S \cong \Lambda.$$

Substitution of $S \cong \Lambda$ back into (6.8) gives the required basic sequence for Λ.

(6.9) $$\begin{tikzcd} & & & K(q) \arrow[dr] & & & \\ 0 \arrow[r] & \overline{I_C} \arrow[r] & \Lambda \arrow[ur] \arrow[rr] & & \Lambda \arrow[r, two heads] & \overline{I_C^*} \arrow[r] & 0. \end{tikzcd}$$

where $K(q)$ is the kernel of the surjection $\Lambda \twoheadrightarrow \overline{I_C^*}$, so proving Theorem C. □

§7: Some cohomological considerations :

We continue to write $\mathbf{Ext}^a$ (resp. Ext^a) when referring to extensions of modules over Λ (resp. $\mathbb{Z}[C_p]$). Observe that $i_*(I_C^*) \cong \mathcal{T}_q \cong \bigoplus_{r=1}^q R(r)$ and $i^*(R(r)) \cong I_C^*$. From the first Eckmann-Shapiro relation we obtain:

$$\begin{aligned} \mathbf{Ext}^2(\mathcal{T}_q, \mathcal{T}_q) &\cong \bigoplus_{r=1}^{q} \mathbf{Ext}^2(i_*(I_C^*), R(r)) \\ &\cong \bigoplus_{r=1}^{q} \mathrm{Ext}^2(I_C^*, i^*(R(r)) \\ &\cong \bigoplus_{r=1}^{q} \mathrm{Ext}^2(I_C^*, I_C^*) \end{aligned}$$

Noting that $\mathrm{Ext}^2(I_C^*, I_C^*) \cong \mathbb{Z}/p$ then $\mathbf{Ext}^2(\mathcal{T}_q, \mathcal{T}_q) \cong \underbrace{\mathbb{Z}/p \oplus \cdots \oplus \mathbb{Z}/p}_{q}.$ Likewise from the second Eckmann-Shapiro relation we deduce that

$$\begin{aligned} \mathbf{Ext}^2(R(r), \mathcal{T}_q) &\cong \mathbf{Ext}^2(R(r), i_*(I_C^*) \\ &\cong \mathrm{Ext}^2(i^*(R(r), I_C^*) \\ &\cong \mathrm{Ext}^2(I_C^*, I_C^*). \end{aligned}$$

Hence we see that $\mathbf{Ext}^2(R(r), \mathcal{T}_q) \cong \mathbb{Z}/p.$ Writing $\mathcal{T}_q \cong \bigoplus_{s=1}^q R(s)$ we have $\displaystyle\bigoplus_{s=1}^{q} \mathbf{Ext}^2(R(r), R(s)) \cong \mathbb{Z}/p$. As $\mathbb{Z}/p$ is indecomposable then for each $r \in \{1, \ldots, q\}$ there exists $\sigma(r) \in \{1, \ldots, q\}$ such that:

(7.1) $$\mathbf{Ext}^2(R(r), R(s)) \cong \begin{cases} \mathbb{Z}/p & s = \sigma(r) \\ 0 & s \neq \sigma(r). \end{cases}$$

The correspondence $i \mapsto \sigma(i)$ evidently defines a mapping $\sigma : \{1, \dots, q\} \to \{1, \dots, q\}$. As $R(1) \cong \overline{I_C}$ and $R(q) \cong \overline{I_C^*}$ it follows from (6.9) that $\sigma(q) = 1$. We claim that the mapping $\sigma : \{1, \dots, q\} \to \{1, \dots, q\}$ is bijective. It suffices to show that σ is surjective. Suppose not; then there exists $k \in \{1, \dots, q\}$ such that for all $i \in \{1, \dots, q\}$ $\mathbf{Ext}^2(R(i), R(k)) = 0$. Thus $\mathbf{Ext}^2(\mathcal{T}_q, R(k)) = \bigoplus_{i=1}^{q} \mathbf{Ext}^2(R(i), R(k)) = 0$. By duality

$$\mathbf{Ext}^2(R(k)^*, \mathcal{T}_q^*) = 0.$$

However, $R(k)^* \cong R(q+1-k)$ and $\mathcal{T}_q^* \cong \mathcal{T}_q \cong \bigoplus_{s=1}^{q} R(s)$ so that, for all $s \in \{1, \dots, q\}$

$$\mathbf{Ext}^2(R(q+1-k), R(s)) = 0.$$

This contradicts (7.1) above. Thus σ is surjective and hence bijective. To summarise:

Proposition 7.2 : There exists a (necessarily unique) permutation σ of $\{1, \dots, q\}$ satisfying $\sigma(q) = 1$ with the property that, for each $i \in \{1, \dots, q\}$,

$$\mathbf{Ext}^2(R(i), R(j)) \cong \begin{cases} \mathbb{Z}/p & j = \sigma(i) \\ 0 & j \neq \sigma(i). \end{cases}$$

Each $R(i)$ is monogenic; hence for each $i \in \{1, \dots, q\}$ there is an exact sequence

$$\mathcal{X}(i) = (0 \to K(i) \to \Lambda \to R(i) \to 0) \tag{7.3}$$

so that, by dimension shifting, $$\mathrm{Ext}^1(K(i), R(j)) \cong \begin{cases} \mathbb{Z}/p & j = \sigma(i) \\ 0 & j \neq \sigma(i). \end{cases}$$

