

PROJECTIVITIES IN FINITE GROUPS

D. W. BARNES

(received 24 September 1963)

Chains of projectivities within the lattice $\mathcal{S}(G)$ of subnormal subgroups of a group G have been considered by various authors, see for example Barnes [1] and Tamaschke [2]. The starting point of the investigations of which this paper is a report, was the theorem, basically due to Wielandt:

THEOREM 1. *If A/B is a non-abelian composition factor of a group G with a finite composition series, then A/B is not projective in $\mathcal{S}(G)$ to any other factor of the same composition series, and any chain of projections from A/B to A/B induces the identity automorphism in A/B .¹*

This is proved by a "homotopy" argument in which the chain of projections is deformed into a chain with a very simple form. A similar argument proves

THEOREM 2. *Let A/B be a composition factor of prime order p of a group G with a finite composition series.*

(i) *If A/B is projective to no other factor of the same composition series, then every chain of projections from A/B to A/B induces the identity automorphism.*

(ii) *If A/B is projective to some other factor of the same composition series, then every automorphism of A/B is induced by some chain of projections in $\mathcal{S}(G)$.*

This leads us to consider for A subnormal in G (which in this paper is always assumed finite) and B normal in A , the group $\pi(A/B, G)$ of automorphisms of A/B induced by chains of projections in $\mathcal{S}(G)$. We ask the question: for given A/B , what subgroups of the automorphism group of A/B can be $\pi(A/B, G)$ for some suitable overgroup G ?

The theorems quoted above give a complete answer to this question for A/B simple. By the same method, it can be proved that $\pi(A/B, G)$ is trivial unless for some prime p , A/B has a normal subgroup of index p . For an elementary abelian quotient A/B , $\pi(A/B, G)$ is non-trivial only if A/B is projective in $\mathcal{S}(G)$ to a subgroup of a larger elementary abelian

¹ See Zassenhaus [4] p. 235 exercises 20 and 21.

quotient, in which case $\pi(A/B, G)$ is the group of all automorphisms of A/B . The next case to consider is the case where A/B is a cyclic p -group of order greater than p .

In part I, we develop a homotopy theory of finite groups in sufficient generality for application to the general problem. In part II, we solve the problem for cyclic quotients A/B in abelian p -groups. We remark that this solves the problem for a cyclic quotient in any finite abelian group since the lattice of a finite abelian group is the direct product of the lattices of its Sylow subgroups. If we denote by G_p the unique Sylow p -subgroup of the abelian group G , and if A/B is a quotient of G , then $\pi(A/B, G)$ is the direct product of the groups $\pi((A/B)_p, G_p)$.

PART I. HOMOTOPY THEORY OF FINITE GROUPS

1. Projectivities

A quotient in a group G is a factor group A/B where A is a subgroup of G and B is a normal subgroup of A . Suppose L is some sublattice of the lattice of all subgroups of G . The quotient A/B is called admissible with respect to L if $A, B \in L$. The lattice L is supposed fixed, and by "quotient" we shall mean "quotient admissible with respect to L ". Suppose $A/B, C/D$ are (admissible) quotients and $A = B \cup C, D = B \cap C$. Then the

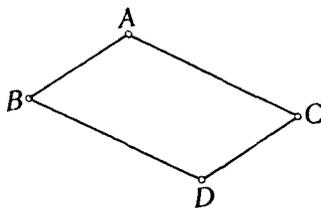


Fig. 1.

map $aB \rightarrow (aB) \cap C$ for all $a \in A$ of the cosets of B in A onto the cosets of D in C is an isomorphism. Such an isomorphism is called a projection down, its inverse is called a projection up.

A chain c of projections is a sequence $\phi_1, \phi_2, \dots, \phi_n$ of projections such that ϕ_i is a map from the image of ϕ_{i-1} ($i = 2, 3, \dots, n$). Since the projection

$$\phi_i : A_{i-1}/B_{i-1} \rightarrow A_i/B_i = (A_{i-1}/B_{i-1})\phi_i$$

is uniquely determined by the intervals A_{i-1}/B_{i-1} and A_i/B_i , we write

² Notice that not every quotient of L in the lattice sense is a quotient in the sense of this paper.

$$c = (A_0/B_0 \rightarrow A_1/B_1 \rightarrow \cdots \rightarrow A_n/B_n).$$

c clearly defines the isomorphism $\phi = \phi_1\phi_2 \cdots \phi_n$ of A_0/B_0 onto A_n/B_n . Such an isomorphism ϕ is called a projectivity (in L). If

$$d = (A_n/B_n \rightarrow A_{n+1}/B_{n+1} \rightarrow \cdots \rightarrow A_{n+m}/B_{n+m})$$

is a chain of projections giving the projectivity ψ of A_n/B_n onto A_{n+m}/B_{n+m} , then we define cd to be the chain

$$cd = (A_0/B_0 \rightarrow A_1/B_1 \rightarrow \cdots \rightarrow A_n/B_n \rightarrow A_{n+1}/B_{n+1} \rightarrow \cdots \rightarrow A_{n+m}/B_{n+m}).$$

Clearly cd gives the projectivity $\phi\psi$ of A_0/B_0 onto A_{n+m}/B_{n+m} . We define c^{-1} to be the chain

$$c^{-1} = (A_n/B_n \rightarrow \cdots \rightarrow A_1/B_1 \rightarrow A_0/B_0).$$

c^{-1} clearly gives the projectivity ϕ^{-1} .

2. The projectivity group $\pi(A)$

If c is a chain starting and finishing at the same quotient A/B , we call c a loop. c then gives an automorphism $\alpha(c)$ of A/B . It is convenient to define $\alpha(c)$ to be the identity automorphism for $c = (A/B)$, the trivial loop consisting of the empty set of projections. Clearly the set of all automorphisms $\alpha(c)$ of A/B given by loops c starting and finishing at A/B is a group which we denote by $\pi(A/B)$. Two quotients $A/B, C/D$ are called projective (in L) if there exists a chain d of projections

$$d = (A/B \rightarrow A_1/B_1 \rightarrow \cdots \rightarrow A_n/B_n = C/D).$$

If A/B and C/D are projective, then $\pi(A/B)$ and $\pi(C/D)$ are isomorphic. Thus $\pi(A/B)$ depends (up to isomorphism) only on the class A of projective quotients to which A/B belongs. We therefore denote the (isomorphism class of the) group by $\pi(A)$.

3. The fundamental group $F(A)$

If in the chain $c = (A_0/B_0 \rightarrow A_1/B_1 \rightarrow \cdots \rightarrow A_n/B_n)$, we have $A_{r+2}/B_{r+2} = A_r/B_r$ for some r , then the projection $A_{r+1}/B_{r+1} \rightarrow A_{r+2}/B_{r+2}$ is the inverse of the projection $A_r/B_r \rightarrow A_{r+1}/B_{r+1}$. If

$$c' = (A_0/B_0 \rightarrow \cdots \rightarrow A_r/B_r = A_{r+2}/B_{r+2} \rightarrow A_{r+3}/B_{r+3} \rightarrow \cdots \rightarrow A_n/B_n)$$

is the chain formed from c by omitting the projections

$$A_r/B_r \rightarrow A_{r+1}/B_{r+1} \rightarrow A_{r+2}/B_{r+2} = A_r/B_r,$$

then c and c' give the same projectivity. We say that c and c' can be obtained from one another by a transformation of type (1).

