Math. Proc. Camb. Phil. Soc. (1977), **82**, 215
Printed in Great Britain

A dual approach to Černikov modules

By B. HARTLEY
University of Warwick

(*Received* 4 *February* 1977)

1. *Introduction.* Let G be a group and A a right G-module. If the additive group A^+ of A is a Černikov group, that is, a direct sum of finitely many cyclic and quasi-cyclic groups, we shall call A a Černikov module over G or over the integral group ring $\mathbb{Z}G$. Suppose that A^+ is, furthermore, a divisible p-group, where p is a prime. Since the endomorphism ring $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_{p^\infty}, \mathbb{Z}_{p^\infty})$ of a quasi-cyclic p-group is isomorphic to the ring $\mathbb{Z}_p$ of p-adic integers, we find that $A^* = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Z}_{p^\infty})$ is a free $\mathbb{Z}_p$-module of finite rank. We can make A^* into a right $\mathbb{Z}_p G$-module in the usual way, and since A^* is actually just the Pontrjagin dual of A, Pontrjagin duality shows that $A \to A^*$ gives rise to a contravariant equivalence between the categories of divisible Černikov p-torsion modules over $\mathbb{Z}G$ and $\mathbb{Z}_p G$-modules which are $\mathbb{Z}_p$-free of finite rank. Since the latter category is to some extent familiar, at least when G is finite – for its objects determine representations of G over the field $\mathbb{Q}_p$ of p-adic numbers, a field of characteristic zero – we may hope to exploit this correspondence systematically to study divisible Černikov p-modules. This is our main theme.

Actually, we may as well proceed in somewhat greater generality, following a paper of Kaplansky (11). We make the convention here and now that all rings considered in this paper have multiplicative identity elements, and all modules are right and unital. Throughout, R denotes a commutative complete discrete valuation ring with field of fractions K, maximal ideal $P = \pi R$, and residue field $\bar{R} = R/\pi R$ of characteristic $p \geqslant 0$. The R-submodules of K are precisely 0, K and the $\pi^i R$ ($i \in \mathbb{Z}$), and these are all distinct. Furthermore, R and K are complete in their topologies which have the $\pi^i R$ ($i \geqslant 0$) as a basis of neighbourhoods of 0. Let R_0 be the R-module K/R, which is isomorphic to $K/\pi^i R$ for any $i \in \mathbb{Z}$.

Let S be any integral domain. We say that an S-module A has *finite rank*, if there exists an integer $n \geqslant 0$ such that every finitely generated submodule of A can be generated by n elements or fewer. The least such n is called the *rank* of A. When $S = R$, it is not hard to see that the rank is additive on direct sums, and it follows from (12), p. 53, that, in this case, A has rank n if and only if A is a direct sum of n submodules, each isomorphic to one of K, R, R_0 or $R/\pi^m R$ for some $m > 0$. Let Mod_S denote the category of all S-modules of finite rank and S-homomorphisms, and Divmod_S denote the full subcategory of divisible S-modules of finite rank. If $\sigma \in S$, write σ-Mod_S, σ-Divmod_S for the full subcategories of Mod_S and Divmod_S respectively whose objects are all σ-torsion modules, that is, modules in which every element is annihilated by a suitable power of σ, from the appropriate category.

We now consider Mod_R in particular, and for $A \in \mathrm{Mod}_R$, let A^* denote the dual of A,

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

that is, the R-module $\mathrm{Hom}_R(A, R_0)$, which derives its (right) R-structure from the right R-structure of R_0. Then A and A^* are dually paired in the sense of (11) (see (11), lemma 4); this essentially follows from the well-known fact that R_0 is R-injective. Further, if $A = R$, R_0, K or $R/\pi^m R$, then A^* is isomorphic to R_0, R, K or $R/\pi^m R$ respectively, from which it follows that $A^* \in \mathrm{Mod}_R$ if $A \in \mathrm{Mod}_R$. In fact, A and A^* have the same R-rank. For $a \in A$, $\phi \in A^*$, let (a, ϕ) denote the effect of ϕ on a, and let $a\chi$ denote the element of A^{**} given by

$$(\phi, a\chi) = (a, \phi) \quad (\phi \in A^*).$$

The $\chi = \chi_A$ is an R-embedding of A in A^{**}, and lemma 2 of (11) asserts that it is actually an isomorphism.