Recall from §1 that $\mathbb{Z}[C_q] \otimes \overline{I_C} \cong i_*(I_C) \cong i_*(I_C^*) \cong \mathbb{Z}[C_q] \otimes \overline{I_C^*}$ and that $\mathbb{Z}[C_q] \otimes \Lambda \cong \Lambda^q$. Applying the functor $\mathbb{Z}[C_q] \otimes -$ to (6.9) gives an exact sequence

$$\begin{tikzcd} & & & K \arrow[dr] & & & \\ 0 \arrow[r] & i_*(I_C) \arrow[r] & \Lambda^q \arrow[ur] \arrow[rr] & & \Lambda^q \arrow[r] & i_*(I_C) \arrow[r] & 0 \end{tikzcd}$$

where $K = \mathbb{Z}[C_q] \otimes K(q)$. By (3.12), $i_*(I_C) \cong \mathcal{T}_q(A, \pi) \cong \bigoplus_{i=1}^{q} R(i)$. Moreover $\bigoplus_{i=1}^{q} R(i) \cong \bigoplus_{i=1}^{q} R(\sigma(i))$ so that we have an exact sequence

$$\begin{tikzcd} & & & K \arrow[dr] & & & \\ 0 \arrow[r] & \bigoplus_{i=1}^{q} R(\sigma(i)) \arrow[r] & \Lambda^q \arrow[ur] \arrow[rr] & & \Lambda^q \arrow[r] & \bigoplus_{i=1}^{q} R(i) \arrow[r] & 0. \end{tikzcd} \tag{7.4}$$

On comparing the portion $0 \to K \to \Lambda^q \to \bigoplus_{i=1}^{q} R(i) \to 0$ of (7.4) with

$$\bigoplus_{i=1}^{q} \mathcal{S}(i) = (0 \to \bigoplus_{i=1}^{q} K(i) \to \Lambda^q \to \bigoplus_{i=1}^{q} R(i) \to 0)$$

it follows from Schanuel's Lemma that $K \oplus \Lambda^q \cong (\bigoplus_{i=1}^{q} K(i)) \oplus \Lambda^q$. We claim

Proposition 7.5 : There exists an exact sequence of the form

$$0 \to \bigoplus_{i=1}^{q} R(\sigma(i)) \to \Lambda^q \to \bigoplus_{i=1}^{q} K(i) \to 0.$$

Proof : Modify the portion $0 \to \bigoplus_{i=1}^{q} R(\sigma(i)) \to \Lambda^q \to K \to 0$ of (7.4) first to $0 \to \bigoplus_{i=1}^{q} R(\sigma(i)) \to \Lambda^q \oplus \Lambda^q \to K \oplus \Lambda^q \to 0$, then, using the other half of (7.4), to

$$0 \to \bigoplus_{i=1}^{q} R(\sigma(i)) \longrightarrow \Lambda^{2q} \longrightarrow (\bigoplus_{i=1}^{q} K(i)) \oplus \Lambda^q \to 0.$$

Dualisation gives $0 \to (\bigoplus_{i=1}^{q} K(i)^*) \oplus \Lambda^q \xrightarrow{\iota} \Lambda^{2q} \longrightarrow \bigoplus_{i=1}^{q} R(\sigma(i))^* \to 0$

which we modify again to $0 \to \bigoplus_{i=1}^{q} K(i)^* \to \Lambda^{2q}/(\iota(\Lambda^q)) \to \bigoplus_{i=1}^{q} R(\sigma(i))^* \to 0$.

Again by the 'de-stabilisation theorem' of [7] we see that $\Lambda^{2q}/(\iota(\Lambda^q)$ is stably free of rank q over Λ. By the Swan-Jacobinski Theorem, $\Lambda^{2q}/(\iota(\Lambda^q) \cong \Lambda^q$ there is an exact sequence

$$0 \to \bigoplus_{i=1}^{q} K(i)^* \longrightarrow \Lambda^q \longrightarrow \bigoplus_{i=1}^{q} R(\sigma(i))^* \to 0.$$

Re-dualisation gives the desired sequence $0 \to \bigoplus_{i=1}^{q} R(\sigma(i)) \to \Lambda^q \to \bigoplus_{i=1}^{q} K(i) \to 0$. □

Theorem 7.6 : For each i there exists an exact sequence

$$\mathcal{W}(i) = (0 \to R(\sigma(i)) \longrightarrow P(i) \longrightarrow K(i) \to 0).$$

in which $P(i)$ is projective of rank 1 over Λ. Moreover, $\bigoplus_{i=1}^{q} P(i) \cong \Lambda^q$.

Proof : Let $[\mathcal{W}]$ denote the congruence class of the extension constructed in (7.5),

$$\mathcal{W} = (0 \to \bigoplus_{j=1}^{q} R(\sigma(j)) \to \Lambda^q \to \bigoplus_{i=1}^{q} K(i) \to 0).$$

Then $[\mathcal{W}] \in \mathrm{Ext}^1(\bigoplus_{i=1}^{q} K(i), \bigoplus_{j=1}^{q} R(\sigma(j))) \cong \bigoplus_{i,j=1}^{q} \mathrm{Ext}^1(K(i), R(\sigma(j)))$. Dimension shifting applied to (7.2) shows that $\mathrm{Ext}^1(K(i), R(j)) = 0$ when $j \neq \sigma(i)$ so that

$$\mathrm{Ext}^1(\bigoplus_{i=1}^{q} K(i), \bigoplus_{j=1}^{q} R(\sigma(j))) \cong \bigoplus_{i=1}^{q} \mathrm{Ext}^1(K(i), R(\sigma(i)))$$

and $\mathcal{W}$ is congruent to a direct sum $\mathcal{W} \approx \mathcal{W}(1) \oplus \cdots \oplus \mathcal{W}(q)$ where $\mathcal{W}(i)$ has the form $\mathcal{W}(i) = (0 \to R(\sigma(i)) \to P(i) \to K(i) \to 0)$. In particular, $\Lambda^q \cong P(1) \oplus \cdots \oplus P(q)$ so that each $P(i)$ is projective. By Swan's 'local freeness' theorem ([4], §32) each $P(i) \otimes \mathbb{Q}$ is free over $\Lambda \otimes \mathbb{Q}$. As each $P(i)$ is nonzero, a straightforward calculation of $\mathbb{Z}$-ranks shows that $\mathrm{rk}_\Lambda(P(i)) = 1$. □