If there exist projections $A_1/B_1 \rightarrow A_2/B_2$, $A_1/B_1 \rightarrow A_3/B_3$ and $A_2/B_2 \rightarrow A_3/B_3$, then $A_1/B_1 \rightarrow A_2/B_2 \rightarrow A_3/B_3$ and $A_1/B_1 \rightarrow A_3/B_3$ give the same projectivity. This follows from the fact that, for some permutation u, v, w of 1, 2, 3, we have $A_u \cong A_v \cong A_w$, $B_u \cong B_v \cong B_w$ and for the coset aB_u of B_u in A_u ,

$$(aB_u \cap B_v) \cap B_w = (aB_u) \cap B_w.$$

If the chain c' is obtained from $c = (A_1/B_1 \rightarrow \dots \rightarrow A_n/B_n)$ by replacing $A_{i+1}/B_{i+1} \rightarrow A_{i+2}/B_{i+2} \rightarrow A_{i+3}/B_{i+3}$ by $A_{i+1}/B_{i+1} \rightarrow A_{i+3}/B_{i+3}$ where $A_{i+u} \cong A_{i+v} \cong A_{i+w}$, $B_{i+u} \cong B_{i+v} \cong B_{i+w}$ for some permutation u, v, w of 1, 2, 3, then the transformation of replacing c by c' or of replacing c' by c is called a transformation of type (2).

We say that the two loops c, c' starting at A/B are homotopic if c' can be obtained from c by a succession of transformations of types (1) and (2), such that the chain obtained after each successive transformation is again a loop starting at A/B . The classes of homotopic loops starting at A/B clearly form a group $F(A/B)$ which we call the fundamental group at A/B . As in ordinary homotopy theory, this group depends (up to isomorphism) only on the class \mathcal{A} of projective quotients to which A/B belongs, not on the actual starting point A/B of the loops, and we therefore denote the fundamental group by $F(\mathcal{A})$. Clearly $c \rightarrow \alpha(c)$ defines a homomorphism $\alpha : F(\mathcal{A}) \rightarrow \pi(\mathcal{A})$. Thus $\pi(\mathcal{A})$ can be determined if we can calculate $\alpha(c)$ for a representative loop c of each element in some generating set of $F(\mathcal{A})$.

We have called this group $F(\mathcal{A})$ the fundamental group of the class \mathcal{A} . This is consistent with the terminology of topology if we make \mathcal{A} a two dimensional complex in the following manner. The vertices of the complex \mathcal{A} are the quotients $A/B \in \mathcal{A}$ and the edges are the projections $A/B \rightarrow C/D$ in \mathcal{A} . This defines the one-skeleton of the complex. Every triangle $A/B \rightarrow C/D \rightarrow E/F \rightarrow A/B$ in \mathcal{A} is spanned by a surface. These surfaces spanning a triangle are the faces of the complex \mathcal{A} . The fundamental group of this complex is precisely the group $F(\mathcal{A})$.³

4. The homology group $H(\mathcal{A})$

We introduce a further two types of transformations of chains. If $c = uabv$ where a, b are loops starting at U/V , u is a chain ending at U/V and v is a chain starting at U/V for some $U/V \in \mathcal{A}$, and if $c' = ubav$, then we say that c' is obtained from c by a transformation of type (3). The equivalence classes of loops starting at some fixed A/B obtainable from one another by transformations of types (1), (2) and (3) form the abelian

³ For the homotopy theory of complexes, see Seifert and Threlfall [3] p. 162-163.

group $F(A/B)/F'(A/B)$ which is the factor group of $F(A/B)$ by its commutator subgroup.

If $c = (A_1/B_1 \rightarrow A_2/B_2 \rightarrow \dots \rightarrow A_n/B_n \rightarrow A_1/B_1)$, and $c' = (A_r/B_r \rightarrow A_{r+1}/B_{r+1} \rightarrow \dots \rightarrow A_n/B_n \rightarrow A_1/B_1 \rightarrow \dots \rightarrow A_r/B_r)$ consists of the same projections as c taken in the same cyclic order, then we say c' is obtained from c by a transformation of type (4).

If c, c' are loops in \mathcal{A} and c' can be obtained from c by a succession of transformations of types (1), (2), (3) and (4), we say that c, c' are homologous loops. The classes of homologous loops form an abelian group $H(\mathcal{A})$ which we call the homology group of \mathcal{A} .

If u is a chain from A/B to C/D , then the map taking the loop c starting at A/B to the loop $u^{-1}cu$ starting at C/D gives an isomorphism of $F(A/B)$ onto $F(C/D)$. This isomorphism is not in general unique but depends on u to the extent of an inner automorphism. Consequently the induced map of $F(A/B)/F'(A/B)$ onto $F(C/D)/F'(C/D)$ is independent of u . The element of $F(A/B)/F'(A/B)$ with the loop c as representative is precisely the set of loops starting at A/B and homologous to c . The element of $F(C/D)/F'(C/D)$ corresponding to this under the map induced by $c \rightarrow u^{-1}cu$ is the set of loops starting at C/D and homologous to c .⁴ Thus if we identify corresponding elements of the different $F(A/B)/F'(A/B)$, the group whose elements are these classes of identified elements is the group $H(\mathcal{A})$. $H(\mathcal{A}) \simeq F(\mathcal{A})/F'(\mathcal{A})$ is the one-dimensional homology group of the two-dimensional complex \mathcal{A} .

If the group $\pi(\mathcal{A})$ is abelian, then the map $c \rightarrow \alpha(c)$ induces a homomorphism of $H(\mathcal{A})$ onto $\pi(\mathcal{A})$. In this case, $\pi(\mathcal{A})$ can be determined if we can find the $\alpha(c)$ given by the elements of a generating set for $H(\mathcal{A})$.

5. The restricted complex

The elements of \mathcal{A} are naturally partially ordered, $A/B \geq C/D$ if $A \geq C, B \geq D$ and $A = B \cup C, D = B \cap C$, i.e. $A/B \geq C/D$ if there is a projection down from A/B to C/D . The maximal elements of \mathcal{A} in this partial ordering we call the peaks of \mathcal{A} , the minimal elements we call the pits.

If $A/B \rightarrow C/D$ is a projection up, and $C/D \rightarrow E/F$ is a projection down, and if C'/D' is a peak, $C'/D' \geq C/D$, then $A/B \rightarrow C/D \rightarrow E/F$ is homotopic with fixed end-points to $A/B \rightarrow C'/D' \rightarrow E/F$. Thus if A/B is a peak or pit, then in every homotopy class in $F(A/B)$ there is a loop $A/B = A_0/B_0 \rightarrow A_1/B_1 \rightarrow \dots \rightarrow A_n/B_n \rightarrow A/B$ in which the A_i/B_i are alternately peaks and pits. It is convenient to study these loops, considering only those homotopies in which all intermediate loops obtained by the successive transformations have this same form. In this, we use

⁴ See Seifert and Threlfall [3] p. 174–176.

transformations of type (1) only. This leads us to consider the complex \mathcal{A}^* whose vertices are the peaks and pits of \mathcal{A} and whose edges are the projections between these peaks and pits. The faces of \mathcal{A} were introduced to allow transformations of type (2). Since these cannot occur between loops of the type we are considering, we do not define faces of \mathcal{A}^* . We call \mathcal{A}^* the restricted complex of \mathcal{A} . Its fundamental group $F(\mathcal{A}^*)$, which we denote by $F^* = F^*(\mathcal{A})$, we call the restricted fundamental group of \mathcal{A} . The homology group $H(\mathcal{A}^*) = H^* = H^*(\mathcal{A})$ of \mathcal{A}^* we call the restricted homology group of \mathcal{A} .

Each restricted homotopy class of loops is contained in a homotopy class, and each homotopy class with peak or pit as starting point contains at least one restricted class. The map in which each element of F^* maps into the element of F in which it is contained, is clearly a homomorphism of F^* onto F . Similarly there is a homomorphism of H^* onto H .

Since \mathcal{A}^* is a one-dimensional complex, F^* is a free group and H^* is free abelian⁵. This, together with the fact that the vertices and edges of \mathcal{A}^* are more easily enumerated than those of \mathcal{A} makes F^* and H^* more convenient tools than F and H for the determination of $\pi(\mathcal{A})$. F^* and H^* are not necessarily groups of simpler structure than F and H , for example, if L is the lattice of all subgroups of the elementary abelian group of order 8 and the vertices of \mathcal{A} are all the quotients of order 2, then $F(\mathcal{A})$ is trivial but $F^*(\mathcal{A})$ is the free group on 15 generators.