For $A, B \in \mathrm{Mod}_R$, $\alpha \in \mathrm{Hom}_R(A, B)$, we can define $\alpha^* = \mathrm{Hom}_R(B^*, A^*)$ by

$$(a, \phi\alpha^*) = (a\alpha, \phi) \quad (\phi \in B^*).$$

Thus, defining $F(A) = A^*$, $F(\phi) = \phi^*$, with A, B, ϕ as above, we obtain a contravariant functor F from Mod_R into itself.

It is easy to see that F is exact, that is, it is additive and preserves arbitrary exact sequences, and also that χ is a natural isomorphism from the identity functor to F^2.

LEMMA 1·1.

(i) *F is exact.*

(ii) *F is a contravariant equivalence from Mod_R into itself.*

This, like most of our preliminary results, is quite straightforward and will not be proved. We point out, however, that (ii) implies that F preserves exact sequences. The fact that annihilation determines an order inverting bijection between the submodules of A and those of A^* follows (see (11) for more details), and a consideration of the homological definitions shows that F interchanges projectives and injectives in Mod_R. This is actually obvious because of the known structure of projectives and injectives, but the homological point of view comes into its own later.

Now let G be a group and Mod_{RG} denote the subcategory of all RG-modules in Mod_R and RG-homomorphisms. We shall use Divmod_{RG}, σ-Divmod_{RG}, and so on, with the obvious meanings. If $A \in \mathrm{Mod}_{RG}$, then the definition

$$(a, \phi g) = (ag^{-1}, \phi) \quad (a \in A, g \in G, \phi \in A^*)$$

makes A^* into an RG-module, and we find, if Lat_{RG} denotes the category of all *RG-lattices*, that is, RG-modules which are R-free of finite rank,

LEMMA 1·2. *F determines a contravariant equivalence of Mod_{RG} with itself, interchanging the full subcategories π-Divmod_{RG} and Lat_{RG}.*

The last assertion follows because a module in π-Divmod_{RG} is, as R-module, just a direct sum of copies of R_0, and R and R_0 are mutually dual.

Now suppose that we have a subring S of R, containing 1, and that P is a prime ideal of S containing π and satisfying

$$S + \pi^m R = R, \quad S \cap \pi^m R = P^m \tag{1}$$

for all $m \geqslant 1$. Then $S/P \cong \bar{R}$. We obtain (1), for example, if we start with a Dedekind

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

domain S and complete it in the topology, having the powers of a given maximal ideal P as a basis of neighbourhoods of 0. The case of particular interest is $S = \mathbb{Z}$. Let $P\text{-Mod}_S$ denote the category of P-torsion modules over S, that is, modules in which every element is annihilated by a power of P, and $P\text{-Divmod}_S$, $P\text{-Mod}_{SG}$, and so on, have the obvious meanings. Let A be a module in $\pi\text{-Mod}_R$. If X is any finite set of elements of A, there exists $m \geqslant 1$ such that $X\pi^m = 0$. Then $\pi^m R$ annihilates X. It follows from (1) that $XR = XS$, and that any set of R-module generators for XR is also a set of S-module generators. Therefore A has finite rank as an S-module, and we have a 'forgetful functor' from $\pi\text{-Mod}_R$ to $P\text{-Mod}_S$.