Splicing the exact sequence $\mathcal{X}(i)$ of (7.3) with $\mathcal{W}(i)$ of (7.6) gives an extension

(7.7)

$$\begin{tikzcd} & & & K(i) \arrow[dr] & & & \\ \mathcal{Z}(i) = (\ 0 \arrow[r] & R(\sigma(i)) \arrow[r] & P(i) \arrow[ur] \arrow[rr] & & \Lambda \arrow[r] & R(i) \arrow[r] & 0\ ). \end{tikzcd}$$

For future reference, we note again that $\sigma(q) = 1$ and that $P(q) = \Lambda$ in the basic sequence $\mathcal{Z}(q) = \mathfrak{S}(q)$. We now proceed to determine the permutation σ.

§8 : A p-adic construction :

Denote by $\widehat{\mathbb{Z}}$ the ring of p-adic integers and by $\widehat{\Lambda} = \Lambda \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ the p-adic completion of Λ. For any Λ-lattice M, we denote by $\widehat{M} = M \otimes_\Lambda \widehat{\Lambda}$. the corresponding $\widehat{\Lambda}$-lattice. We have p-adic analogues of (4.8) and (4.9):

(8.1) There is an exact sequence of $\widehat{\Lambda}$-modules $0 \to \widehat{R}(1) \hookrightarrow \widehat{R}(q) \to \mathbb{F}_p(1) \to 0$.

(8.2) For $1 \leq k \leq q-1$ there are exact sequences of $\widehat{\Lambda}$-modules

$$0 \to \widehat{R}(k+1) \hookrightarrow \widehat{R}(k) \to \mathbb{F}_p(\overline{a}^k) \to 0.$$

Let $\natural : \widehat{\mathbb{Z}} \to \mathbb{F}_p$ be the canonical mapping. There exists a q^{th} root of unity $\widehat{a} \in \widehat{\mathbb{Z}}$ such that $\natural(\widehat{a}) = \overline{a}$. so that $\widehat{\lambda}(y^{-1})$ takes the form

$$\widehat{\lambda}(y^{-1}) \;=\; \begin{pmatrix} \widehat{a} & * & * & * & * & * \\ & \widehat{a}^2 & * & * & * & * \\ & & \widehat{a}^3 & * & * & * \\ & & & \ddots & & \\ & & & & \widehat{a}^{q-1} & * \\ & & & & & 1 \end{pmatrix}.$$

Let $\widehat{\mathbb{Z}}(\widehat{a}^k)$ denote the $\widehat{\mathbb{Z}}[C_q]$ module whose underlying $\widehat{\mathbb{Z}}$ module is $\widehat{\mathbb{Z}}$ on which y acts, on the right, as multiplication by $\widehat{a}^k$.

Proposition 8.3 : $\widehat{R}(k+1) \;\cong_{\widehat{\Lambda}}\; \widehat{R}(k) \otimes_{\widehat{\mathbb{Z}}} \widehat{\mathbb{Z}}(\widehat{a})$ for $1 \le k \le q-1$.

Proof : There is a canonical ring homomorphism $\mathcal{T}_q(\widehat{A}, \widehat{\pi}) \to \mathbb{F}_p[C_q]$ whose kernel is the Jacobson radical of $\mathcal{T}_q(\widehat{A}, \widehat{\pi})$. However from the product structure of (4.7) it follows by Rosen's Theorem ([4], [20]) that $\mathcal{T}_q(\widehat{A}, \widehat{\pi})$ decomposes uniquely as a direct sum of ideals

$$\mathcal{T}_q(\widehat{A}, \widehat{\pi}) \;\cong\; \widehat{J}_1 \,\oplus\, \cdots \oplus\, \widehat{J}_q$$

where $\widehat{J}_k / \widehat{J}_k \cap \mathrm{rad}(\mathcal{T}_q(\widehat{A}, \widehat{\pi})) \;\cong\; \mathbb{F}_p[\overline{a}^k]$. However $\mathcal{T}_q(\widehat{A}, \widehat{\pi}) \;\cong\; \widehat{R}(1) \,\oplus\, \cdots \oplus\, \widehat{R}(q)$ and so, by (8.2), $\widehat{R}(k)/\widehat{R}(k) \cap \mathrm{rad}(\mathcal{T}_q(\widehat{A}, \widehat{\pi})) \;\cong\; \mathbb{F}[\overline{a}^k]$ so that $\widehat{J}_k = \widehat{R}(k)$. Now consider the exact sequence $0 \to i_*(\widehat{I}_C) \to \widehat{\Lambda} \to \widehat{\mathbb{Z}}[C_q] \to 0$ and take tensor product $- \otimes \widehat{\mathbb{Z}}[\widehat{a}]$. As $\widehat{\Lambda} \otimes \widehat{\mathbb{Z}}[\widehat{a}] \cong \widehat{\Lambda}$ and $\widehat{\mathbb{Z}}[C_q] \otimes \widehat{\mathbb{Z}}[\widehat{a}] \cong \widehat{\mathbb{Z}}[C_q]$ it follows that $i_*(\widehat{I}_C) \otimes \widehat{\mathbb{Z}}[\widehat{a}] \cong i_*(\widehat{I}_C)$. As in (3.12), $i_*(\widehat{I}_C) \cong \mathcal{T}_q(\widehat{A}, \widehat{\pi})$ so that $\mathcal{T}_q(\widehat{A}, \widehat{\pi}) \otimes \widehat{\mathbb{Z}}[\widehat{a}] \cong \mathcal{T}_q(\widehat{A}, \widehat{\pi})$. By uniqueness of the above decomposition it follows that there is a permutation τ of $\{1, \dots, q\}$ such that $\widehat{R}(k) \otimes \widehat{\mathbb{Z}}[a] \cong \widehat{R}(\tau(k))$. The permutation is easily determined; as $\widehat{R}(k) \twoheadrightarrow \mathbb{F}_p[\overline{a}^k]$ it follows that $\widehat{R}(k) \otimes \widehat{\mathbb{Z}}[\widehat{a}] \twoheadrightarrow \mathbb{F}_p[\overline{a}^k] \otimes \widehat{\mathbb{Z}}[\widehat{a}] \cong \mathbb{F}_p[\overline{a}^{k+1}]$. As $\widehat{R}(k+1) \twoheadrightarrow \mathbb{F}_p[\overline{a}^{k+1}]$ we see that $\widehat{R}(k) \otimes \widehat{\mathbb{Z}}[\widehat{a}] \cong \widehat{R}(k+1)$ as claimed. □

