THE STRUCTURE OF THE GROUP RING OF A p-GROUP OVER A MODULAR FIELD

BY

S. A. JENNINGS

This paper deals with the group ring of a group of prime power order over the prime field $GF(p)$, where p is the prime dividing the order of the group. It is well known that in the case of the group ring of a group over a field whose characteristic divides the order of the group, the ordinary theory of group characters is no longer valid: recently, Brauer and Nesbitt([1]) have investigated the properties of the modular representations in this case, but this general theory yields only little in the special case that we consider here. We investigate the group ring from the point of view of the structure of its radical, and in particular, determine a basis for, and the ranks of, the various powers of the radical in terms of the elements and order of a new series of characteristic subgroups. These subgroups are defined by a certain minimal property which combines the commutator and the pth power structure of the group, and should prove useful in general investigations on the structure of p-groups.

1. It is well known that the group ring of a group of order g is semi-simple, provided the characteristic of the underlying field is zero, or a prime which does not divide g([2]). If, however, the underlying field has characteristic p, and p divides g, then it is readily seen that the group ring has a radical which is not zero. Let the elements of the group be $G_1=1, G_2, \cdots, G_g$. Consider the element $\sigma=G_1+G_2+\cdots+G_g$ in the group ring. We have $\sigma\cdot G_i=\sigma$, and hence, if $A=\sum\alpha_iG_i$ is any element in the ring, $\sigma\cdot A=A\cdot\sigma=(\sum\alpha_i)\cdot\sigma$; that is, scalar multiples of σ form an ideal (σ). However, $(\sigma)\cdot(\sigma)=0$, since $\sigma\cdot\sigma=\sigma\cdot(\sum 1)=0$, $((\sum 1)=g\equiv 0$ modulo $p)$, and hence the group ring contains a nilpotent ideal different from zero. We have proved([3]), therefore,

THEOREM 1.1. *The group ring of a group over a field whose characteristic divides the order of the group is not semi-simple.*

We investigate the structure of the group ring in the extreme case, where

Presented to the Society, October 28, 1939; received by the editors November 24, 1939, and, in revised form, September 20, 1940.

The essentials of this paper comprise a thesis submitted in conformity with the requirements for the degree of Doctor of Philosophy at the University of Toronto, May, 1939. It was written under the direction of Professor Richard Brauer, and I would like to acknowledge my debt to him for the assistance and encouragement that he gave me.

([1]) R. Brauer and C. Nesbitt, University of Toronto Studies, Mathematical Series, no. 4.

([2]) See, for example, van der Waerden, *Moderne Algebra*, vol. 2, §125.

([3]) E. Noether, Mathematische Zeitschrift.

the order of the group is a power of the characteristic of the underlying field. In what follows, $\mathfrak{G}$ is a p-group of order p^a, and Γ is the group ring of $\mathfrak{G}$ over the prime field $GF(p)$. Where necessary, we emphasize the fact that Γ is the group ring of $\mathfrak{G}$ by writing $\Gamma=\Gamma(\mathfrak{G})$.

We prove first the following

THEOREM 1.2. *The radical, $\mathfrak{N}$, of the group ring Γ of a p-group $\mathfrak{G}$ of order p^a over the field $GF(p)$ is of rank p^a-1, and has as basis all elements of the form G_i-1, where $G_i\in\mathfrak{G}$, $G_i\neq 1$. A necessary and sufficient condition that an element $A=\sum\alpha_iG_i$ of Γ lie in $\mathfrak{N}$ is that $\sum\alpha_i=0$. The semi-simple part of Γ is of rank one and is isomorphic to $GF(p)$.*

It is known that the only irreducible modular representation of $\mathfrak{G}$ is the 1-representation(4) and hence, if $\mathfrak{A}$ is any representation of $\mathfrak{G}$, $\mathfrak{A}$ may be transformed to the form

$$\mathfrak{A}\sim\begin{pmatrix}(1)&&\\&\ddots&\\*&&(1)\end{pmatrix}.$$

Every representation of $\mathfrak{G}$ also gives a representation of Γ. In particular, if we take for $\mathfrak{A}$ the regular representation of $\mathfrak{G}$, we obtain a (1:1) representation of Γ. Every element of the form (G_i-1), where $G_i\in\mathfrak{G}$, is represented by matrices

$$G_i-1\leftrightarrow\begin{pmatrix}0&&\\&\ddots&\\*&&0\end{pmatrix} \tag{1.3}$$

with zeros in the main diagonal. All elements which are represented by matrices of this form with zeros in and above the main diagonal form a nilpotent ideal, and hence G_i-1 belongs to the radical $\mathfrak{N}$ of Γ. Since there are p^a-1 independent elements G_i-1, the rank of $\mathfrak{N}$ is at least p^a-1. Since Γ is of rank p^a, $\Gamma/\mathfrak{N}$ is of rank 0 or 1. The element 1 is not in $\mathfrak{N}$, however, since it is not nilpotent; and hence the rank of Γ is p^a-1, and the rank of $\Gamma/\mathfrak{N}$ is 1. It follows that $\Gamma/\mathfrak{N}\simeq GF(p)$. That the elements G_i-1 form a basis for $\mathfrak{N}$ follows, since there are p^a-1 of them, and they are independent. The remainder of the theorem is immediate(5).

COROLLARY 1.4. *If G is any element of $\mathfrak{G}$, then $G\equiv 1$ modulo $\mathfrak{N}$.*

The corollary follows from the fact that $G-1\equiv 0$ modulo $\mathfrak{N}$.

(4) L. E. Dickson, these Transactions, vol. 8 (1907), pp. 389–398. Cf. also Brauer and Nesbitt, loc. cit.