Conversely, let $B \in P\text{-Mod}_S$, and let $b \in B$, $r \in R$. We have $bP^m = 0$ for some $m \geqslant 1$. Using (1), write $r = \pi^m u + v$ with $u \in R$, $v \in S$, and define br to be bv. Then this is well defined. For if also $r = \pi^{m'}u' + v'$, where $m' \geqslant m$, $u' \in R$, $v' \in S$, then $\pi^m(\pi^{m'-m}u' - u) = v - v' \in \pi^m R \cap S = P^m$ by (1), whence $bv = bv'$. It is now trivial to verify that we obtain an R-module structure on B which restricts to the S-module structure with which we began. We call this the extension of B to R. If B is S-divisible then its extension will be R-divisible, since $\pi \in S$ and every non-zero element of R is the product of a power of π and a unit. Clearly, if B, B' are modules in $P\text{-Mod}_S$, then S-homomorphisms from B to B' are the same things as R-homomorphisms between their extensions to R, and so we have a functor $P\text{-Mod}_S \to \pi\text{-Mod}_R$ inverting the forgetful functor. Thus $P\text{-Mod}_S$ and $\pi\text{-Mod}_R$ are isomorphic categories; so are $P\text{-Mod}_{SG}$ and $\pi\text{-Mod}_{RG}$, and so on.

From Lemma 1·2 we obtain

LEMMA 1·3. *If* (1) *holds, then the categories* $P\text{-Divmod}_{SG}$ *and* Lat_{RG} *are contravariantly equivalent.*

The rest of the paper will be concerned with exploiting the connexions set up above to obtain information about Mod_{SG} and its subcategories, particularly when G is a finite group. The notation will be as above. Our investigations follow several different paths, united mainly by the point of view explained above, and we shall not attempt to summarize our results here.

2. *Divisibly irreducible and rationally irreducible modules.* Let A be a P-torsion SG-module. We say that A is *divisibly irreducible*, if $A \in P\text{-Divmod}_{SG}$ and the only SG-submodules of A in that category are 0 and A. We may make the analogous definition for π-torsion RG-modules. As we saw in the Introduction, a module in either of these categories may be viewed as a module in the other, and obviously the two concepts of divisible irreducibility so obtained are equivalent. Now, starting with $A \in P\text{-Divmod}_{SG}$ and viewing it as an RG-module, we find that A is a direct sum of finitely many copies of R_0 and so satisfies the minimal condition on R-submodules.

Hence, if B is any SG-submodule of A, then, as B is also an RG-submodule, the chain $B \geqslant B\pi \geqslant B\pi^2 \geqslant \ldots$ terminates after finitely many steps in a submodule which is R-divisible and *a fortiori* S-divisible. Therefore $A \in P\text{-Divmod}_{SG}$ is divisibly irreducible if and only if every proper submodule of A is annihilated by a power of π.

For $B \in \text{Lat}_{RG}$, we say that B is *rationally irreducible*, if $B^K = B \otimes_R K$ is an irreducible KG-module. This amounts to saying that if C is any non-zero submodule of B, then B/C is annihilated by a power of π. From the Introduction, we obtain

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

LEMMA 2·1. *Let $A \in P\text{-Divmod}_{SG}$. Then A is divisibly irreducible if and only if A^* is rationally irreducible.*

Suppose now for a moment that G is finite and $|G| \neq 0$ in S. Let $A \in P\text{-Divmod}_{SG}$, $B = A^*$, $V = B^K$. Then V is a KG-module of finite K-dimension, and by Maschke's Theorem, $V = V_1 \oplus \ldots \oplus V_t$, where the V_i are irreducible KG-modules. Let $U_i = B \cap V_i$. Now if $v \in V$, then there exists $n \geqslant 0$ such that $v\pi^n \in B$. Therefore U_i contains a K-basis of V_i, and $U = U_1 \oplus \ldots \oplus U_t$ contains a K-basis of V. Hence $B\pi^m \leqslant U$ for some $m \geqslant 0$. Clearly $U_i^K \cong V_i$, so U_i is rationally irreducible. Dualizing by means of Lemma 1·2, we obtain the first part of

LEMMA 2·2. *Let G be a finite group such that $|G| \neq 0$ in S, and let $A \in P\text{-Divmod}_{SG}$.*

(i) *There exists a submodule M of A such that $M\pi^m = 0$ for some $m \geqslant 0$ and A/M is a direct sum of divisibly irreducible modules.*