Corollary 8.4 : $\widehat{R}(k+1) \;\cong_{\widehat{\Lambda}}\; \widehat{R}(1) \otimes_{\widehat{\mathbb{Z}}} \widehat{\mathbb{Z}}(\widehat{a}^k)$ for $1 \le k \le q-1$.

Corollary 8.5 : $\widehat{R}(1) \;\cong_{\widehat{\Lambda}}\; \widehat{R}(q) \otimes_{\widehat{\mathbb{Z}}} \widehat{\mathbb{Z}}(\widehat{a})$.

Start with a basic sequence $0 \to \overline{I_C} \longrightarrow \Lambda \longrightarrow \Lambda \to \overline{I_C^*} \to 0$ and, using (4.10), (4.11) rewrite in 'row notation' thus

(8.6)
$$\begin{tikzcd} & & & K(q) \arrow[dr] & & & \\ 0 \arrow[r] & R(1) \arrow[r] & \Lambda \arrow[rr] \arrow[ur] & & \Lambda \arrow[r] & R(q) \arrow[r] & 0. \end{tikzcd}$$

Applying $- \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ to (8.6) gives an exact sequence

(**8.7**)
$$\begin{tikzcd} & & & \widehat{K}(q) \arrow[dr] & & & \\ 0 \arrow[r] & \widehat{R}(1) \arrow[r] & \widehat{\Lambda} \arrow[rr] \arrow[ur] & & \widehat{\Lambda} \arrow[r] & \widehat{R}(q) \arrow[r] & 0. \end{tikzcd}$$

On applying $- \otimes_{\widehat{\mathbb{Z}}} \widehat{\mathbb{Z}}(\widehat{a})$ to (8.7) iteratively and appealing to (8.3) and (8.5) we generate exact sequences $\widehat{\mathbf{S}(\mathbf{k})}$ with $2 \le k \le q$ thus.

$\widehat{\mathbf{S}(\mathbf{k})}$
$$\begin{tikzcd} & & & \widehat{K}(k\text{-}1) \arrow[dr] & & & \\ 0 \arrow[r] & \widehat{R}(k) \arrow[r] & \widehat{\Lambda} \arrow[rr] \arrow[ur] & & \widehat{\Lambda} \arrow[r] & \widehat{R}(k\text{-}1) \arrow[r] & 0. \end{tikzcd}$$

Splicing the sequences $\widehat{\mathbf{S(k)}}$ together gives the following periodic sequence of length $2q$ which shows that strongly diagonal resolutions exist at the p-adic level.

$$\begin{tikzcd}[column sep=small]
 & & & \widehat{K}(q) \arrow[dr] & & & & \widehat{K}(q-1) \arrow[dr] & & & & \widehat{K}(2) \arrow[dr] & & & & \widehat{K}(1) \arrow[dr] & & & \\
0 \arrow[r] & \widehat{R}(1) \arrow[r] & \widehat{\Lambda} \arrow[ur] \arrow[rr] & & \widehat{\Lambda} \arrow[rr] \arrow[dr] & & \widehat{\Lambda} \arrow[ur] \arrow[rr] & & \widehat{\Lambda} & \cdots & \widehat{\Lambda} \arrow[ur] \arrow[rr] & & \widehat{\Lambda} \arrow[rr] \arrow[dr] & & \widehat{\Lambda} \arrow[ur] \arrow[rr] & & \widehat{\Lambda} \arrow[r] & \widehat{R}(1) \arrow[r] & 0. \\
 & & & & & \widehat{R}(q) \arrow[ur] & & & & & & & & \widehat{R}(2) \arrow[ur] & & & & &
\end{tikzcd}$$

§9 : Proof of Theorem D :

As above $\widehat{\mathbb{Z}}$ will denote the completion of $\mathbb{Z}$ at p. We denote by $\mathcal{D}$er the derived module category of the group ring $\widehat{\Lambda} = \widehat{\mathbb{Z}}[G]$ and by '$\approx$' the relation of isomorphism in $\mathcal{D}$er. A standard calculation (cf [8] p. 133) gives

$$\mathrm{End}_{\mathcal{D}\mathrm{er}}(\widehat{\mathbb{Z}}) \;\cong\; \widehat{\mathbb{Z}}/|G| \;\cong\; \widehat{\mathbb{Z}}/pq.$$

As q is invertible in $\widehat{\mathbb{Z}}$ this simplifies to $\mathrm{End}_{\mathcal{D}\mathrm{er}}(\widehat{\mathbb{Z}}) \cong \mathbb{Z}/p$. Given a lattice L over $\widehat{\mathbb{Z}}$, $\mathbf{D}_n(L)$ will denote the n^{th} generalised syzygy of L. Then (cf [8] p.107) for each $n \geq 1$ there is a ring isomorphism $\mathrm{End}_{\mathcal{D}\mathrm{er}}(\mathbf{D}_n(L)) \cong \mathrm{End}_{\mathcal{D}\mathrm{er}}(L)$. In particular:

(9.1) $\qquad \mathrm{End}_{\mathcal{D}\mathrm{er}}(\mathbf{D}_n(\widehat{\mathbb{Z}})) \;\cong\; \mathbb{Z}/p$ for all $n \geq 1$.