(5) L. Lombardo-Radici, in a recent paper has given a group-theoretical proof of Theorem 1.2.

2. When $\mathfrak{N}$ is the radical of Γ, we may form the various powers of $\mathfrak{N}$(6)

$$\mathfrak{N} \supset \mathfrak{N}^2 \supset \cdots \supset \mathfrak{N}^L \supset \mathfrak{N}^{L+1} = 0. \tag{2.1}$$

$\mathfrak{N}^w$ consists of sums of products of w elements of $\mathfrak{N}$. If the situation is as in (2.1) with $\mathfrak{N}^L \neq 0$, $\mathfrak{N}^{L+1}=0$, we say that L is the *exponent* of $\mathfrak{N}$. We define $\mathfrak{N}^0=\Gamma$.

Let $\mathfrak{K}_\lambda$ be the set of all elements $K_\lambda \in \mathfrak{G}$ such that $K_\lambda \equiv 1$ modulo $\mathfrak{N}^\lambda$. $\mathfrak{K}_\lambda$ is a subgroup of $\mathfrak{G}$, since if K_λ, $K_\lambda' \equiv 1$ modulo $\mathfrak{N}^\lambda$, then $K_\lambda K_\lambda' \equiv 1$ modulo $\mathfrak{N}^\lambda$. Moreover, $\mathfrak{K}_\lambda$ is a self-conjugate subgroup of $\mathfrak{G}$, for if G is any element of $\mathfrak{G}$ then $G^{-1}K_\lambda G \equiv 1$ modulo $\mathfrak{N}^\lambda$, since $\mathfrak{N}^\lambda$ is an ideal of Γ. Indeed, it is clear that $\mathfrak{K}_\lambda$ is a characteristic subgroup of $\mathfrak{G}$, since any automorphism of $\mathfrak{G}$ leaves $\mathfrak{N}$ and its powers unaltered. Since $\mathfrak{N}^\lambda \supset \mathfrak{N}^\mu$ for $\lambda < \mu$, we have $\mathfrak{K}_\lambda \supseteq \mathfrak{K}_\mu$, $\lambda < \mu$. By Corollary 1.4 $\mathfrak{K}_1 = \mathfrak{G}$, and by (2.1) $\mathfrak{K}_{L+1}=1$. We have proved, therefore,

THEOREM 2.2. *The sets* $\mathfrak{K}_\lambda$, $\lambda = 1, 2, \cdots$, *consisting of group elements which may be written in the form* $1+n_\lambda$, $n_\lambda \in \mathfrak{N}^\lambda$, *form a decreasing series of characteristic subgroups of* $\mathfrak{G}$:

$$\mathfrak{G} = \mathfrak{K}_1 \supseteq \mathfrak{K}_2 \supseteq \cdots \supseteq \mathfrak{K}_{L+1} = 1.$$

We shall refer to these subgroups as the $\mathfrak{K}$-series of the group $\mathfrak{G}$(7). We write $\mathfrak{K}_\lambda(\mathfrak{G})$ for $\mathfrak{K}_\lambda$ when necessary to stress the fact that $\mathfrak{K}_\lambda$ is a member of the $\mathfrak{K}$-series of a particular group $\mathfrak{G}$.

THEOREM 2.3. *The* $\mathfrak{K}$*-series of any group* $\mathfrak{G}$ *has the following properties*

(1) $(\mathfrak{K}_\lambda, \mathfrak{K}_\mu) \subseteq \mathfrak{K}_{\lambda+\mu}$(8),

(2) $K_i^p \in \mathfrak{K}_{ip}$ *if* $K_i \in \mathfrak{K}_i$.

As a consequence of (1) *and* (2), *we have*

(3) $\mathfrak{K}_\lambda/\mathfrak{K}_{2\lambda}$ *is abelian of type* $(p, p, \cdots, p)$.

Proof. To prove (1) we must show that if $K_\lambda \in \mathfrak{K}_\mu$, $K_\mu' \in \mathfrak{K}_\mu$, then $K_\lambda^{-1}K_\mu'^{-1}K_\lambda K_\mu' \in \mathfrak{K}_{\lambda+\mu}$. Now if $K_\lambda \in \mathfrak{K}_\lambda$, $K_\mu' \in \mathfrak{K}_\mu$, we may write

$$\begin{aligned} K_\lambda &= 1 + n_\lambda, & n_\lambda &\in \mathfrak{N}^\lambda, \\ K_\mu' &= 1 + n_\mu', & n_\mu' &\in \mathfrak{N}^\mu, \end{aligned} \tag{2.4}$$

and we have

(6) Cf. Dickson, *Algebren und ihre Zahlentheorie*, chap. 6.

(7) In a paper which appeared after the present paper had been written, H. Zassenhaus has described (*Ein Verfahren, jeder endlichen p-Gruppe einen Lie-Ring mit Charakteristik p zuzuordnen*, Abhandlungen aus dem mathematischen Seminar der Hamburgischen Universität, vol. 13 (1939), pp. 200–206), for a given p-group, a series which he calls "the dimensional groups modulo p." This series appears to be identical with our $\mathfrak{K}$-series. It is interesting that these groups should arise both from the ring, and from the Lie-algebra associated with a p-group over a modular field.