(ii) *A is a sum of divisibly irreducible submodules.*

To prove (ii), write $A/M = \bigoplus_{i=1}^{t} B_i/M$, where each B_i is divisibly irreducible. The conclusion we want is equivalent to the same result for RG-modules, and it is more convenient to work over RG since R is a principal ideal domain. Each B_i is an RG-module; let C_i be its maximal R-divisible submodule. Then B_i/C_i is annihilated by a power of π and therefore so is $B_i/(C_i + M)$. Hence $B_i = C_i + M$ and, if $C = \sum_{i=1}^{t} C_i$, then $A = M + C$. Therefore A/C is annihilated by a power of π, and since $A = A\pi$, $A = C$. Finally, let D_i be any non-zero R-divisible RG-submodule of C_i. Then $D_i \nleqslant M$, so $D_i + M = B_i = C_i + M$. Multiplying by π^m, we obtain $D_i = D_i\pi^m = B_i\pi^m = C_i\pi^m = C_i$. It follows that C_i is divisibly irreducible.

This result has been obtained by Zaicev ((19), Lemma 4) in the case $S = \mathbb{Z}$ (which is, after all, the most important one) by more direct means, but it provides a convenient first illustration of our methods. Zaicev deduces Lemma 2·2 from the following interesting and useful result ((19), theorem 1), in which the divisible abelian group occurring is not assumed to have finite rank:

Let F be a finite group of automorphisms of a divisible abelian group C, and let A be a divisible F-admissible subgroup of C. Then there exists a divisible F-admissible subgroup B of C, such that $C = A + B$ and $(A \cap B)|F| = 0$.

The proof is a simple adaptation of the proof of Maschke's Theorem.

In the case when the characteristic p of $\bar{R} = R/\pi R$ does not divide $|G|$, we can, of course, do much better. For $X \in \mathrm{Lat}_{RG}$, let $\bar{X} = X/X\pi$. The following result of Thompson (17), which is a quite straightforward consequence of idempotent lifting, is a convenient starting point for our remarks.

LEMMA 2·3. (Thompson.) *Let $X \in \mathrm{Lat}_{RG}$. If $Q/X\pi$ is any $\bar{R}G$-projective submodule of $\bar{X}$, then there exists an RG-projective RG-direct summand Y of X such that $Y + X\pi = Q$. In particular, $\bar{Y} \cong Q/X\pi$.*

Now for $A \in P\text{-Mod}_{SG}$, we define

$$\Omega_1(A) = \{a \in A : a\pi = 0\} = \{a \in A : aP = 0\}.$$

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

The last equality follows by extending A to RG and noting $\pi \in P \leqslant \pi R$. The dual of $\Omega_1(A)$ is the largest factor module of A^* annihilated by π, and so the annihilator in A^* of $\Omega_1(A)$ is $A^*\pi$. If $p \nmid |G|$, then every $\bar{R}G$-module is projective, and the dual of 2·3, obtained by taking annihilators twice, tells us that if $A \in P\text{-Divmod}_{SG}$ and V is any SG-submodule of $\Omega_1(A)$, then there exists an RG-direct summand U of A such that $U \cap \Omega_1(A) = V$. We obtain immediately the first two parts of:

THEOREM 2·4. *Suppose that $p \nmid |G|$, and let $A \in P\text{-Divmod}_{SG}$. Then*

(i) *A is a direct sum of divisibly irreducible modules.*

(ii) *A is indecomposable $\Leftrightarrow$ A is divisibly irreducible $\Leftrightarrow$ $\Omega_1(A)$ is irreducible.*

(iii) *If $B \in P\text{-Divmod}_{SG}$, then $A \cong B \Leftrightarrow \Omega_1(A) \cong \Omega_1(B)$.*

(iv) *The summands in any two direct decompositions of A into divisibly irreducible submodules can be paired so that corresponding summands are isomorphic.*

(v) *If S is Dedekind, then A is injective in the categories of all RG-modules and all SG-modules.*

Proof (iii). We have $A^* \in \text{Lat}_{RG}$ and of course A^* is projective in Lat_{RG}, since $|G|$ is a unit in R. Hence A is injective in $P\text{-Divmod}_{SG}$ (Lemma 1·3) and so any isomorphism from $\Omega_1(A)$ to $\Omega_1(B)$ extends to a homomorphism $\phi: A \to B$. Consideration of the R-structure of A and B shows that ϕ must be an isomorphism.