For lattices L, M over $\widehat{\Lambda}$, Yoneda's cohomological interpretation of module extensions ([23]; see also Chap III of [12]) gives an isomorphism $\mathrm{Ext}^n(L, M) \cong H^n(L, M)$. Also the Corepresentation Theorem (cf [8], p.78, more generally Chap. 5 of [9]) computes cohomology in the derived module category as $H^n(L, M) \cong \mathrm{Hom}_{\mathcal{D}\mathrm{er}}(\mathbf{D}_n(L), M)$. Combining the two we see that:

(9.2) $\qquad \mathrm{Ext}^n(L, M) \cong \mathrm{Hom}_{\mathcal{D}\mathrm{er}}(\mathbf{D}_n(L), M)$ for $n \geq 1$.

In particular, $\mathrm{Ext}^2(\mathbf{D}_i(\widehat{\mathbb{Z}}), \mathbf{D}_{i+2}(\widehat{\mathbb{Z}})) \cong \mathrm{End}_{\mathcal{D}\mathrm{er}}(\mathbf{D}_{i+2}(\widehat{\mathbb{Z}}))$ so that, by (9.1),

(9.3) $\qquad \mathrm{Ext}^2(\mathbf{D}_i(\widehat{\mathbb{Z}}), \mathbf{D}_{i+2}(\widehat{\mathbb{Z}})) \;\cong\; \mathbb{Z}/p$ for all $i \geq 1$.

Next we note:

Proposition 9.4 : $[y-1) \otimes \widehat{\mathbb{Z}}$ is projective as a module over $\widehat{\mathbb{Z}}[G]$.

Proof : Let $j : \widehat{\mathbb{Z}}[C_q] \hookrightarrow \widehat{\mathbb{Z}}[G]$ be the inclusion of group rings and let $I(C_q)$ denote the augmentation ideal in $\widehat{\mathbb{Z}}[C_q]$. As q is invertible in $\widehat{\mathbb{Z}}$ it follows, as in the proof of Maschke's Theorem, that $I(C_q) \oplus \widehat{\mathbb{Z}} \cong \widehat{\mathbb{Z}}[C_q]$. Hence $j_*(I(C_q)) \oplus j_*(\widehat{\mathbb{Z}}) \cong j_*(\widehat{\mathbb{Z}}[C_q]) \cong \widehat{\mathbb{Z}}[G]$. Thus $j_*(I(C_q))$ is projective over $\widehat{\mathbb{Z}}[G]$. The result now follows as $[y-1) \otimes \widehat{\mathbb{Z}} = j_*(I(C_q))$. $\square$

Theorem 9.5 : σ is the q-cycle given by $\sigma(i) = i+1$ for $1 \leq i \leq q-1$ and $\sigma(q) = 1$.

Proof : Consider the following statements $\mathbf{P}(i)$ for $1 \leq i \leq q-1$:

$\mathbf{P}(i)$: $\qquad \widehat{R(i)} \approx \mathbf{D}_{2i-1}(\widehat{\mathbb{Z}}) \qquad$ and $\qquad \sigma(r) = r+1 \quad$ for $1 \leq r < i$.

We have already observed that $\sigma(q) = 1$ so it will suffice to prove that each $\mathbf{P}(i)$ is true. Recall from (5.9) that the augmentation ideal $I(G)$ splits as a direct sum

$$I(G) \;=\; \overline{I_C} \oplus [y-1) \;\cong\; R(1) \oplus [y-1).$$

From the augmentation sequence $0 \to \widehat{R(1)} \oplus ([y-1] \otimes \widehat{\mathbb{Z}}) \longrightarrow \widehat{\mathbb{Z}}[G] \longrightarrow \widehat{\mathbb{Z}} \to 0$ we see from (9.4) that $\widehat{R(1)} \approx \mathbf{D}_1(\widehat{\mathbb{Z}})$ so establishing $\mathbf{P}(1)$. Now suppose that $\mathbf{P}(i)$ is true for $i < q$ and note that the sequence $\widehat{\mathbf{S(i)}}$ of §8 has the form

$$\begin{tikzcd}
 & & & & \widehat{K(i)} \arrow[dr] & & & \\
\widehat{\mathbf{S(i)}} & 0 \arrow[r] & \widehat{R(i+1)} \arrow[r] & \widehat{\Lambda} \arrow[ur] \arrow[rr] & & \widehat{\Lambda} \arrow[r] & \widehat{R(i)} \arrow[r] & 0.
\end{tikzcd}$$

Hence $\widehat{R(i+1)} \approx \mathbf{D}_2(\widehat{R(i)})$. The inductive hypothesis $\widehat{R(i)} \approx \mathbf{D}_{2i-1}(\widehat{\mathbb{Z}})$ now implies

(*) $\widehat{R(i+1)} \approx \mathbf{D}_{2i+1}(\widehat{\mathbb{Z}})$.