(8) For this notation, see P. Hall, *A contribution to the theory of groups of prime power orders*, Proceedings of the London Mathematical Society, vol. 36 (1933–1934), pp. 29–95, especially §2.

$$K_\lambda^{-1}K_\mu'^{-1}K_\lambda K_\mu = 1 + K_\lambda^{-1}K_\mu'^{-1}(K_\lambda K_\mu' - K_\mu' K_\lambda)$$
$$= 1 + K_\lambda^{-1}K_\mu'^{-1}((1+n_\lambda)(1+n_\mu') - (1+n_\mu')(1+n_\lambda))$$
$$= 1 + K_\lambda^{-1}K_\mu'^{-1}(n_\lambda n_\mu' - n_\mu' n_\lambda) = 1 + \bar{n}_{\lambda+\mu}$$

where $\bar{n}_{\lambda+\mu} \in \mathfrak{N}^{\lambda+\mu}$, which proves that $(K_\lambda, K_\mu') \equiv 1$ modulo $\mathfrak{N}^{\lambda+\mu}$. Again, if $K_i \in \mathfrak{K}_i$, then $K_i = 1 + n_i$, where $n_i \in \mathfrak{N}^i$; and since 1 and n_i permute, and we are in a field of characteristic p, we have

$$K_i^p = (1 + n_i)^p = 1 + n_i^p,$$

which shows that $K_i^p \equiv 1$ modulo $\mathfrak{N}^{ip}$, and proves (2). Statement (3) follows readily from (1) and (2).

Theorem 2.4, (1), shows that the $\mathfrak{K}$-series is a central series of $\mathfrak{G}$, as defined by Hall(9).

By 2.4, (3), $\mathfrak{K}_\lambda/\mathfrak{K}_{\lambda+1}$ is elementary abelian. Let $\mathfrak{K}_\lambda/\mathfrak{K}_{\lambda+1}$ be of order p^{d_λ} (it may happen that $d_\lambda = 0$ if $\mathfrak{K}_\lambda = \mathfrak{K}_{\lambda+1}$), and let $F_{\lambda,1}, \cdots, F_{\lambda,d_\lambda}$ be a complete set of representatives in $\mathfrak{G}$ of a minimal basis for $\mathfrak{K}_\lambda/\mathfrak{K}_{\lambda+1}$ (again if $\mathfrak{K}_\lambda = \mathfrak{K}_{\lambda+1}$ we set $F_{\lambda,i} = 1$). Then any element $G \in \mathfrak{G}$ may be written

$$G = F_{1,1}^{x_{1,1}} F_{1,2}^{x_{1,2}} \cdots F_{1,d}^{x_{1,d_1}} \cdots F_{\lambda,1}^{x_{\lambda,1}} \cdots F_{\lambda,d_\lambda}^{x_{\lambda,d_\lambda}} \cdots \tag{2.5}$$

where $0 \leqq x_{\lambda,i} < p$, and the $x_{\lambda,i}$ are uniquely determined modulo p.

If $F_{\lambda,i} \neq 1$, then $F_{\lambda,i}$ is not in $\mathfrak{K}_{\lambda+1}$, and hence $(F_{\lambda,i} - 1)$ is in $\mathfrak{K}_\lambda$, and not in $\mathfrak{K}_{\lambda+1}$. Suppose K_λ is any element of $\mathfrak{K}_\lambda$. Using (2.5) we may write

$$K_\lambda \equiv F_{\lambda,1}^{x_{\lambda,1}} \cdots F_{\lambda,d_\lambda}^{x_{\lambda,d_\lambda}} \text{ modulo } \mathfrak{K}_{\lambda+1}, \qquad 0 \leqq x_{\lambda,i} < p,$$

where the $x_{\lambda,i}$ are uniquely determined. Using the identity

$$(AB - 1) = (A - 1)(B - 1) + (A - 1) + (B - 1) \tag{2.6}$$

we readily obtain

$$K_\lambda - 1 \equiv \sum_i x_{\lambda,i}(F_{\lambda,i} - 1) \text{ modulo } \mathfrak{N}^{\lambda+1} \tag{2.7}$$

(since $x_{\lambda,i} < p$, we may suppose $x_{\lambda,i}$ in the underlying field). Conversely, if $K_\lambda \in \mathfrak{K}_\lambda$, and we have a relation of the form

$$K_\lambda - 1 \equiv \sum_i y_{\lambda,i}(F_{\lambda,i} - 1) \text{ modulo } \mathfrak{N}^{\lambda+1}, \qquad y_{\lambda,i} \in GF(p),$$

this implies that

$$K_\lambda \equiv F_{\lambda,1}^{y_{\lambda,1}} \cdots F_{\lambda,d_\lambda}^{y_{\lambda,d_\lambda}} \text{ modulo } \mathfrak{K}_{\lambda+1}, \qquad 0 \leqq y_{\lambda,i} < p.$$

From these facts we obtain

(9) Hall, loc. cit., §2.4.

THEOREM 2.8. *A minimal generating set* $\{F_{\lambda,1}, \cdots, F_{\lambda,d_\lambda}\}$ *for* $\mathfrak{R}_\lambda$ *modulo* $\mathfrak{R}_{\lambda+1}$ *may be taken as any maximal set of elements* $F_{\lambda,i}$ *of* $\mathfrak{R}_\lambda$ *for which* $(F_{\lambda,i}-1)$ *are linearly independent modulo* $\mathfrak{N}^{\lambda+1}$.