(iv) This can be deduced from the Krull–Schmidt Theorem for RG-lattices ((6), Corollary 43·7), using Lemma 1·3, or from the Krull–Schmidt Theorem for $\bar{R}G$-modules, using (iii) above.

(v) We have seen that A is injective in $P\text{-Divmod}_{SG}$, and also in $\pi\text{-Divmod}_{RG}$, since these are essentially the same. Although A^* is projective in the category of *all* RG-modules, we cannot use this fact to get what we want, since our contravariant equivalence is only defined on a subcategory. But since S and R are Dedekind and A is divisible as S- or R-module, A is injective in either the category of all S-modules or of all R-modules ((16), theorem 3·20). Therefore, (v) follows by taking $\mathscr{C}$ to be $P\text{-Divmod}_{SG}$ or $\pi\text{-Divmod}_{RG}$ in the lemma below, which is no doubt well known.

LEMMA 2·5. *Let G be a finite group, T be a ring, and A a TG-module. Suppose that A is T-injective, and is also injective in a category $\mathscr{C}$ of TG-modules which contains every TG-module T-isomorphic to a direct sum of finitely many copies of A. Then A is TG-injective.*

The proof requires another lemma, many versions of which are in the literature.

LEMMA 2·6. *Let T be a ring with identity, U a subring of T containing the identity of T, and M an injective right U-module. Then $\text{Hom}_U(T_U, M)$ is an injective right T-module.*

The right T-structure on $\text{Hom}_U(T_U, M)$ is given by

$$(\phi r)(t) = \phi(rt) \quad (r, t \in T, \phi \in \text{Hom}_U(T_U, M)).$$

(We write maps on the left here in order to make the above structure more transparent.) More generally, the result remains true if we have a ring homomorphism of U into T, preserving the identities, *via* which the right U-module structure of T is determined.

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

Proof. Since the proof is just the same as a standard special case, we only sketch it (see (5), (57·7) for example). In the first place, the given operation makes $\mathrm{Hom}_U(T_U, M)$ into a right T-module. Let J be right ideal of T and ψ a T-homomorphism of J into $\mathrm{Hom}_U(T_U, M)$. If $j \in J$, then $\psi(j)(1) \in M$, and one checks that $j \to \psi(j)(1)$ is a U-homomorphism of J into M. Since M is U-injective, there exists a U-homomorphism $\chi: T \to M$ such that $\chi(j) = \psi(j)(1)\,(j \in J)$. Then one checks that

$$\psi(j) = \chi j \quad (\text{in } \mathrm{Hom}_U(T_U, M)),$$

for all $j \in J$. The claim then follows from Baer's criterion for injectivity ((5), Theorem 57·14).

Proof of Lemma 2·5. Since A is T-injective, Lemma 2·6 shows that $\mathrm{Hom}_T(TG, A)$ is TG-injective. Now $A \cong \mathrm{Hom}_{TG}(TG, A)$ (an element $a \in A$ corresponding to the homomorphism which sends 1 to a), and $\mathrm{Hom}_{TG}(TG, A) \leqslant \mathrm{Hom}_T(TG, A)$. Furthermore, as T-module, $\mathrm{Hom}_T(TG, A)$ is a direct sum of $|G|$ copies of A, so is an object in $\mathscr{C}$. Therefore A is (isomorphic to) a direct summand of an injective TG-module, and so is TG-injective.

One consequence of Theorem 2·4 is that, when $p \nmid |G|$, the isomorphism classes of divisibly irreducible modules in $P\text{-Divmod}_{SG}$ are in one-to-one correspondence with the isomorphism classes of irreducible $\bar{R}G$-modules.

Some of these results were treated in a different way in (7).