6. Covering spaces

For each of the complexes \mathcal{A} , \mathcal{A}^* we can define in a natural way a covering space whose monodromie group is $\pi(\mathcal{A})$ ⁶.

Let K be either of the complexes \mathcal{A} , \mathcal{A}^* . Each vertex V of K is a quotient A/B of the group G . The points of the covering space \tilde{K} which lie over V are the elements of A/B . If $V_1 = A_1/B_1$ is joined to $V_2 = A_2/B_2$ in K by an edge, then in \tilde{K} each element $a_1 \in A_1/B_1$ is joined by an edge to the element $a_2 \in A_2/B_2$ to which it maps under the projection $A_1/B_1 \rightarrow A_2/B_2$. Every triangle in \tilde{K} is spanned by a face. The points $a_1, a_2, a_3 \in \tilde{K}$ can be vertices of a face only if the points V_1, V_2, V_3 of K over which they lie are vertices of a face of K . Conversely, if V_1, V_2, V_3 are vertices of a face of K and if a_1 lies over V_1, a_2, a_3 the images of a_1 under the projections $V_1 \rightarrow V_2$ and $V_1 \rightarrow V_3$, then a_3 is the image of a_2 under the projection $V_2 \rightarrow V_3$ and a_1, a_2, a_3 are the vertices of a face of \tilde{K} . If n is the order of the quotients in \mathcal{A} , then over each vertex of K lie n points of \tilde{K} , n edges of \tilde{K} lie over

⁵ See Seifert and Threlfall [3] p. 165–168.

⁶ For the theory of covering spaces, see Seifert and Threlfall [3], chapter 8, p. 181–203. The monodromie group is discussed in § 58, p. 198–203.

each edge of K and n faces of \tilde{K} lie over each face of K . By taking suitable coordinate systems in the faces and edges of K and \tilde{K} and mapping each point of \tilde{K} to the point in the corresponding face or edge of K and with the same coordinates, we can clearly define a map of \tilde{K} onto K making \tilde{K} a covering space for K .

The theory of covering spaces is usually developed under the assumption that the covering space is connected. If the quotients in \mathcal{A} are not trivial, then \tilde{K} cannot be connected since any projection preserves the order of an element, and in particular, maps the identity element to the identity element. We can however apply the theory of connected covering spaces to the connected components of \tilde{K} .

Take any vertex V of K and let a_1, \dots, a_n be the points of \tilde{K} lying over V . For any loop c in K starting at V , there is a uniquely defined path p_i starting at a_i and lying over c . The map which takes a_i into the point at which the path p_i ends is a permutation of the points a_i . The monodromie group of \tilde{K} is the group of all such permutations. Since the end-point of p_i is $a_i\alpha(c)$, the monodromie group is precisely the group $\pi(\mathcal{A})$. Since \tilde{K} is not connected, the monodromie group of K is not transitive.

A connected covering space \tilde{W} of the complex W is called regular if, for every loop l in W , the paths p_i in \tilde{W} lying over l are either all closed or all open. Since every transitive abelian permutation group is regular, every component of \tilde{K} is regular if $\pi(\mathcal{A})$ is abelian, in particular, if the quotients $A/B \in \mathcal{A}$ are cyclic. If on the other hand, \mathcal{A} is a class of elementary abelian quotients of order p^n ($n \geq 2$) in $\mathcal{S}(G)$ and $\pi(\mathcal{A})$ is not trivial, then $\pi(\mathcal{A})$ is the general linear group $GL(n, p)$ and is transitive on the non-identity elements of any quotient in \mathcal{A} . A connected covering space is regular if and only if its multiplicity is equal to the order of its monodromie group. In this example, $\pi(\mathcal{A})$ is the monodromie group of the non-identity component of $\tilde{\mathcal{A}}$. Since the multiplicity of the component is $p^n - 1$ which is not equal to $|\pi(\mathcal{A})| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$, it is not a regular covering space.

7. Lengths

Suppose c is a loop in \mathcal{A} or \mathcal{A}^* . We define the length of c to be the number of projections in c . Suppose T is one of the groups F, F^*, H, H^* and that t is an element of T . (In the case of F , we suppose the starting point of the loops to be some fixed peak or pit.) Then t is a class of loops. We define the length $l(t)$ of t to be the length of the shortest loop in t . Since the shortest loop in t must consist of projections alternately up and down, $l(t)$ is an even integer. t is called reducible if there exist $t_1, t_2, \dots, t_r \in T$ such that $t = t_1 t_2 \cdots t_r$ and $l(t_i) < l(t)$ for all i . Otherwise t is called irreducible.

We denote by $T^{(n)}$ the subgroup of T generated by all elements of T of length less than or equal to $2n$. The length $l(T)$ of T is the length of its longest irreducible element. If $l(T) = 2n$, then $T = T^{(n)} \neq T^{(n-1)}$.

If T is F or F^* , then an element of T is a class of loops with fixed end-point. Although the group T (up to isomorphism) is independent of that fixed end-point, $l(T)$ may depend on the end-point. For example, suppose $G = \langle a, b \rangle$, $a^4 = b^2 = aba^{-1}b^{-1} = 1$, and L the lattice of all subgroups of G .

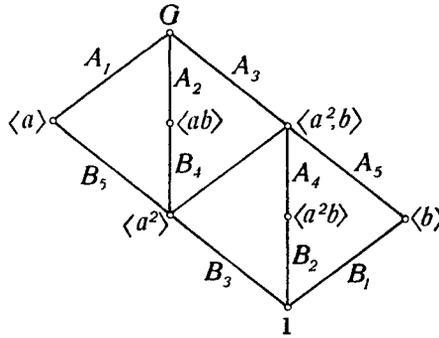


Fig. 2.

We consider the quotients of order 2. The peaks of Λ are $A_1 = G/\langle a \rangle$, $A_2 = G/\langle ab \rangle$, $A_3 = G/\langle a^2, b \rangle$, $A_4 = \langle a^2, b \rangle / \langle a^2, b \rangle$, $A_5 = \langle a^2, b \rangle / \langle b \rangle$ and the pits are $B_1 = \langle b \rangle$, $B_2 = \langle a^2, b \rangle$, $B_3 = \langle a^2 \rangle$, $B_4 = \langle ab \rangle / \langle a^2 \rangle$, $B_5 = \langle a \rangle / \langle a^2 \rangle$ as marked on the lattice diagram. Λ^* is the complex

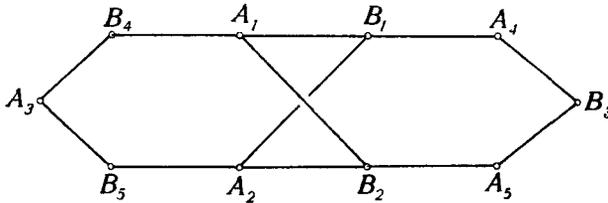


Fig. 3.

$F^*(A_1)$ is generated by the irreducible loops $(A_1 \rightarrow B_1 \rightarrow A_2 \rightarrow B_2 \rightarrow A_1)$,

$$(A_1 \rightarrow B_4 \rightarrow A_3 \rightarrow B_5 \rightarrow A_2 \rightarrow B_1 \rightarrow A_1)$$

and

$$(A_1 \rightarrow B_1 \rightarrow A_4 \rightarrow B_3 \rightarrow A_5 \rightarrow B_2 \rightarrow A_1).$$

Thus $l(F^*(A_1)) = 6$. $F^*(A_3)$ is generated by the irreducible loops

$$(A_3 \rightarrow B_4 \rightarrow A_1 \rightarrow B_2 \rightarrow A_2 \rightarrow B_5 \rightarrow A_3),$$

$$(A_3 \rightarrow B_4 \rightarrow A_1 \rightarrow B_1 \rightarrow A_2 \rightarrow B_5 \rightarrow A_3)$$

and

$$(A_3 \rightarrow B_4 \rightarrow A_1 \rightarrow B_1 \rightarrow A_4 \rightarrow B_3 \rightarrow A_5 \rightarrow B_2 \rightarrow A_2 \rightarrow B_5 \rightarrow A_3).$$

Thus $l(F^*(A_3)) = 10$. Thus to define $F^{(n)}, F^{*(n)}, l(F)$ or $l(F^*)$, it is necessary to specify the point at which the loops start. This difficulty does not arise with H and H^* . Trivially, $l(H) \leq l(F)$ and $l(H^*) \leq l(F^*)$.