3. We are now in a position to determine a basis for $\mathfrak{N}^\lambda$ modulo $\mathfrak{N}^{\lambda+1}$ in terms of the elements $F_{\lambda,i}$ defined above. For fixed w consider all products of the form

$$\prod_{i,\lambda} (F_{\lambda,i}-1)^{\alpha_{\lambda,i}}, \qquad 0 \leqq \alpha_{\lambda,i} < p, \tag{3.1}$$

with $\sum_{i,\lambda}(\lambda\alpha_{\lambda,i})=w$, the summation extending over the same λ and i as in the product. We insist that in such a product those factors which are present shall be in the natural order of increasing i and λ, as in (2.5). Let us call the various distinct products (3.1)

$$N_1^{(w)}, N_2^{(w)}, \cdots, N_{l_w}^{(w)}.$$

We define w to be the "weight" of these products. Letting $w=1, 2, 3, \cdots$, we obtain exactly p^a-1 such products which are formally distinct, since $d_1+d_2+\cdots=a$. However, any element of the form $G-1$, where $G\in\mathfrak{G}$, may be expressed as a linear combination of the $N_\lambda^{(w)}$, since by (2.5) $G-1=(\prod F_{\lambda,i}^{\alpha_{\lambda,i}})-1$ and by using the identity (2.6) a sufficient number of times we get the result. Hence, using Theorem 1.2, we see that the products $N_\lambda^{(w)}$ are independent, and form a basis for $\mathfrak{N}$.

We prove now the following:

THEOREM 3.2. *The elements* $N_\lambda^{(i)}$, *with* $i\geqq w$, *form a basis for* $\mathfrak{N}^w$.

Proof. Certainly the $N_\lambda^{(i)}$ lie in $\mathfrak{N}^w$, and are independent. We have to show that every $n_w\in\mathfrak{N}^w$ can be expressed as a linear combination of these elements. Suppose the theorem false. Let w be the largest power of $\mathfrak{N}$ for which the theorem does not hold (such a largest power exists since the theorem is true for $w=L+1$), and let $n_w\in\mathfrak{N}^w$ be an element which cannot be expressed linearly in terms of the $N_\lambda^{(i)}$. Then there is no relation of the form

$$n_w \equiv \sum_\lambda c_\lambda N_\lambda^{(w)} \text{ modulo } \mathfrak{N}^{w+1}$$

where the c_λ are in the underlying field, since otherwise $n_w-\sum c_\lambda N_\lambda^{(w)}$, which is in $\mathfrak{N}^{w+1}$, could be expressed by $N_\mu^{(j)}$ with $j\geqq w+1$, by our choice of w, and we would obtain a contradiction.

Now by the definition of $\mathfrak{N}^w$, n_w may be written, modulo $\mathfrak{N}^{w+1}$, in the form

$$n_w \equiv \sum \prod_i (F_{1,\rho_i}-1) \qquad (w \text{ factors}). \tag{3.3}$$

There must be at least one product $\prod_i(F_{1,\rho_i}-1)$ which, modulo $\mathfrak{N}^{w+1}$, is linearly independent of the $N_\lambda^{(w+1)}$.

More generally, consider all products

$$\pi = \prod_i (F_{\sigma_i,\tau_i} - 1) \qquad \text{with } \sum_i \sigma_i = w. \tag{3.4}$$

A product π is here taken as "higher" than a product π' if the number of factors with $\sigma_i = w$ is greater in π than in π'; if they have the same number of such factors, then π is "higher" than π' if π has the greater number of factors with $\sigma_i = w-1$, etc. We select a highest product π (cf. (3.4)) which is linearly independent of the $N_\lambda^{(w)}$ modulo $\mathfrak{N}^{w+1}$.

We show now that if π is chosen thus, and if we interchange two consecutive factors in π, then the new product thus obtained (which is as "high" as π), again is linearly independent of the $N_\lambda^{(w)}$.

Let $(A-1)$ and $(B-1)$ be the two factors in π to be interchanged, A being in $\mathfrak{R}_\rho$ and B in $\mathfrak{R}_\sigma$. Set $\pi = \pi_1(B-1)\cdot(A-1)\pi_2$. Using the identity

$$(B-1)\cdot(A-1) = (A-1)\cdot(B-1) + (AB-1)\cdot(C-1) + (C-1) \tag{3.5}$$

where $C=(B, A)$, we obtain

$$\pi = \pi_1(A-1)\cdot(B-1) + \pi_1(AB-1)\cdot(C-1)\pi_2 + \pi_1(C-1)\pi_2.$$

Using (2.4), (1) we see that the second term on the right is in $\mathfrak{N}^{w+1}$, and the factor $(C-1)$ is in $\mathfrak{N}^{\rho+\sigma}$, whence, using (2.5) and (2.7), we get a formula of the form

$$\pi \equiv \pi_1(A-1)(B-1)\pi_2 + \sum_\mu a_\mu \pi_1(F_{\rho+\sigma,\mu} - 1)\pi_2 \text{ modulo } \mathfrak{N}^{w+1}, \qquad a_\mu \in GF(p).$$

All terms of the form $\pi_1(F_{\rho+\sigma,\mu}-1)\pi_2$ are "higher" than π, however, and can therefore be expressed by the $N_\lambda^{(w)}$, modulo $\mathfrak{N}^{w+1}$, and since π is independent of the $N_\lambda^{(w)}$, so is $\pi_1(A-1)(B-1)\pi_2$.

We may therefore take the factors in π in any order we please, and still have a product which is independent of the $N_\lambda^{(w)}$. Order the factors in π as in (3.1):

$$\pi = \prod_i (F_{i,\nu} - 1)^{\beta_{i,\nu}}, \qquad \sum_i (i\beta_{i,\nu}) = w.$$

Suppose an exponent $\beta_{i,\nu}$ were greater than $p-1$. We replace $(F_{i,\nu}-1)^p$ by $(F_{i,\nu}^p-1)$, and since $F_{i,\nu}^p \in \mathfrak{R}_{ip}$, we use (2.7) to express $(F_{i,\nu}-1)^p$ in the form

$$(F_{i,\nu} - 1)^p \equiv \sum_\mu c_\mu (F_{ip,\mu} - 1) \text{ modulo } \mathfrak{N}^{ip+1}.$$

On making this substitution for $(F_{i,\nu}-1)^p$ in π we get π expressed as a sum of terms all "higher" than π, which is impossible, since π is independent of the $N_\lambda^{(w)}$ and these "higher" terms are not. However, if all the $\beta_{i,\nu}$ are less than p, then π itself is an $N_\lambda^{(w)}$. In any case we get a contradiction, and Theorem 3.2 is therefore proven.