3. *Divisibly irreducible modules for abelian groups.* In this section, we consider modules over a finite abelian group G. We shall classify the divisibly irreducible modules in $p\text{-Divmod}_{ZG}$ and prove a result of Krull–Schmidt type for the decompositions of an arbitrary module in $p\text{-Divmod}_{ZG}$ as sums of divisibly irreducible submodules.

LEMMA 3·1. *Let G be a finite abelian group and A be a divisibly irreducible module in $P\text{-Divmod}_{SG}$. If A is faithful for G, then G is cyclic.*

Proof. This is because A^{*K} is an irreducible KG-module faithful for G, and finite abelian irreducible linear groups are cyclic.

This result, like some others in this section, was obtained by Zaicev ((19), section 3) for the case when G is an abelian p-group. Because of it, we now restrict attention to cyclic groups G.

CONVENTION. *Throughout the rest of this section, R will denote the ring of p-adic integers and K its field of fractions.*

We shall also take $S = \mathbb{Z}$ and π to be a prime p, but indicate to what extent our results are true more generally.

We have seen that studying divisibly irreducible modules in $p\text{-Divmod}_{ZG}$ is equivalent to studying rationally irreducible RG-modules. These have been completely classified by Berman (3) in the case when G has a cyclic normal Sylow p-subgroup, and some of the results in this section can be deduced from his. However, the case when G itself is cyclic is particularly transparent, requiring only some elementary facts about finite extensions of the p-adic field, and so we shall treat it directly here.

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

Let G now denote a finite cyclic group of order n and let $K_1 = K(\zeta)$, where ζ is a primitive nth root of 1. Then any irreducible KG-module, faithful for G, is isomorphic to a module (K_1, θ) determined by an isomorphism $\theta: G \to \langle\zeta\rangle$; the underlying K-space of the module is K_1, and the action of G is defined by

$$(v, g) \to v \,.\, g\theta \quad (v \in K_1, g \in G).$$

Two such KG-modules, corresponding to isomorphisms θ, θ', are isomorphic if and only if $\theta' = \theta\mu$ for some element μ in the Galois group $\mathrm{Gal}\,(K_1/K)$ of K_1 over K. These well-known facts are proved for instance in (7).

Let ν be the exponential valuation of K such that $\nu(p) = 1$. Then ν can be uniquely extended to an exponential valuation of K_1, also denoted by ν. The valuation ν of K_1 is discrete, and so the ring of integers R_1 of K_1 is a discrete valuation ring (see (18), theorem 2-2-10). Let P_1 be the maximal ideal of R_1. Then $P_1 \cap R = P$. For our purposes, the following observation is crucial:

LEMMA 3·2. $R_1 = R[\zeta]$.

Proof. Write $n = p^d l$, where $(p, l) = 1$, and $\zeta = \alpha\beta$, where α is a primitive p^dth root of 1 and β a primitive lth root of 1. Suppose, first, $d \geqslant 1$. Then

$$1 + (X+1)^{p^{d-1}} + (X+1)^{2p^{d-1}} + \ldots + (X+1)^{(p-1)p^{d-1}} \tag{1}$$

is an Eisenstein polynomial over R, having $\alpha - 1$ as a root (see Weiss (18), pp. 80–88 for the facts and terminology relating to this argument), and so $\alpha - 1$ is a prime element in R_2, the ring of integers of $K_2 = K(\alpha)$, and $1, (\alpha-1), \ldots, (\alpha-1)^{m-1}$ is an integral basis of K_2, where $m = p^{d-1}(p-1)$ ((18), theorem 3-3-1, corollary 3-3-2). In particular, $R_2 = R[\alpha]$. If $d = 0$, this is obviously still true.

Since the polynomial $X^l - 1$ has no repeated roots in a field of characteristic p, (18), theorem 3-2-6, shows that $K_1 = K_2(\beta)$ is an unramified extension of K_2, and certain powers of β form an integral basis of K_1 over K_2. Hence $R_1 = R_2[\beta] = R[\alpha, \beta] = R[\zeta]$, as claimed.