LEMMA 7.1. $H/H^{(2)} \simeq H^*/H^{*(2)}$.

PROOF. Let $c = (A_1/B_1 \rightarrow A_2/B_2 \rightarrow \dots \rightarrow A_n/B_n \rightarrow A_1/B_1)$ be a representative loop of an element of H . We may choose c such that the projections are alternately up and down. If $A_i/B_i \rightarrow A_{i+1}/B_{i+1}$ is a projection up, take A'_{i+1}/B'_{i+1} any peak such that $A'_{i+1}/B'_{i+1} \geq A_{i+1}/B_{i+1}$, and A'_i/B'_i any pit such that $A'_i/B'_i \leq A_i/B_i$. Put

$$c' = (A'_1/B'_1 \rightarrow A'_2/B'_2 \rightarrow \dots \rightarrow A'_n/B'_n \rightarrow A'_1/B'_1).$$

Then c' is a loop in A^* and gives an element of $H^*/H^{*(2)}$ which is completely determined by c . This clearly defines a homomorphism of H onto $H^*/H^{*(2)}$, and $H^{(2)}$ is clearly contained in the kernel. Since the loops c and c' are homologous, c' is a representative of an element of $H^{*(2)}$ only if c is a representative of an element of $H^{(2)}$. Hence $H/H^{(2)} \simeq H^*/H^{*(2)}$.

PART II. CYCLIC QUOTIENTS IN ABELIAN p -GROUPS

We now restrict ourselves to the case where G is a finite abelian p -group, L is the lattice of all subgroups of G and \mathcal{A} is a class of projective cyclic quotients. The group G is a direct product of cyclic groups $\langle u_1 \rangle, \dots, \langle u_k \rangle$ of orders $p^{\lambda_1}, \dots, p^{\lambda_k}$. We may suppose the numbering of the u_i chosen so that $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k$, in which case we say that G is of type $(\lambda_1, \dots, \lambda_k)$. Let p^λ be the order of the quotients in \mathcal{A} . We shall determine the number of classes \mathcal{A} of cyclic quotients of order p^λ in G , show that the groups $F(\mathcal{A}), F^*(\mathcal{A}), H(\mathcal{A}), H^*(\mathcal{A})$ and $\pi(\mathcal{A})$ depend only on $p, \lambda, \lambda_1, \dots, \lambda_k$, not on the actual class \mathcal{A} chosen, and determine $\pi(\mathcal{A})$ in terms of these.

8. The classes of projective cyclic quotients

LEMMA 8.1. *Let G be any p -group and C a cyclic group of order p^λ . Then every cyclic quotient of order p^λ in $G \times C$ is projective to C .*

PROOF. Let A/B be such a quotient. Then AC/B is abelian of type

(λ, r) , $r \leq \lambda$, and therefore $(G \cap AC)/G \cap B$, being isomorphic to a subgroup of AC/B , is abelian of type (r_1, r_2) , $\lambda \geq r_1 \geq r_2$. Since $AC = (AC \cap G)C$, we may take $G = AC \cap G$ without loss of generality. Since trivially $(G \cap B)C/G \cap B$ is projective to C , we may further suppose $G \cap B = 1$. Thus we need only consider the case G abelian of type (r_1, r_2) , $r_i \leq \lambda$. Then $G \times C$ has exponent p^λ . Take any coset representative a of a generator of A/B . Then $\langle a \rangle$ is a cyclic subgroup of $G \times C$ and $A/B \rightarrow \langle a \rangle$ is a projection. $\langle a \rangle C$ is an abelian group of type (λ, r) , $r \leq \lambda$. There exists $D \leq \langle a \rangle C$, $|D| = p^r$ such that $D \cap \langle a \rangle = D \cap C = 1$. Then $\langle a \rangle \rightarrow \langle a \rangle C/D \rightarrow C$ is a chain of projections.

THEOREM 3.7 *Let G be an abelian p -group of type $(\lambda_1, \dots, \lambda_k)$.*

(a) *If $\lambda_2 \geq \lambda$, then G has only one class of projective cyclic quotients of order p^λ .*

(b) *If $\lambda_1 = \lambda + r$, $\lambda_2 < \lambda$, then G has precisely $r + 1$ classes of projective cyclic quotients of order p^λ . If $G = U \times V$ where U is cyclic of order p^{λ_1} , then these classes are the sets of all cyclic quotients of order p^λ of $(U^{p^i} \times V)/U^{p^{i+\lambda}}$ for $i = 0, 1, \dots, r$.*

PROOF. (a) G is the direct product of cyclic groups U_i of orders p^{λ_i} . Suppose A/B is a cyclic quotient of order p^λ , and let a be a coset representative of a generator of A/B . Then $A/B \rightarrow \langle a \rangle / \langle a \rangle \cap B$ is a projection. At least one of $\langle a \rangle \cap U_1$, $\langle a \rangle \cap U_2$ is trivial and therefore at least one of $\langle a \rangle U_1^{p^{\lambda_1 - \lambda}}$, $\langle a \rangle U_2^{p^{\lambda_2 - \lambda}}$ is a direct product. By lemma 8.1, $\langle a \rangle / \langle a \rangle \cap B$ is projective to $U_i^{p^{\lambda_i - \lambda}}$ for $i = 1$ or $i = 2$. But $U_1^{p^{\lambda_1 - \lambda}}$ is projective to $U_2^{p^{\lambda_2 - \lambda}}$. Hence all cyclic quotients of order p^λ are projective to $U_1^{p^{\lambda_1 - \lambda}}$.

(b) Suppose A/B is a cyclic quotient of order p^λ . For some i , $U^{p^i} \times V \geq A$ but $U^{p^{i+1}} \times V \not\geq A$. Then $A = \langle u^{p^i} v, V \rangle$ for some $v \in V$, where $\langle u \rangle = U$. $B \geq A^{p^\lambda}$ and therefore $u^{p^{i+\lambda}} \in B$. Therefore A/B is a quotient of $(U^{p^i} \times V)/U^{p^{i+\lambda}}$. By lemma 8.1, all cyclic quotients of $(U^{p^i} \times V)/U^{p^{i+\lambda}}$ of order p^λ are projective to $U^{p^i}/U^{p^{i+\lambda}}$.

We complete the proof by showing that $A_1/B_1, A_2/B_2$ cyclic quotients of order p^λ , A_1/B_1 a quotient of $(U^{p^i} \times V)/U^{p^{i+\lambda}}$, A_2/B_2 a quotient of $(U^{p^j} \times V)/U^{p^{j+\lambda}}$ and $A_1/B_1 \rightarrow A_2/B_2$ a projection implies $i = j$. If we denote by $\exp G$ the exponent of the group G , then we have $\exp A_1 = p^{\lambda_1 - i} > \exp B_1$ and $\exp A_2 = p^{\lambda_1 - j}$. If $A_1/B_1 \rightarrow A_2/B_2$ is a projection down, then $A_1 = B_1 A_2$ and $\exp A_1 = \max \{ \exp A_2, \exp B_1 \}$. Therefore $\exp A_1 = \exp A_2$ and $i = j$.

The groups $(U^{p^i} \times V)/U^{p^{i+\lambda}}$ $i = 0, 1, \dots, r$ are isomorphic, hence we have:

⁷ The classes of projective quotients of order p in any p -group have also been determined. See Barnes [1], theorem 2.1, Tamaschke [2], theorem 3.3.