Consequently $\mathrm{Ext}^2(\widehat{R(i)}, \widehat{R(i+1)}) \cong \mathrm{Ext}^2(\mathbf{D}_{2i-1}(\widehat{\mathbb{Z}}), \mathbf{D}_{2i+1}(\widehat{\mathbb{Z}})) \cong \mathbb{Z}/p$. In particular, $\mathrm{Ext}^2(\widehat{R(i)}, \widehat{R(i+1)}) \neq 0$. However, by (7.2) there exists a unique $j \in \{1, \dots, q\}$ such that $\mathrm{Ext}^2(\widehat{R(i)}, \widehat{R(j)}) \neq 0$ namely $j = \sigma(i)$. Consequently, $\sigma(i) = i+1$ and $\mathbf{P}(i) \Rightarrow \mathbf{P}(i+1)$ as claimed. □

On writing $1 \equiv q+1 \bmod q$ the sequences $\mathcal{Z}(i)$ of (7.7) now become

$$\begin{tikzcd}
 & & & & & K(i) \arrow[dr] & & & \\
\textbf{(9.7)} \quad \mathcal{Z}(i) \quad = & (\, 0 \arrow[r] & R(i+1)) \arrow[r] & P(i) \arrow[urr] \arrow[rrr] & & & \Lambda \arrow[r] & R(i) \arrow[r] & 0 \,).
\end{tikzcd}$$

By splicing the sequences $\mathcal{Z}(i)$ we thereby obtain the following exact sequence

$$\begin{tikzcd}
 & & & K(q) \arrow[dr] & & & & K(q-1) \arrow[dr] & & K(2) \arrow[dr] & & & & K(1) \arrow[dr] & & & \\
0 \arrow[r] & R(1) \arrow[r] & P(q) \arrow[ur] \arrow[rr] & & \Lambda \arrow[dr] \arrow[rr] & & P(q\text{-}1) \arrow[ur] \arrow[rr] & & \cdots \arrow[ur] \arrow[rr] & & \Lambda \arrow[dr] \arrow[rr] & & P(1) \arrow[ur] \arrow[rr] & & \Lambda \arrow[r] & R(1) \arrow[r] & 0 \\
 & & & & & R(q) \arrow[ur] & & & & & & R(2) \arrow[ur] & & & & &
\end{tikzcd}$$

in which each $P(i)$ is projective of rank 1 over Λ and, by (6.9), $P(q) = \Lambda$. As in (7.6)

$$\left(\bigoplus_{i=1}^{q-1} P(i) \right) \oplus \Lambda \cong \bigoplus_{i=1}^{q} P(i) \cong \Lambda^q.$$

Hence $\bigoplus_{i=1}^{q-1} P(i)$ is stably free of rank $q-1$ and so, by the Swan-Jacobinski Theorem,

$$\textbf{(9.8)} \qquad \bigoplus_{i=1}^{q-1} P(i) \cong \Lambda^{q-1}.$$

This completes the proof of Theorem D. □

§10 : Proof of Theorem A:

Consider the exact sequences $\{\mathcal{Z}(i)\}_{1 \le i \le q}$ constructed in (9.7) above. Defining $\mathcal{Z}(n) = \mathcal{Z}(i)$ when $n \equiv i \bmod q$ we obtain exact sequences $\{\mathcal{Z}(n)\}_{n \in \mathbb{Z}}$. Splicing the sequences $\mathcal{Z}(n)$ together gives the following exact sequence

$$\mathcal{S}_+ = \left(\dots \xrightarrow{\partial^+_{2n+3}} P(n+1) \xrightarrow{\partial^+_{2n+2}} \Lambda \xrightarrow{\partial^+_{2n+1}} P(n) \xrightarrow{\partial^+_{2n}} \Lambda \xrightarrow{\partial^+_{2n-1}} P(n-1) \xrightarrow{\partial^+_{2n-2}} \cdots \right)$$

where $\partial^+_{2n-1} = \iota_n \circ \pi_n$ and $\partial^+_{2n} = \alpha_n$. Taking $\partial^-_{2n-1} = (y-1)_*$ and $\partial^+_{2n} = (\Sigma_y)_*$ where $\Sigma_y = 1 + y + \cdots + y^{q-1}$ it is straightforward to see that the following sequence $\mathcal{S}_-$ is exact

$$\mathcal{S}_- = (\quad \cdots \to \Lambda \overset{\partial^-_{2n+3}}{\to} \Lambda \overset{\partial^-_{2n+2}}{\to} \Lambda \overset{\partial^-_{2n+1}}{\to} \Lambda \overset{\partial^-_{2n}}{\to} \Lambda \overset{\partial^-_{2n-1}}{\to} \Lambda \overset{\partial^-_{2n-2}}{\to} \ldots\ldots \quad).$$

Indeed, if $j : C_q \hookrightarrow G(p,q)$ is the inclusion then $\mathcal{S}_-$ is the induced resolution $\mathcal{S}_- = j_*(\mathcal{E})$ where $\mathcal{E}$ is the standard resolution of $\mathbb{Z}$ over $\mathbb{Z}[C_q]$

$$\mathcal{E} \quad = \qquad (\quad \cdots \overset{y-1}{\to} \mathbb{Z}[C_q] \overset{\Sigma_y}{\to} \mathbb{Z}[C_q] \overset{y-1}{\to} \mathbb{Z}[C_q] \overset{\Sigma_y}{\to} \mathbb{Z}[C_q] \overset{y-1}{\to} \mathbb{Z}[C_q] \overset{\Sigma_y}{\to} \ldots\ldots \quad).$$

Taking direct sums we obtain the following exact sequence

$$\mathcal{S}_+ \oplus \mathcal{S}_- = (\ \ldots \overset{\left(\begin{smallmatrix} \partial^+_{2n+3} & 0 \\ 0 & \partial^-_{2n+3} \end{smallmatrix}\right)}{\longrightarrow} P(n+1) \oplus \Lambda \overset{\left(\begin{smallmatrix} \partial^+_{2n+2} & 0 \\ 0 & \partial^-_{2n+2} \end{smallmatrix}\right)}{\longrightarrow} \Lambda \oplus \Lambda \overset{\left(\begin{smallmatrix} \partial^+_{2n+1} & 0 \\ 0 & \partial^-_{2n+1} \end{smallmatrix}\right)}{\longrightarrow} P(n) \oplus \Lambda \overset{\left(\begin{smallmatrix} \partial^+_{2n} & 0 \\ 0 & \partial^-_{2n} \end{smallmatrix}\right)}{\longrightarrow} \ldots \ ).$$