As immediate corollaries we have:

THEOREM 3.6. *The elements $N_\lambda^{(w)}$ for fixed w form a basis of $\mathfrak{N}^w$ modulo $\mathfrak{N}^{w+1}$. The number l_w of these elements is equal to the rank of $\mathfrak{N}^w/\mathfrak{N}^{w+1}$.*

THEOREM 3.7. *The rank l_w of $\mathfrak{N}^w/\mathfrak{N}^{w+1}$ is equal to the coefficient of x^w in the expansion of*

$$(1 + x + x^2 + \cdots + x^{p-1})^{d_1}\cdot(1 + x^2 + x^4 + \cdots + x^{2(p-1)})^{d_2}\cdots \cdot(1 + x^\lambda + x^{2\lambda} + \cdots + x^{\lambda(p-1)})^{d_\lambda}\cdots$$

and the exponent L of $\mathfrak{N}$ is equal to $\sum_\lambda \lambda d_\lambda(p-1)$.

To prove Theorem 3.7 we need only notice that the coefficient of x^w is the number of ways of selecting the formally distinct products (3.1).

The set of numbers $(L; l_1, \cdots, l_L)$ has been called the "genus" of the radical by Hazlett([10]). They determine, to a certain extent, the structure of $\mathfrak{N}$. We have obtained an explicit expression for the genus of the radical of the group ring of a p-group in terms of the orders of the $\mathfrak{K}$-series of the group.

4. In this section we establish certain properties of the $\mathfrak{K}$-series which are necessary to identify this series abstractly. We proceed at once to prove:

THEOREM 4.1. *If $\mathfrak{H}$ is a self-conjugate subgroup of $\mathfrak{G}$, and $\mathfrak{H}\subseteq\mathfrak{K}_i(\mathfrak{G})$, then the $\mathfrak{K}$-series of $\mathfrak{G}/\mathfrak{H}$ starts with $\mathfrak{G}/\mathfrak{H}$, $\mathfrak{K}_2/\mathfrak{H}$, $\cdots$, $\mathfrak{K}_i/\mathfrak{H}$, that is,*

$$\mathfrak{K}_\lambda(\mathfrak{G}/\mathfrak{H}) \simeq \mathfrak{K}_\lambda(\mathfrak{G})/\mathfrak{H}, \qquad \lambda \leqq i.$$

Let $\mathfrak{G}/\mathfrak{H}=\mathfrak{G}'$. Then we have a homomorphic mapping $\mathfrak{G}\to\mathfrak{G}'$. Let Γ' be the group ring of $\mathfrak{G}'$ over the field $GF(p)$. The homomorphism above can be extended to a homomorphism of Γ upon Γ' in a natural manner as follows. Let $\{\overline{G}_\mu\}$ be a complete set of representatives in $\mathfrak{G}$ of $\mathfrak{G}/\mathfrak{H}$, and let H_ν, $\nu=1, 2, \cdots$, be the elements of $\mathfrak{H}$. Every element $\gamma\in\Gamma$ may be written therefore

$$\gamma = \sum_{\mu,\nu} c_{\mu,\nu}\overline{G}_\mu H_\nu \qquad C_{\mu,\nu}\in GF(p).$$

In the mapping $\mathfrak{G}\to\mathfrak{G}'$, every element $\overline{G}_\mu H_\nu\to\overline{G}_\mu\mathfrak{H}$. A mapping of Γ upon Γ' can be defined thus:

$$\gamma = \sum c_{\mu,\nu}\overline{G}_\mu H_\nu \to \gamma' = \sum_\mu\Big(\sum_\nu c_{\mu\nu}\Big)\overline{G}_\mu\mathfrak{H}. \tag{4.2}$$

It is readily verified that the mapping as given by (4.2) is a homomorphism. Consider those elements of Γ which map into 0 in Γ': if γ is such an element, by (4.2) we must have $\sum_\nu c_{\mu,\nu} = 0$ and hence we may write

$$\gamma = \sum c_{\mu,\nu}\overline{G}_\mu(H_\nu - 1);$$

([10]) O. Hazlett, *On the classification and invariantive characterization of nilpotent algebras*, American Journal of Mathematics, vol. 6 (1905), pp. 109–138. Cf. also G. Pickert, Mathematische Annalen, vol. 116 (1938), pp. 217–280.

and since $\mathfrak{H} \subseteq \mathfrak{K}_i(\mathfrak{G})$, we see that $\gamma \in \mathfrak{N}^i(\Gamma)$. Hence if γ and γ_1, in Γ, map into the same element in Γ', then