COROLLARY 8.2. *If G is a finite abelian p -group and Λ a class of projective cyclic quotients of order p^λ in G , then the groups $F(\Lambda)$, $F^*(\Lambda)$, $H(\Lambda)$, $H^*(\Lambda)$ and $\pi(\Lambda)$ depend only on G and λ , not on the particular class Λ .*

9. Classification of the peaks and pits

LEMMA 9.1. *A/B is a pit in G if and only if A is cyclic. Dually, A/B is a peak if and only if G/B is cyclic.*

PROOF. Trivially, if A is cyclic, then A/B is a pit. If A is not cyclic, take a coset representative a of a generator of A/B . Then $A/B \rightarrow \langle a \rangle / \langle a \rangle \cap B$ is a projection down.

LEMMA 9.2. *Suppose $A/B, C/B$ are pits, $A^{p^{\lambda-1}} = C^{p^{\lambda-1}}$ and E/F is a peak, $E/F \rightarrow A/B$ a projection. Then there is a projection $E/F \rightarrow C/B$.*

PROOF. $F \not\cong C^{p^{\lambda-1}}$, $F \geq B = C^{p^\lambda}$ and therefore $F \cap C = B$. $C/B \rightarrow C \cup F/F$ is a projection. Therefore $|C \cup F : F| = p^\lambda$. But G/F is cyclic and therefore $C \cup F = E$.

LEMMA 9.3. *Let c be a loop in Λ^* , $A/B, C/B$ pits such that $A^{p^{\lambda-1}} = C^{p^{\lambda-1}}$. Let c' be a loop obtained from c by replacing A/B by C/B at some (not necessarily all) occurrences of A/B in c . Let $(c), (c')$ be the homology classes (in Λ^*) of c, c' . Then*

$$(c)H^{*(2)} = (c')H^{*(2)}.$$

PROOF. We consider only the case in which one change is made.

$$c = (\dots \rightarrow E_1/F_1 \rightarrow A/B \rightarrow E_2/F_2 \rightarrow \dots)$$

$$c' = (\dots \rightarrow E_1/F_1 \rightarrow C/B \rightarrow E_2/F_2 \rightarrow \dots).$$

c' is a chain of projections by the previous lemma. Put

$$h = (E_1/F_1 \rightarrow A/B \rightarrow E_2/F_2 \rightarrow C/B \rightarrow E_1/F_1).$$

Then $(c) = (c')(h)$ and $(h) \in H^{*(2)}$.

We define an equivalence relation on the pits, putting $A/B \sim C/D$ if $A^{p^{\lambda-1}} = C^{p^{\lambda-1}}$. Then the above two lemmas state that, in any loop representing an element of H^* , replacing a pit A/B by an equivalent pit gives a loop representing an element of H^* in the same coset of $H^{*(2)}$. Thus working in $H^*/H^{*(2)}$, we may replace pits by equivalent pits.

Dually, we say that the peaks $A/B, A/D$ are equivalent if $A^p B = A^p D$. Then working in $H^*/H^{*(2)}$ we may replace any peak by an equivalent peak.

We now give the classes of equivalent peaks and pits homogeneous coordinates, and find a condition for the existence of a projection from a peak to a pit in terms of the coordinates of the equivalence classes to

which they belong. We call a class of equivalent pits a point and a class of equivalent peaks we call a line. We say that the point P lies on the line l if for some $A/B \in P$ and $C/D \in l$ there is a projection $A/B \rightarrow C/D$. By the lemmas above, if P lies on l , then for every $A/B \in P$ and $C/D \in l$, there is a projection $A/B \rightarrow C/D$. The “plane” consisting of these points and lines with this incidence relation, we denote by Π . It is not a projective plane.

Suppose $G = \langle u_1, \dots, u_k \rangle$, $w_i^{p^{\lambda_i}} = 1$, $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_r \geq \lambda$, $\lambda > \lambda_{r+1} \geq \lambda_{r+2} \geq \dots \geq \lambda_k$. If $A/B \in P$, then A is cyclic and therefore $A = \langle w_1^{x_1} w_2^{x_2} \dots w_k^{x_k} \rangle$ for some x_1, \dots, x_k . P is completely determined by $A^{p^{\lambda-1}} = \langle v_1^{x_1} v_2^{x_2} \dots v_r^{x_r} \rangle$ where $v_i = w_i^{p^{\lambda-1}}$. We take the row vector $\mathbf{x} = (x_1, \dots, x_r)$ as a coordinate vector for P . The x_i are integers mod $p^{\lambda-\lambda+1}$. If t is an integer $\not\equiv 0 \pmod p$, then $t\mathbf{x} = (tx_1, tx_2, \dots, tx_r)$ is again a coordinate vector for P and all coordinate vectors for P can be obtained in this way from any one. The points $P = \{A/B\}$ of Π are in one-to-one correspondence with the non-trivial cyclic subgroups $H = A^{p^{\lambda-1}}$ of $\Omega_{\lambda-1}(G) = \{x^{p^{\lambda-1}} \mid x \in G\}$.

If $l = \{C/D\}$ is a line of Π , then $K = C^p D$ is the same for all peaks $C/D \in l$, and l is determined by K .

$$K \geq \Omega_{\lambda-1}(G) = \{x \mid x \in G, x^{p^{\lambda-1}} = 1\},$$

and G/K is a non-trivial cyclic group. Since the lattice of all subgroups of G is self-dual, the lines of Π are in one-to-one correspondence with the subgroups $K < G$, $K \geq \Omega_{\lambda-1}$ such that G/K is cyclic, such K being the dual of the non-trivial cyclic subgroups H of $\mathcal{O}_{\lambda-1}(G)$. Since for every such K , G/K is isomorphic to a non-trivial subgroup of the additive group Z_{p^μ} of integers mod p^μ , where $\mu = \lambda_1 - \lambda + 1$, the lines of Π are in one-to-one correspondence with the kernels $K/\Omega_{\lambda-1}$ of non-zero homomorphisms of $G/\Omega_{\lambda-1}$ into Z_{p^μ} . If we put $w_i = u_i \Omega_{\lambda-1}$, then $G/\Omega_{\lambda-1} = \{w_1^{x_1} \dots w_r^{x_r}\}$ where the x_i are integers mod $p^{\lambda-\lambda+1}$. Every homomorphism of $G/\Omega_{\lambda-1}$ into Z_{p^μ} has the form $w_1^{x_1} \dots w_r^{x_r} \rightarrow \sum_{i=1}^r l_i x_i p^{\lambda_1 - \lambda_i} \pmod{p^\mu}$, where l_i are integers mod $p^{\lambda-\lambda+1}$. We define the scalar product of the row vectors $\mathbf{l} = (l_1, \dots, l_r)$, $\mathbf{x} = (x_1, \dots, x_r)$ where l_i, x_i are integers mod $p^{\lambda-\lambda+1}$ to be the residue class mod p^μ given by

$$\mathbf{l} \cdot \mathbf{x} = \sum_{i=1}^r l_i x_i p^{\lambda_1 - \lambda_i} \pmod{p^\mu}.$$

Every homomorphism of $G/\Omega_{\lambda-1}$ into Z_{p^μ} then has the form $w_1^{x_1} \dots w_r^{x_r} \rightarrow \mathbf{l} \cdot \mathbf{x}$ and has kernel

$$K/\Omega_{\lambda-1} = \{w_1^{x_1} \dots w_r^{x_r} \mid \mathbf{l} \cdot \mathbf{x} = 0\}.$$

G/K is non-trivial if and only if $\mathbf{l} \neq \mathbf{0}$. We take the row vector \mathbf{l} as a coor-

dinate vector for the line l corresponding to K . If $t \not\equiv 0 \pmod{p}$, then tl is also a coordinate vector for l and all coordinate vectors for l may be obtained in this way.