Evidently $\mathcal{S}_+ \oplus \mathcal{S}_-$ is infinite in both directions and is periodic with period $2q$. Truncating at the third differential gives an exact sequence, infinite to the left:

$$\textbf{(10.1)} \qquad \ldots \overset{\left(\begin{smallmatrix} \partial^+_5 & 0 \\ 0 & \partial^-_5 \end{smallmatrix}\right)}{\longrightarrow} P(2) \oplus \Lambda \overset{\left(\begin{smallmatrix} \partial^+_4 & 0 \\ 0 & \partial^-_4 \end{smallmatrix}\right)}{\longrightarrow} \Lambda \oplus \Lambda \overset{\left(\begin{smallmatrix} \partial^+_3 & 0 \\ 0 & \partial^-_3 \end{smallmatrix}\right)}{\longrightarrow} P(1) \oplus \Lambda$$

However, we also have an exact sequence

(10.2)

$$\begin{tikzcd}
P(1) \oplus \Lambda \arrow[r, "\left(\begin{smallmatrix} \partial^+_2 & 0 \\ 0 & \partial^-_2 \end{smallmatrix}\right)"] & \Lambda \oplus \Lambda \arrow[rr, "\partial^+_1 + \partial^-_1"] \arrow[dr] & & \Lambda \arrow[r, "\epsilon"] & \mathbb{Z} \arrow[r] & 0 \\
& & \overline{I_C} \oplus [y-1] \arrow[ur] & & &
\end{tikzcd}$$

Merging the two gives a complete resolution of $\mathbb{Z}$ which begins

$$\cdots \overset{\left(\begin{smallmatrix} \partial^+_{2n+3} & 0 \\ 0 & y-1 \end{smallmatrix}\right)}{\longrightarrow} P(1) \oplus \Lambda \overset{\left(\begin{smallmatrix} \partial^+_2 & 0 \\ 0 & \partial^-_2 \end{smallmatrix}\right)}{\longrightarrow} \Lambda \oplus \Lambda \overset{\partial^+_1 + \partial^-_1}{\longrightarrow} \Lambda \overset{\epsilon}{\to} \mathbb{Z} \to 0$$

and continues

$$\ldots P(n+1) \oplus \Lambda \overset{\left(\begin{smallmatrix} \partial^+_{2n+2} & 0 \\ 0 & \Sigma_y \end{smallmatrix}\right)}{\longrightarrow} \Lambda \oplus \Lambda \overset{\left(\begin{smallmatrix} \partial^+_{2n+1} & 0 \\ 0 & y-1 \end{smallmatrix}\right)}{\longrightarrow} P(n) \oplus \Lambda \overset{\left(\begin{smallmatrix} \partial^+_{2n} & 0 \\ 0 & \Sigma_y \end{smallmatrix}\right)}{\longrightarrow} \Lambda \oplus \Lambda \ldots$$

and where
$$\left\{ \begin{array}{rclcrcl} P(q) & = & \Lambda & ; & P(k+mq) & = & P(k) \\ \partial^+_{k+2mq} & = & \partial^+_k & ; & \partial^-_{k+2m} & = & \partial^-_k . \end{array} \right.$$

We have constructed a diagonal resolution of $\mathbb{Z}$ with period $2q$. Moreover, by (9.8), $\bigoplus_{i=1}^{q-1} P(i) \cong \Lambda^{q-1}$. This completes the proof of Theorem A. □

§11: Proof of Theorem B :

By a *projective n-segment* $\mathcal{P}$ we shall mean an exact sequence of Λ-modules

$$\mathcal{P} = (0 \to N \to P_n \to \cdots \to P_1 \to M \to 0)$$

where $P_1, \ldots, P_n$ are finitely generated projective Λ-modules. Given a projective n-segment $\mathcal{P}$ we recall the Swan-Wall finiteness obstruction $\chi(\mathcal{P})$ is defined by

$$\chi(\mathcal{P}) = \textstyle\sum_{r=1}^{n} (-1)^r [P_r] \in \widetilde{K}_0(\Lambda).$$

We say that a projective n-segment $\mathcal{P}$ is *free* when each P_r is free. It is well known and straightforward to prove that:

Proposition 11.1 : If $n \geq 2$ and $\mathcal{P} = (0 \to N \to P_n \to \cdots \to P_1 \to M \to 0)$ is a projective n-segment with $\chi(\mathcal{P}) = 0$ then there exists a free n-segment

$$\mathcal{F} = (0 \to N \to \Lambda^{a_n} \to \Lambda^{a_{n-1}} \to \cdots \to \Lambda^{a_1} \to M \to 0).$$

Put $\mathcal{Y} = (0 \to [y-1) \to \Lambda) \overset{\Sigma_y}{\to} \Lambda \to [y-1) \to 0)$. and for $1 \leq i \leq q-1$ denote by $\mathcal{W}(i)$ the direct sum $\mathcal{W}(i) = \mathcal{Z}(i) \oplus \mathcal{Y}$ where $\mathcal{Z}(i)$ constructed as in (9.7). Then $\mathcal{W}(i)$ is a projective 2-stem $\mathcal{W}(i) = (0 \to R(i+1) \oplus [y-1) \to P(i) \oplus \Lambda \to \Lambda \oplus \Lambda \to R(i) \oplus [y-1) \to 0)$. Splicing the sequences $\mathcal{W}(i)$ together by Yoneda product gives a projective $(2q$-$2)$-stem $\mathcal{Q} = \mathcal{W}(q-1) \circ \mathcal{W}(q-2) \circ \cdots \circ \mathcal{W}(1)$ thus :

$$\mathcal{Q} = (0 \to R(q) \oplus [y-1) \to Q_{2q-2} \to \cdots \to Q_1 \to R(1) \oplus [y-1) \to 0)$$

where $$Q_r = \begin{cases} \Lambda \oplus \Lambda & r \text{ odd} \\ \Lambda \oplus P(r/2) & r \text{ even.} \end{cases}$$