$$\gamma \equiv \gamma_1 \text{ modulo } \mathfrak{N}^i(\Gamma).$$

It is clear that $\mathfrak{N}(\Gamma)$ maps upon a subset of $\mathfrak{N}(\Gamma')$, and hence $\mathfrak{N}(\Gamma)^\rho$ maps upon a subset of $\mathfrak{N}(\Gamma')^\rho$. Conversely, if $\nu' = \sum c_\nu(\overline{G}_\nu \mathfrak{H} - 1)$, C_ν in $GF(p)$, is an element of Γ', the element $\nu = \sum c_\nu(\overline{G}_\nu - 1)$ of Γ is mapped upon ν'. It follows that if ν_ρ' is an element of $\mathfrak{N}(\Gamma')^\rho$, we may find an element ν_ρ of $\mathfrak{N}(\Gamma)^\rho$ with this image ν_ρ'. If $\tilde{\nu}_\rho$ is any other element of Γ with this image, then $\nu_\rho \equiv \tilde{\nu}_\rho$ modulo $\mathfrak{N}^i$, according to the remark above. If $\rho \leqq i$, then $\tilde{\nu}_\rho \equiv \nu_\rho \equiv 0$ modulo $\mathfrak{N}(\Gamma)^\rho$. Hence, for $\rho \leqq i$, the elements of $\mathfrak{N}(\Gamma)^\rho$ and only these elements are mapped upon elements of $\mathfrak{N}(\Gamma')^\rho$. This implies that $\mathfrak{K}_\rho(\mathfrak{G})$ is mapped upon $\mathfrak{K}_\rho(\mathfrak{G}')$ and hence $\mathfrak{K}_\rho(\mathfrak{G})/\mathfrak{H} \simeq \mathfrak{K}_\rho(\mathfrak{G}')$ for $\rho \leqq i$.

5. Consider any central series of $\mathfrak{G}$

$$\mathfrak{G} = \mathfrak{F}_1 \supseteq \mathfrak{F}_2 \supseteq \mathfrak{F}_3 \supseteq \cdots \tag{5.1}$$

such that

(1) $(\mathfrak{F}_i, \mathfrak{G}) \subseteq \mathfrak{F}_{i+1}$,

(2) $F_i^p \in \mathfrak{F}_{ip}$ if $F_i \in \mathfrak{F}_i$.

The $\mathfrak{K}$-series is such a one, with the stronger property (2.4), (1).

Among all the series (5.1) there is a minimal series

$$\mathfrak{G} = \mathfrak{M}_1 \supseteq \mathfrak{M}_2 \supseteq \mathfrak{M}_3 \supseteq \cdots \tag{5.2}$$

which is defined by

$$\mathfrak{M}_i = \{(\mathfrak{M}_{i-1}, \mathfrak{G}), \mathfrak{M}_{(i/p)}^{(p)}\},$$

(i/p) being the least integer $\geqq i/p$, and $\mathfrak{M}_\lambda^{(p)}$ the set of all pth powers of elements of $\mathfrak{M}_\lambda$. It is easily verified that $\mathfrak{F}_i \supseteq \mathfrak{M}_i$, for any series (5.1), and in particular

$$\mathfrak{K}_i \supseteq \mathfrak{M}_i. \tag{5.3}$$

We call the series (5.2) the $\mathfrak{M}$-series of $\mathfrak{G}$. Where necessary we write $\mathfrak{M}_\lambda = \mathfrak{M}_\lambda(\mathfrak{G})$ to stress the fact that we are discussing the $\mathfrak{M}$-series of the particular group $\mathfrak{G}$. It is obvious that we have the following:

THEOREM 5.4. *If $\mathfrak{H}$ is a self-conjugate subgroup of $\mathfrak{G}$, then the subgroup $\mathfrak{M}_\lambda(\mathfrak{G})$ maps on the subgroup $\mathfrak{M}_\lambda(\mathfrak{G}/\mathfrak{H})$ in the homomorphism of $\mathfrak{G}$ upon $\mathfrak{G}/\mathfrak{H}$.*

We proceed to prove:

THEOREM 5.5[11]. *The $\mathfrak{K}$-series and $\mathfrak{M}$-series of $\mathfrak{G}$ are identical.*

[11] I am indebted to Professor R. Brauer for the definition of the $\mathfrak{M}$-series and for the subsequent proof of Theorem 5.5.

Proof. Suppose that we know already $\mathfrak{M}_i = \mathfrak{K}_i$ for $i = 1, 2, \cdots, t$, so that we have

$$\begin{aligned} \mathfrak{G} = \mathfrak{M}_1 = \mathfrak{K}_1 \supseteq \mathfrak{M}_2 = \mathfrak{K}_2 \supseteq \cdots \supseteq \mathfrak{M}_t = \mathfrak{K}_t \\ \supseteq \mathfrak{K}_{t+1} \supseteq \mathfrak{M}_{t+1} \supseteq \cdots . \end{aligned} \tag{5.6}$$

We apply (4.1) and (5.4) with $\mathfrak{H} = \mathfrak{M}_{t+1}$ and write $\mathfrak{G}' = \mathfrak{G}/\mathfrak{M}_{t+1}$. We then have

$$\begin{aligned} \mathfrak{G}' = \mathfrak{M}_1(\mathfrak{G}') = \mathfrak{K}_1(\mathfrak{G}') \supseteq \cdots \supseteq \mathfrak{M}_t(\mathfrak{G}') \\ = \mathfrak{K}_t(\mathfrak{G}') \supseteq \mathfrak{K}_{t+1}(\mathfrak{G}') \supseteq \mathfrak{M}_{t+1}(\mathfrak{G}') = \{1\}. \end{aligned} \tag{5.6'}$$

If we can prove $\mathfrak{K}_{t+1}(\mathfrak{G}') = \{1\}$, it will follow that $\mathfrak{K}_{t+1}(\mathfrak{G}) = \mathfrak{M}_{t+1}(\mathfrak{G})$, and this will finish our proof. If we replace $\mathfrak{G}'$ by $\mathfrak{G}$, we see that it is sufficient to treat the following case, namely, that in (5.6) $\mathfrak{M}_{t+1} = \{1\}$, in which we have to show that also $\mathfrak{K}_{t+1} = \{1\}$.