LEMMA 9.4. *The point P with coordinate vector x lies on the line l with coordinate vector l if and only if*

$$\begin{cases} l \cdot x \neq 0 \\ p l \cdot x = 0 \end{cases} \pmod{p^a}.$$

PROOF. Let A/B be a pit in P , C/D a peak in l and let $K = C^p D$. Clearly, if there exists a projection $A/B \rightarrow C/D$, then $A \not\leq K$, $A^p \leq K$. Conversely, if $A \not\leq K$, $A^p \leq K$ then $A \cap K = A^p$ and $AK/K \simeq A/A^p$. But

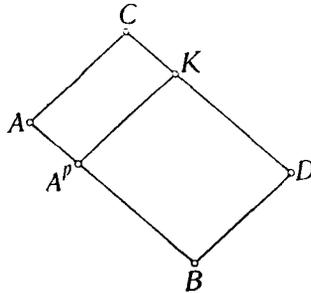


Fig. 4.

G/K is cyclic and has only one subgroup C/K of order p . Hence $AK = C$. G/D is cyclic and $AD \not\leq K$, so $AD > K$. Therefore $AD = C$. $AD/D \simeq A/A \cap D$ and A has only one subgroup B of index p^a . Therefore $A \cap D = B$ and there is a projection $A/B \rightarrow C/D$.

$$\begin{aligned} K &= \{u_1^{\theta_1} \cdots u_r^{\theta_r} u_{r+1}^{\theta_{r+1}} \cdots u_k^{\theta_k} \mid l \cdot (\theta_1, \dots, \theta_r) = 0\}. \\ A &= \langle u_1^{x_1} \cdots u_r^{x_r} u_{r+1}^{x_{r+1}} \cdots u_k^{x_k} \rangle \\ A^p &= \langle u_1^{px_1} \cdots u_k^{px_k} \rangle. \end{aligned}$$

Therefore $A \leq K$ if and only if $l \cdot x = 0$, and $A^p \leq K$ if and only if $pl \cdot x = 0$. Therefore $l \cdot x \neq 0$, $pl \cdot x = 0$ is a necessary and sufficient condition for $A \not\leq K$, $A^p \leq K$ and hence for $P \in l$.

10. The length of H

LEMMA 10.1. *Suppose u, v are vectors such that $u \cdot x = 0$ implies $v \cdot x = 0$. Then $v = \alpha u$ for some integer α .*

PROOF. Let V be the additive group of the row vectors x . With each row vector u , we have associated the homomorphism $u : V \rightarrow Z_{p^a}$ given

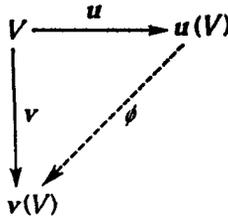


Fig. 5.

by $u(x) = u \cdot x$. By hypothesis, $\ker v \supseteq \ker u$. Therefore there exists a homomorphism $\phi : u(V) \rightarrow v(V)$ such that $v = \phi u$. But Z_{p^m} is cyclic and its subgroups form a chain. Thus $\ker v \supseteq \ker u$ implies $\text{im } v \subseteq \text{im } u$. If z_0 generates $\text{im } u$, then $\phi(z_0) = \alpha z_0$ for some integer α . Since ϕ is a homomorphism, $\phi(z) = \alpha z$ for all $z \in \text{im } u$. That is

$$\begin{aligned} v \cdot x &= \alpha(u \cdot x) \\ &= (\alpha u) \cdot x \end{aligned}$$

for all $x \in V$. Therefore $v = \alpha u$.

LEMMA 10.2. *A necessary and sufficient condition for there to be a line of Π through the points P_1, P_2 with coordinate vectors a, b is that for all integers α, β ,*

$$a \neq \alpha \phi b, \quad b \neq \beta \phi a,$$

that is, P_1, P_2 are distinct collinear points if and only if $\theta a + \phi b = 0$ implies $\theta \equiv \phi \equiv 0 \pmod{p}$.

PROOF. Suppose that $a = \alpha \phi b$ for some integer α . For any line with coordinates l passing through P_2 , $\phi b \cdot l = 0$ and therefore $a \cdot l = 0$. Therefore no line through P_2 passes through P_1 .

Conversely, suppose $a \neq \alpha \phi b, b \neq \beta \phi a$. We have to find l such that

$$\begin{aligned} l \cdot a &\neq 0 & \phi l \cdot a &= 0 \\ l \cdot b &\neq 0 & \phi l \cdot b &= 0. \end{aligned}$$

By lemma 10.1, there exists x such that $\phi a \cdot x = 0, b \cdot x \neq 0$. By replacing x by a suitable multiple, we can find x satisfying also $\phi b \cdot x = 0$. If in addition, we have $a \cdot x \neq 0$, we take $l = x$. Similarly there exists y such that $\phi a \cdot y = 0, \phi b \cdot y = 0$ and $a \cdot y \neq 0$. If also $b \cdot y \neq 0$, then we can take $l = y$. If both $a \cdot x = 0$ and $b \cdot y = 0$, then we take $l = x + y$.

Any loop $c = (A_1/B_1 \rightarrow C_1/D_1 \rightarrow A_2/B_2 \rightarrow \dots \rightarrow A_1/B_1)$ in A^* gives a loop $\bar{c} = (P_1 \xrightarrow{l_1} P_2 \xrightarrow{l_2} \dots \xrightarrow{l_n} P_1)$ in Π , where P_i is the point of Π to which A_i/B_i belongs and l_i is the line of Π to which C_i/D_i belongs. Conversely, to every loop in Π , there corresponds at least one loop in A^* . We define $\bar{c}_1 \sim \bar{c}_2$ if c_1 and c_2 belong to the same coset of $H^{*(2)}$ in H^* . Then

these classes of equivalent loops form a group $\bar{H} \simeq H^*/H^{*(2)}$. We define the length of the loop $\bar{c} = (P_1 \xrightarrow{l_1} P_2 \xrightarrow{l_2} \cdots \xrightarrow{l_n} P_1)$ to be n , the length of an equivalence class to be the length of its shortest member and define $\bar{H}^{(n)}$ to be the subgroup of \bar{H} generated by the classes of length less than or equal to n . We can work with the loops in Π in the same way as with loops in Λ , Λ^* . We observe that replacing in \bar{c} the line l_i passing through the points P_i and P_{i+1} by any other such line l'_i does not change the equivalence class of \bar{c} .

LEMMA 10.3. $\bar{H} = \bar{H}^{(3)}$.

PROOF. Suppose $\bar{c} = (P_1 \rightarrow P_2 \rightarrow \cdots \rightarrow P_n \rightarrow P_1)$ is an irreducible loop in Π of length greater than 3. If there is a line through P_1, P_3 , then

$$\bar{c} = (P_1 \rightarrow P_2 \rightarrow P_3 \rightarrow P_1)(P_1 \rightarrow P_3 \rightarrow \cdots \rightarrow P_1)$$

which is a product of a loop of length 3 and a loop of length $n-1$, contrary to the assumption that \bar{c} is irreducible. Thus if \mathbf{a}_i is a coordinate vector for P_i , either $\mathbf{a}_3 = \alpha\mathbf{a}_1$ or $\mathbf{a}_1 = \alpha\mathbf{a}_3$ for some α . If also there is no line through P_1 and P_4 , then either $\mathbf{a}_4 = \beta\mathbf{a}_1$ or $\mathbf{a}_1 = \beta\mathbf{a}_4$ for some β . Since P_1, P_3 and P_4 are distinct points, in each of these four cases we must have either $\mathbf{a}_3 = \gamma\mathbf{a}_4$ or $\mathbf{a}_4 = \gamma\mathbf{a}_3$ for some γ , contrary to the existence of a line through P_3 and P_4 . Therefore

$$\bar{c} = (P_1 \rightarrow P_2 \rightarrow P_3 \rightarrow P_4 \rightarrow P_1)(P_1 \rightarrow P_4 \rightarrow \cdots \rightarrow P_1),$$

a product of a loop of length 4 and a loop of length $n-2$. Hence no loop of length greater than 4 is irreducible.