We also have

LEMMA 3·3. $(K_1 : K) = \phi(p^d)\, o(p, l)$, *where* ϕ *is the Euler* ϕ*-function, so that* $\phi(p^d) = p^{d-1}(p-1)$ *if* $d \geqslant 1$ *and* $\phi(1) = 1$, *and* $o(p, l)$ *is the order of* $p \bmod l$.

Proof. Retaining the notation of the proof of Lemma 3·2, we have that (1) is irreducible, and so $(K_2 : K) = \phi(p^d)$; also the residue field of R_2 is the field $\mathbb{F}_p$ of p elements ((18), theorem 3-3-1). Since K_1/K_2 is unramified, $(K_1 : K_2)$ is the same as the degree of the residue field $\bar{R}_1$ of K_1 over the residue field $\bar{R}_2 = \mathbb{F}_p$ of K_2. Since $X^l - 1$ factorizes completely in R_1, it also does so in $\bar{R}_1$, and also its roots generate $\bar{R}_1$ over $\mathbb{F}_p$. Hence $(K_1 : K_2) = (\bar{R}_1 : \mathbb{F}_p) = o(p, l)$.

THEOREM 3·4. *Let* G *be a cyclic group of order* $n = p^d l$, $(p, l) = 1$. *Then*

(i) *The number of isomorphism classes of divisibly irreducible modules, faithful for* G, *in* p-$\mathrm{Divmod}_{\mathbb{Z}G}$, *is* $\phi(l)/o(p, l)$.

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

(ii) *Each such module has rank* $\phi(p^d)\,o(p,l) = \psi_p(n)$.

(iii) *If* A *is a divisibly irreducible module in* p-Divmod_{ZG}, *then* A *is uniserial, and every non-zero quotient module of* A *is isomorphic to* A.

A module is *uniserial* if its lattice of submodules is totally ordered.

Proof. (i) Let A be any divisibly irreducible module in p-Divmod_{ZG}. By 2·1, A^* is a rationally irreducible RG-lattice, and so A^{*K} is an irreducible KG-module. By the remarks following the proof of Lemma 3·1, A^{*K} is isomorphic to a module of the form (K_1, θ), where θ is some isomorphism of G onto $\langle\zeta\rangle$, and the number of isomorphism types of such modules is

$$|\mathrm{Aut}\, G|/|\mathrm{Gal}\,(K_1/K)| = \phi(n)/(K_1:K) = \phi(p^d)\,\phi(l)/\phi(p^d)\,o(p,l)$$

(using 3·3) $= \phi(l)/o(p,l) = t$, say. Let $(K_1, \theta_1), \ldots, (K_1, \theta_t)$ represent these isomorphism types. Then there is a unique i, $1 \leqslant i \leqslant t$, such that A^* is isomorphic to an RG-submodule of (K_1, θ_i). Now θ_i determines a homomorphism of RG onto $R[\zeta]$ and we denote this homomorphism also by θ_i. By 3·2, $R[\zeta] = R_1$, and so RG-submodules of (K_1, θ_i) are precisely the same as R_1-submodules. But the non-zero finitely generated R_1-submodules of K_1 all have the form $\omega^j R_1$ ($j = 0, \pm 1, \pm 2, \ldots$), where ω is a prime element of R_1, and hence are all isomorphic under multiplication by a suitable power of ω. Therefore A^* determines, and is determined by, a unique integer i with $1 \leqslant i \leqslant t$, and (i) is established, in virtue of the duality given by 1·3.

(ii) This is immediate from the foregoing discussion and 3·3, since A, A^* and K_1 all have the same rank.

(iii) Continuing with the same notation, we may identify A^* with R_1, viewed as an RG-module using the homomorphism $\theta: RG \to R_1$. The R_1-submodules of R_1 are $\omega^j R_1$ ($j = 0, 1, \ldots$) and 0, and these are totally ordered by inclusion; also each $\omega^j R_1$ is isomorphic to R_1 itself. The claim now follows by Lemma 1·3.