Let n_L be an element of $\mathfrak{N}^L$. As in Theorem 3.2, and because $\mathfrak{N}^{L+1} = 0$, n_L is a linear combination of products $\prod_i (F_{1,\rho_i} - 1)$, with L factors. As before, consider more generally all products

$$\pi = \prod (F_{\sigma_i,\tau_i} - 1) \tag{5.7}$$

with $\sum_i \sigma_i = L$, and $\sigma_i \leqq t$ (any order of factors admitted).

LEMMA 5.8. *Every product π of the type* (5.7) *may be expressed linearly by the products*

$$M_\lambda^{(L)} = \prod_{i,\nu} (F_{i,\nu} - 1)^{\beta_{i,\nu}}, \qquad \nu = 1, 2, \cdots, d_i;\ i = 1, 2, \cdots, t,$$

where $0 \leqq \beta_{i,\nu} < p$, and $\sum_{i,\nu} i\beta_{i,\nu} = L$, the factors being in the natural order as in (2.5).

To prove this lemma we use a method similar to that used in Theorem 3.2. A modification is necessary because we postulated only the property (5.1), (1) for the $\mathfrak{M}$-series, rather than the stronger $(\mathfrak{M}_i, \mathfrak{M}_j) \subseteq \mathfrak{M}_{i+j}$.

Suppose the lemma false and let π be the "highest" product which cannot be expressed linearly in terms of the $M_\lambda^{(L)}$. As before[12], we show that the same property is enjoyed by the product obtained by interchanging two consecutive factors $(A-1)$ and $(B-1)$ of π. Let $\pi = \pi_1(B-1)(A-1)\pi_2$ and suppose $A \in \mathfrak{K}_\rho$, $B \in \mathfrak{K}_\sigma$, $\rho, \sigma \leqq t$. Now $(A-1)$ may be replaced by an expression

$$\begin{aligned} (A-1) \equiv \sum c_{\lambda_1 \cdots \lambda_\rho} (F_{1,\lambda_1} - 1) \cdots (F_{1,\lambda_\rho} - 1) \text{ modulo } \mathfrak{N}^{\rho+1}, \\ c_{\lambda_1 \cdots \lambda_\rho} \in GF(p), \end{aligned} \tag{5.9}$$

and since $\mathfrak{N}^{L+1} = 0$, and $\pi \in \mathfrak{N}^L$, we may replace $(A-1)$ by this sum in the expression for π above, and obtain

[12] Compare the proof of Theorem 3.2.

$$\pi = \sum c_{\lambda_1 \cdots \lambda_\rho} \pi_1 (B-1)(F_{1,\lambda_1}-1) \cdots (F_{1,\lambda_\rho}-1)\pi_2.$$

As before, we use the identity (3.5) to interchange successively $(B-1)$ and $(F_{1,\lambda_1}-1), \cdots, (F_{1,\lambda_\rho}-1)$. When, in one of the terms of π, $(B-1)(F_{1,\lambda_i}-1)$ is replaced by $(F_{1,\lambda_i}-1)(B-1)$, we get, in the expression for π, two additional terms T_1 and T_2. In the first, the two interchanged factors $(B-1)(F_{1,\lambda_i}-1)$ are replaced by $(F_{1,\lambda_i}B-1)((B, F_{1,\lambda_i})-1)$ and in the second by $((B, F_{1,\lambda_i})-1)$. The first term T_1 vanishes since it is in $\mathfrak{N}^{L+1}=0$. The other term T_2 is transformed as follows: (B, F_{1,λ_i}) lies in $(\mathfrak{K}_\sigma, \mathfrak{G}) = (\mathfrak{M}_\sigma, \mathfrak{G}) \subseteq \mathfrak{M}_{\sigma+1}$. If $\sigma = t$, then $((B, F_{1,\lambda_i})-1)=0$, since $\mathfrak{M}_{t+1}=1$; if $\sigma<t$, we have $\mathfrak{K}_{\sigma+1}=\mathfrak{M}_{\sigma+1}$. We replace, using (2.7), $((B, F_{1,\lambda_i})-1)$ by a linear combination, modulo $\mathfrak{N}^{\sigma+2}$ of terms $(F_{\sigma+1,\nu}-1)$. Hence this term T_2 becomes a sum of terms "higher" than π and of a term in $\mathfrak{N}^{L+1}$. The latter vanishes, the first terms can be expressed by the $M_\lambda^{(L)}$. This shows that T_2 can also be disregarded. Finally, $\pi_1(B-1)(A-1)\pi_2$ will be replaced by

$$\pi_1\Big(\sum c_{\lambda_1 \cdots \lambda_\rho}(F_{1,\lambda_1}-1) \cdots (F_{1,\lambda_\rho}-1)(B-1)\Big)\pi_2 = \pi_1(A-1)(B-1)\pi_2.$$

Since π could not be expressed linearly by the M_λ^L, this new product $\pi_1(A-1)(B-1)\pi_2$ cannot be expressed by them either.

We may therefore pick π in the form

$$\pi = \prod (F_{i,\nu}-1)^{\beta_{i,\nu}}, \qquad \sum_{i,\nu} i\beta_{i,\nu} = L.$$

If all $\beta_{i,\nu}<p$, then π is itself an $M_\lambda^{(L)}$, which is a contradiction. Suppose $\beta_{i,\nu}\geqq p$. Then we write $(F_{i,\nu}-1)^p=(F_{i,\nu}^p-1)$: $F_{i,\nu}\in\mathfrak{K}_i=\mathfrak{M}_i$, and hence $F_{i,\nu}^p\in\mathfrak{M}_{ip}$. If $ip>t$, $\mathfrak{M}_{ip}=1$, and $F_{i,\nu}^p=1$, which would lead to $\pi=0$. If $ip\leqq t$, then $\mathfrak{M}_{ip}=\mathfrak{K}_{ip}$, and we replace $(F_{i,\nu}-1)^p$ by a combination of the $(F_{ip,\mu}-1)$, which gives rise to terms all "higher" than π. This again is a contradiction, and the lemma is proven.