Let $\bar{c} = (P_1 \rightarrow P_2 \rightarrow P_3 \rightarrow P_4 \rightarrow P_1)$ be any loop of length 4, and let the coordinates of P_i be \mathbf{a}_i . Either \bar{c} is reducible or P_1 and P_3 are not collinear, and P_2 and P_4 are not collinear. Without loss of generality, we may suppose $\mathbf{a}_3 = \alpha\mathbf{a}_1$ and $\mathbf{a}_4 = \beta\mathbf{a}_2$. Since $P_1 \neq P_2$, $\mathbf{a}_1 + \mathbf{a}_2 \neq \mathbf{0}$. Put $\mathbf{b} = \mathbf{a}_1 + \mathbf{a}_2$. Then the point Q with coordinates \mathbf{b} is collinear with each of the P_i . Therefore

$$\begin{aligned} \bar{c} &= (Q \rightarrow P_1 \rightarrow P_2 \rightarrow Q)(Q \rightarrow P_2 \rightarrow P_3 \rightarrow Q) \\ &\quad (Q \rightarrow P_3 \rightarrow P_4 \rightarrow Q)(Q \rightarrow P_4 \rightarrow P_1 \rightarrow Q). \end{aligned}$$

Therefore every loop of length 4 is reducible and $\bar{H} = \bar{H}^{(3)}$.

THEOREM 4. Suppose G is an abelian p -group of type $(\lambda_1, \dots, \lambda_k)$, $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k$, and let Λ be a class of projective cyclic quotients of order p^λ . If

- (1) $\lambda_2 < \lambda$, or
- (2) $\lambda_3 \geq \lambda$, or
- (3) $\lambda_2 = \lambda$ and $p \neq 2$,

then $H(\Lambda) = H^{(2)}(\Lambda)$ and $H(\Lambda^*) = H^{(2)}(\Lambda^*)$.

PROOF. $H(\Lambda)/H^{(2)}(\Lambda) \simeq H(\Lambda^*)/H^{(2)}(\Lambda^*) \simeq \bar{H}$. $\bar{H}^{(2)}$ is trivial. If $\lambda_2 < \lambda$, then there is only one point and one line in Π and the result follows. For the cases (2), (3), we prove $\bar{H} = \bar{H}^{(2)}$ by showing that every loop of length 3 in Π is reducible. The loop $(P_1 \rightarrow P_2 \rightarrow P_3 \rightarrow P_1)$ is reducible if there is a line passing through all three points. If $\mathbf{a}_i = (a_{i1}, a_{i2}, \dots, a_{ir})$ is the coordinate vector of P_i , then to find such a line, we must find a row vector \mathbf{x} such that

$$\begin{aligned} \mathbf{a}_1 \cdot \mathbf{x} &= \alpha_1 p^{\mu-1} \\ \mathbf{a}_2 \cdot \mathbf{x} &= \alpha_2 p^{\mu-1} \\ \mathbf{a}_3 \cdot \mathbf{x} &= \alpha_3 p^{\mu-1} \end{aligned}$$

with $\alpha_1, \alpha_2, \alpha_3 \not\equiv 0 \pmod{p}$, that is, we must find (x_1, \dots, x_r) such that

$$\sum_j a_{ij} x_j p^{\lambda_1 - \lambda_j} = \alpha_i p^{\mu-1} \pmod{p^\mu}.$$

Put $b_{ij} = a_{ij} p^{\lambda_1 - \lambda_j}$, $B = (b_{ij})$. Then B is a matrix over the ring Z_{p^μ} of integers mod p^μ . If

$$\mathbf{X} = \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} \text{ and } \mathbf{k} = p^{\mu-1} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix},$$

then the equations are $B\mathbf{X} = \mathbf{k}$ where $B, \mathbf{X}, \mathbf{k}$ are matrices over Z_{p^μ} .

We define the degree of the residue $x \pmod{p^\mu}$ to be the index of the highest power of p which divides x if $x \not\equiv 0 \pmod{p^\mu}$, and put degree $x = \mu$ if $x \equiv 0 \pmod{p^\mu}$. There exist matrices P, Q over Z_{p^μ} with inverses P^{-1}, Q^{-1} over Z_{p^μ} such that

$$PBQ = \left(\begin{array}{ccc|c} u & 0 & 0 & 0 \\ 0 & v & 0 & 0 \\ 0 & 0 & w & 0 \end{array} \right)$$

where degree $u \leq \text{degree } v \leq \text{degree } w$. Put $\mathbf{Y} = Q^{-1}\mathbf{X}$. Then the equations $B\mathbf{X} = \mathbf{k}$ have a solution if and only if the equations $PBQ\mathbf{Y} = P\mathbf{k}$ have a solution. These equations have the form

$$\begin{aligned} uy_1 &= \theta \\ vy_2 &= \phi \\ wy_3 &= \psi \end{aligned}$$

where

$$\mathbf{Y} = \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix} \text{ and } \begin{pmatrix} \theta \\ \phi \\ \psi \end{pmatrix} = P\mathbf{k}$$

whence θ, ϕ, ψ have degree $\geq \mu - 1$. Thus the equations certainly have a

solution for all $\alpha_1, \alpha_2, \alpha_3$ if p^μ does not divide w . But p^μ divides w if and only if there exist α, β, γ not all $\equiv 0 \pmod p$ such that

$$\alpha \mathbf{a}_1 + \beta \mathbf{a}_2 + \gamma \mathbf{a}_3 = \mathbf{0}.$$

Thus there exists a solution unless for some numbering of P_1, P_2, P_3 , we have $\mathbf{a}_3 = \alpha \mathbf{a}_1 + \beta \mathbf{a}_2$. Suppose $\mathbf{a}_3 = \alpha \mathbf{a}_1 + \beta \mathbf{a}_2$.

Case 1: $r \geq 3$. If we can find a point Q such that each of the sets $P_1, P_2, Q; P_1, P_3, Q; P_2, P_3, Q$ is a set of three collinear points, then

$$\begin{aligned} (P_1 \rightarrow P_2 \rightarrow P_3 \rightarrow P_1) &= (Q \rightarrow P_1 \rightarrow P_2 \rightarrow Q) \\ &\quad (Q \rightarrow P_2 \rightarrow P_3 \rightarrow Q)(Q \rightarrow P_3 \rightarrow P_1 \rightarrow Q), \end{aligned}$$

and each of the loops on the right is reducible. Since $r \geq 3$, the additive group of row vectors is an abelian group with at least three generators. Therefore there exists a non-trivial cyclic subgroup $\langle \mathbf{b} \rangle$ such that $\langle \mathbf{b} \rangle \cap \langle \mathbf{a}_1, \mathbf{a}_2 \rangle = \mathbf{0}$. Suppose \mathbf{u}, \mathbf{v} are any two of $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$ and $\theta \mathbf{b} + \phi \mathbf{u} + \psi \mathbf{v} = \mathbf{0}$. Then $\theta \mathbf{b} \in \langle \mathbf{b} \rangle \cap \langle \mathbf{a}_1, \mathbf{a}_2 \rangle$ and therefore $\theta \mathbf{b} = \mathbf{0}$, p divides θ and $\phi \mathbf{u} + \psi \mathbf{v} = \mathbf{0}$. But \mathbf{u}, \mathbf{v} correspond to distinct collinear points. Therefore p divides ϕ, ψ . Therefore the point Q with coordinates \mathbf{b} has the required property.

Case 2: $r = 2, \lambda_2 = \lambda, p \neq 2$. Then $\mathbf{a}_1 = (\theta_1, \theta_2), \mathbf{a}_2 = (\phi_1, \phi_2)$. Here θ_2 and ϕ_2 are residues mod p . For some numbering of $\mathbf{a}_1, \mathbf{a}_2$, we have $\phi_1 = t\theta_1$ for some integer t , and $\theta_1 \neq 0$. Put $\mathbf{b} = \mathbf{a}_2 - t\mathbf{a}_1 = (0, \phi_2 - t\theta_2)$ and let Q be the point with coordinates \mathbf{b} . Then Q is collinear with each of the points P_1, P_2, P_3 , and

$$\begin{aligned} (P_1 \rightarrow P_2 \rightarrow P_3 \rightarrow P_1) &= (Q \rightarrow P_1 \rightarrow P_2 \rightarrow Q) \\ &\quad (Q \rightarrow P_2 \rightarrow P_3 \rightarrow Q)(Q \rightarrow P_3 \rightarrow P_1 \rightarrow Q). \end{aligned}$$

It is sufficient to prove each of these three loops reducible.