Then $\chi(\mathcal{Q}) = \sum_{s=1}^{q-1}[P(s)] = [\bigoplus_{s=1}^{q-1} P(s)]$. However, by (9.8), $\bigoplus_{s=1}^{q-1} P(s) \cong \Lambda^{q-1}$. Hence $\chi(\mathcal{Q}) = 0$. By (4.11) and (5.12) we see that $R(1) \oplus [y-1) \cong I_G$. However $R(q) \cong R(1)^*$ and $[y-1) \cong [y-1)^*$ so that $R(q) \oplus [y-1) \cong I_G^*$. We have constructed a projective $(2q$-$2)$-segment

$$\mathcal{Q} = (0 \to I_G^* \to Q_{2q-2} \to \cdots \to Q_1 \to I_G \to 0)$$

with $\chi(\mathcal{Q}) = 0$. It follows immediately from (11.1) that:

(11.2) There exists a free $(2q$-$2)$-segment $(0 \to I_G^* \to \Lambda^{a_{2q-2}} \to \cdots \to \Lambda^{a_1} \to I_G \to 0)$.

Corollary 11.3 : There exists a free $2q$-segment

$$\mathcal{S} = (0 \to \mathbb{Z} \to \Lambda \to \Lambda^{a_{2q-2}} \to \cdots \to \Lambda^{a_1} \to \Lambda \to \mathbb{Z} \to 0).$$

Proof : Let $\mathcal{E}$ be the standard exact sequence $\mathcal{E} = (0 \to I_G \to \Lambda \to \mathbb{Z} \to 0)$. The dual sequence has the form $\mathcal{E}^* = (0 \to \mathbb{Z} \to \Lambda \to I_G^* \to 0)$. Taking $\mathcal{F}$ to be the free $(2q$-$2)$-segment constructed in (11.2) we see that the Yoneda product $\mathcal{S} = \mathcal{E}^* \circ \mathcal{F} \circ \mathcal{E}$ is a free $2q$-segment of the required form

$$\mathcal{S} = (0 \to \mathbb{Z} \to \Lambda \to \Lambda^{a_{2q-2}} \to \cdots \to \Lambda^{a_1} \to \Lambda \to \mathbb{Z} \to 0). \qquad \square$$

Theorem B is now immediate, being a slightly weaker statement than (11.3).

F.E.A. Johnson

Department of Mathematics

University College London

Gower Street, London WC1E 6BT, U.K.

e-mail address : feaj@math.ucl.ac.uk

J.J. Remez

Department of Mathematics

University College London

Gower Street, London WC1E 6BT, U.K.

e-mail address : j.remez@alumni.ucl.ac.uk

REFERENCES

[1] : S.Bentzen and I. Madsen ; On the Swan subgroup of certain periodic groups. Math. Ann. 264 (1983) 447-474.

[2] : B.J. Birch; Cyclotomic fields and Kummer extensions; pp 85-93 of 'Algebraic Number Theory' JWS Cassels and A. Fröhlich (Editors). Academic Press 1965.

[4] : C.W. Curtis and I. Reiner ; Methods of Representation Theory; Volume I. Wiley-Interscience, 1981.

[5] : C.W. Curtis and I. Reiner ; Methods of Representation Theory; Volume II. Wiley-Interscience, 1987.

[7]: K.W. Gruenberg and K.W. Roggenkamp; Decomposition of the augmentation ideal and of the relation modules of a finite group. Proc. Lond. Math. Soc. 31 (1975) 149-166.

[8]: F.E.A. Johnson; Stable modules and the D(2)-problem. LMS Lecture Notes In Mathematics, vol. 301. CUP 2003.

[9] : F.E.A. Johnson; Syzygies and homotopy theory. Springer-Verlag 2011.

[10] : F.E.A. Johnson ; Syzygies and diagonal resolutions for dihedral groups. Communications in Algebra 44 (2015) 2034-2047.

[11] : F.E.A. Johnson and J.J. Remez; Strongly diagonal resolutions for metacyclic groups. (in preparation).

[12] : S. Mac Lane ; Homology. Springer-Verlag 1963.

[13] : R.J. Milgram ; Evaluating the Swan finiteness obstruction for periodic groups (preprint, Stanford University 1979).

[14] : R.J. Milgram ; Odd index subgroups of units in cyclotomic fields and applications : pp 269-298 of Lecture Notes in Mathematics, vol. 854, Springer-Verlag, 1981.

[15] : A.J. Nadim. A periodic monogenic resolution. PhD Thesis, University College London 2015.

[16] : T. Petrie; Free metacyclic group actions on homotopy spheres. Ann. of Math. 94 (1971) 108-124.

[17]: L.C. Pu. Integral representations of non-abelian groups of order pq. Michigan Journal of Mathematics 12 (1965) 231-246.

[18] : I. Reiner; Maximal Orders. Academic Press, 1975.

[19] : J.J. Remez; Diagonal resolutions for the metacyclic groups $G(pq)$. PhD Thesis, University College London 2012.

[20] : M. Rosen; Representations of twisted group rings. PhD Thesis, Princeton University 1963.

[21] : R.G. Swan ; Periodic resolutions for finite groups.
Ann.of Math. 72 (1960) 267-291.

[22] : C.T.C. Wall ; Periodic projective resolutions.
Proc. London Math. Soc. 39 (1979) 509-553.

[23] : N. Yoneda ; On the homology theory of modules.
J. Fac. Sci. Tokyo, Sec. I, 7 (1954) 193- 227.