The proof of Theorem 5.5 now follows at once. There is an $\mathfrak{M}_\lambda^L\neq 0$, since $\mathfrak{N}^L\neq 0$, and hence $L=\sum i\beta_{i,\nu}\leqq\sum i(p-1)d_i$, where $\nu=1, 2, \cdots, d_i$; $i=1, 2, \cdots, t$. However, $L=\sum j(p-1)d_j$, where $j=1, 2, \cdots, e$ if $\mathfrak{K}_e\neq 1$, $\mathfrak{K}_{e+1}=1$. Comparing we see $t\geqq e$, and hence $\mathfrak{K}_{t+1}=\mathfrak{K}_{e+1}=1$, which proves $\mathfrak{M}_{t+1}=\mathfrak{K}_{t+1}$ as required.

COROLLARY 5.10. $(\mathfrak{M}_i, \mathfrak{M}_j)\subseteq\mathfrak{M}_{i+j}$.

6. We conclude with a discussion of the $\mathfrak{K}$-series of two special types of p-groups, namely, groups all of whose elements except the identity are of order p, and abelian groups. Lombardo-Radici([13]) has investigated the structure of the radical of the group ring of an abelian group by elementary methods, and we shall show that the application of the more powerful ideas of the present paper leads to identical results.

([13]) L. Lombardo-Radici, Rendiconti del Seminario Matematico della Università di Roma, (4), vol. 2 (1938), p. 312.

Consider first a group $\mathfrak{G}$ which contains no element of order greater than p. Clearly conditions (2.4), (2) and (5.1), (2), become trivially satisfied, and the $\mathfrak{R}$-series of $\mathfrak{G}$ is defined by the relation (5.2), (1), which becomes

$$\mathfrak{R}_1 = \mathfrak{G}, \qquad \mathfrak{R}_i = (\mathfrak{R}_{i-1}, \mathfrak{G}). \tag{6.1}$$

These relations, however, imply that the $\mathfrak{R}$-series is the "lower central series" of $\mathfrak{G}$[14]. That is, $\mathfrak{R}_\lambda = \mathfrak{M}_\lambda = \mathfrak{H}_\lambda$, where $\mathfrak{G} = \mathfrak{H}_1 \supset \mathfrak{H}_2 \supset \cdots \supset \mathfrak{H}_c \supset 1$ is the lower central series of $\mathfrak{G}$.

THEOREM 6.2. *The $\mathfrak{R}$-series of a group which contains no elements whose order is greater than p is identical with the lower central series of the group. The "length" of the $\mathfrak{R}$-series of such a group is equal to the class of the group.*

Now let $\mathfrak{A}$ be an abelian group of type $(p^{\mu_1}, p^{\mu_2}, \cdots, p^{\mu_d})$, where $\mu_1 \geqq \mu_2 \geqq \cdots \geqq \mu_d$. In this case conditions (2.4), (1) and (5.1), (1), become trivially satisfied, and the $\mathfrak{R}$-series of $\mathfrak{A}$ is defined by the relation (5.2), (2), which becomes

$$\mathfrak{R}_1 = \mathfrak{A}, \qquad \mathfrak{R}_i = \{\mathfrak{R}^p_{(i/p)}\}. \tag{6.3}$$

Let $\mathfrak{A}^{(\lambda)}$ be the subgroup of the p^λth powers of elements of $\mathfrak{A}$. It is readily verified that

$$\mathfrak{R}_{p^\lambda} = \mathfrak{A}^{(\lambda)} \subset \mathfrak{R}_{p^\lambda+1} = \cdots = \mathfrak{R}_{p^{\lambda+1}} = \mathfrak{A}^{(\lambda+1)}, \qquad \lambda = 0, 1, 2, \cdots, \mu_1. \tag{6.4}$$

In particular, since $\mathfrak{A}^{(\mu_1-1)} \neq 1$, $\mathfrak{A}^{(\mu_1)} = 1$, we have

THEOREM 6.5. *The $\mathfrak{R}$-series of an abelian group of type $(p^{\mu_1}, p^{\mu_2}, \cdots, p^{\mu_d})$, $\mu_1 \geqq \cdots \geqq \mu_d$, has length p^{μ_1-1}.*

From Theorem 3.7, we deduce that for the group ring of an abelian group the rank of $\mathfrak{N}^w/\mathfrak{N}^{w+1}$ is equal to the coefficient of x^w in the expansion of

$$(1 + x + \cdots + x^{(p-1)})^{\delta_0}(1 + x^p + \cdots + x^{p(p-1)})^{\delta_1} \cdots (1 + x^{p^\lambda} + \cdots + x^{p^\lambda(p-1)})^{\delta_\lambda} \cdots,$$

where p^{δ_λ} is the order of $\mathfrak{A}^{(\lambda)}/\mathfrak{A}^{(\lambda+1)}$. By remarking that δ_λ is equal to the number of the integers μ_ρ which exceed λ, it is readily verified that the above product is equal to

$$(1 + x + \cdots + x^{p^{\mu_1}-1})(1 + x + \cdots + x^{p^{\mu_2}-1}) \cdots (1 + x + \cdots + x^{p^{\mu_d}-1}),$$

which is the form in which Lombardo-Radici obtained his result.

UNIVERSITY OF TORONTO,
TORONTO, ONTARIO, CANADA,
YALE UNIVERSITY,
NEW HAVEN, CONN.

[14] Cf. Hall, loc. cit., §2.