If \mathbf{u}, \mathbf{v} are any two of $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$, then in each case, one of the three vectors $\mathbf{u}, \mathbf{v}, \mathbf{b}$ is expressible in terms of the other two, as is obvious if \mathbf{u}, \mathbf{v} are $\mathbf{a}_1, \mathbf{a}_2$ or $\mathbf{a}_1, \mathbf{a}_3$. For $\mathbf{u} = \mathbf{a}_2, \mathbf{v} = \mathbf{a}_3 = \alpha \mathbf{a}_1 + \beta \mathbf{a}_2$, we have either $\alpha = r t$ for some r , in which case $\mathbf{a}_3 = (r + \beta) \mathbf{a}_2 - r \mathbf{b}$, or $t = s \alpha$ for some s , in which case $\mathbf{b} = (1 + s\beta) \mathbf{a}_2 - s \mathbf{a}_3$. Thus in each case, $\theta \mathbf{u} + \phi \mathbf{v} + \psi \mathbf{b} = \mathbf{0}$ for some θ, ϕ, ψ not all congruent 0 mod p . But $p \mathbf{b} = \mathbf{0}$. Further, $\theta \mathbf{u} + \phi \mathbf{v} = \mathbf{0}$ implies $\theta \equiv \phi \equiv 0 \pmod p$ since \mathbf{u}, \mathbf{v} correspond to distinct collinear points. Hence $\psi \not\equiv 0 \pmod p$. But $p(0, 1) = \mathbf{0}$ and so if $\theta \equiv \phi \equiv 0 \pmod p$, then $-\psi \mathbf{b}$ has second component 0 and so $\psi \mathbf{b} = \mathbf{0}$. Hence θ, ϕ are not both congruent 0 mod p and we may suppose $\mathbf{v} = \theta \mathbf{u} + \psi \mathbf{b}, \psi \not\equiv 0 \pmod p$. We have thus reduced the problem to the case $\mathbf{a}_3 = \alpha \mathbf{a}_1 + \mathbf{a}_2, \mathbf{a}_2 = (0, 1)$.

For $\mathbf{x} = (x, 1)$, we have $\mathbf{a}_3 \cdot \mathbf{x} = p^{\mu-1}$. Since $\mathbf{a}_1 = (\theta_1, \theta_2)$ with $\theta_1 \neq 0$, we can choose x such that

$$a_1 \cdot x = \begin{cases} p^{\mu-1} & \text{if } \alpha \equiv 0 \pmod{p} \\ \beta p^{\mu-1} & \text{where } \alpha\beta \equiv 1 \pmod{p} \text{ if } \alpha \not\equiv 0 \pmod{p}. \end{cases}$$

Then

$$a_3 \cdot x = \begin{cases} p^{\mu-1} & \text{if } \alpha \equiv 0 \pmod{p} \\ 2p^{\mu-1} & \text{if } \alpha \not\equiv 0 \pmod{p}. \end{cases}$$

Since $p \neq 2$, the line with coordinates x passes through P_1, P_2, P_3 and the loop $(P_1 \rightarrow P_2 \rightarrow P_3 \rightarrow P_1)$ is reducible.

11. The determination of $\pi(\Lambda)$

THEOREM 5. *Let G be an abelian p -group of type $(\lambda_1, \lambda_2, \dots, \lambda_k)$, $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k$, and let Λ be a class of projective cyclic quotients of order p^λ . If $\lambda_2 \geq \lambda$, then $\pi(\Lambda)$ is the group of all automorphisms of the cyclic group of order p^λ . If $\lambda_2 < \lambda$, then $\pi(\Lambda)$ is the group of all automorphisms of the group $\langle x \rangle$ of order p^λ of the form*

$$x \rightarrow x^{1+t p^{\lambda-\lambda_2}} \quad (t \text{ integer}).$$

PROOF. (1) We consider first the case $G = \langle x, y \rangle$, $x^{p^\lambda} = y^{p^\mu} = 1$, $\mu \leq \lambda$. By Theorem 4 (1), $H^* = H^{*(2)}$. Let $c = (A \rightarrow G/B \rightarrow C \rightarrow G/D \rightarrow A)$ be any loop of length 4 in Λ^* . Without loss of generality, we may take $A = \langle x \rangle$, $B = \langle y \rangle$. Since $C \cap B = 1$, $C^{p^{\lambda-1}} \not\leq B$ and therefore $C = \langle xy^r \rangle$ for some r . Since $|D| = p^\mu$ and $D^{p^{\mu-1}} \not\leq A$, $D = \langle x^{sp^e} y \rangle$ for some s , where $e = \lambda - \mu$. If $e \geq 1$, then for any values r, s , we have $\langle xy^r \rangle \cap \langle x^{sp^e} y \rangle = 1$ and there is a loop with these values of r, s . If $e = 0$, then $\langle xy^r \rangle \cap \langle x^s y \rangle = 1$ if and only if $rs \not\equiv 1 \pmod{p}$ and for any values of r, s such that $rs \not\equiv 1 \pmod{p}$, there is a corresponding loop. In this loop c ,

$$\begin{aligned} \langle x \rangle &\rightarrow G/\langle y \rangle \rightarrow \langle xy^r \rangle \rightarrow G/\langle x^{sp^e} y \rangle \rightarrow \langle x \rangle, \\ x &\rightarrow \{xy^t \mid \text{all } t\} \rightarrow xy^r \rightarrow \{x^{1+isp^e} y^{r+t} \mid \text{all } t\} \rightarrow x^{1-rsp^e}. \end{aligned}$$

Thus $\alpha(c) = x^{1-rsp^e}$. If $e = 0$, then every automorphism of $\langle x \rangle$ is given by some values of r, s . If $e \geq 1$, then every automorphism of the form $x \rightarrow x^{1+isp^e}$ is given by some values of r, s , and since these automorphisms form a group, $\pi(\Lambda)$ contains only these automorphisms.

(2) If $\lambda_2 \geq \lambda$, then by (1), all automorphisms of the cyclic group of order p^λ are given by loops of length 4 within $\Omega_\lambda(G)$, and therefore $\pi(\Lambda)$ is the group of all automorphisms of the cyclic group of order p^λ .

(3) Suppose $\lambda_2 < \lambda$. Since $\pi(\Lambda)$ does not depend on the class Λ , we need only consider the class Λ contained in $\Omega_\lambda(G)$. Hence we may suppose $\lambda_1 = \lambda$. By Theorem 4 (1), $H(\Lambda) = H^{(2)}(\Lambda)$ and it is sufficient to find $\alpha(c)$ for all loops c of length 4. If A/B is a pit, then $B = 1$. Let

$$c = (A \rightarrow G/B \rightarrow C \rightarrow G/D \rightarrow A)$$

be any loop of length 4 in A^* . Then c is homotopic (in A) to

$$A \rightarrow (A \cup C)/(A \cup C) \cap B \rightarrow C \rightarrow (A \cup C)/(A \cup C) \cap D \rightarrow A.$$

Thus to determine the $\alpha(c)$ given by loops of length 4 in A , it is sufficient to determine the $\alpha(c)$ given by loops of length 4 within the two-generator subgroups of G . Since every two-generator subgroup of exponent p^λ of G is isomorphic to a subgroup of the group of type (λ, λ_2) , the result follows from (1).

References

- [1] Barnes, D. W., Lattice embeddings of prime power groups, *This Journal* 2 (1961) 17–34.
- [2] Tamaschke, O., Die Kongruenzrelationen im Verband der zugänglichen Subnormalteiler, *Math. Zeitschr.* 75 (1961) 115–126.
- [3] Seifert, H. and Threlfall, W., *Lehrbuch der Topologie*. New York, 1947.
- [4] Zassenhaus, H., *The theory of groups*. Second English edition. New York, 1958.

University of Sydney.