The crucial ingredient in the proof of Theorem 3·4 is Lemma 3·2, which will, of course, remain true if we take K to be a finite cyclotomic extension of $\mathbb{Q}_p$ and R to be the ring of integers in K. Thus Theorem 3·4 can be extended in an obvious way to this situation, although not with the same numerical values.

COROLLARY 3·5 (Zaicev (19)). *Let* G *be cyclic of order* p^d. *Then, up to isomorphism, there exists a unique divisibly irreducible module, faithful for* G, *in* p-Divmod_{ZG}.

COROLLARY 3·6. *Let* A *be a divisible abelian Černikov* p*-group. Then* A *admits an automorphism of order* p^d ($d \geqslant 1$) *if and only if the rank of* A *is at least* $p^{d-1}(p-1)$.

Proof. By Lemma 2·2, if A admits such an automorphism α, then it contains a divisibly irreducible $\langle\alpha\rangle$-submodule B faithfully transformed by $\langle\alpha\rangle$. By Theorem 3·4 (ii), the rank of B is $p^{d-1}(p-1)$. The converse is an immediate application of Theorem 3·4.

The following is a useful criterion for deciding whether a given module in p-Divmod_{ZG} (where G is cyclic) is divisibly irreducible.

LEMMA 3·6. *Let* G *be a cyclic group of order* n *and* A *be a module, faithful for* G, *in* p-Divmod_{ZG}. *Then* A *is divisibly irreducible if and only if the following conditions hold*:

(i) A *has rank* $\psi_p(n)$,

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

(ii) *Every element of prime order different from p in G operates fixed point freely on $\Omega_1(A)$.*

Proof. First suppose that A is divisibly irreducible, and let x be an element of prime order $q \neq p$ in G. Applying Fitting's Lemma to the finite $\langle x \rangle$-invariant subgroups of A, we obtain $A = C_A(x) \oplus A(x-1)$, where $C_A(x) = \{a \in A : ax = a\}$. Both summands are divisible G-submodules, and $A(x-1) \neq 0$ since A is faithful. Hence $C_A(x) = 0$ and so x operates fixed point freely on A itself. By Theorem 3·4 (ii), A has rank $\psi_p(n)$.

Now suppose that (i) and (ii) hold. By Lemma 2·2, A is a sum of divisibly irreducible submodules, and since A is faithful for G, we can choose one of these submodules, say B, on which the subgroup of order p of G operates non-trivially, in case such a subgroup exists. Otherwise, let B be any of the divisibly irreducible submodules. Then (ii) guarantees that B is faithful for G. Hence, by Lemma 3·4, B has rank $\psi_p(n)$, and since B is additively a direct summand of A, it follows that $B = A$.

Having considered divisibly irreducible modules, we now prove a 'Krull–Schmidt Theorem' for decompositions of an arbitrary module in p-Divmod$_{\mathbb{Z}G}$ (where G is now finite abelian) into divisibly irreducible submodules.

THEOREM 3·7. *Let G be a finite abelian group, $A \in p$-Divmod$_{\mathbb{Z}G}$, and let*

$$A = A_1 + \ldots + A_m = B_1 + \ldots + B_n$$

be two irredundant expressions of A as sums of divisibly irreducible submodules. Then $m = n$ and the summands in the two sums can be paired so that corresponding summands are isomorphic.

Note that the above sums are not assumed direct.

Proof. The hypothesis amounts to saying that there is an exact sequence of $\mathbb{Z}G$-modules

$$A_1 \oplus \ldots \oplus A_m \xrightarrow{\phi} A \to 0$$

such that ϕ ceases to be surjective when restricted to the sum of any proper subset of the A_i, and also that a similar situation prevails for $B_1 \oplus \ldots \oplus B_n$. By Lemma 1·3, there is an exact sequence

$$0 \to A^* \xrightarrow[\phi^*]{} A_1^* \oplus \ldots \oplus A^m$$

such that ϕ^* ceases to be injective when followed by the projection onto the sum of any proper subset of the A_i^*. Identifying A^* with its image in $A_1^* \oplus \ldots \oplus A_m^*$, we find that $A^* \cap A_i^* \neq 0$ for all $1 \leqslant i \leqslant m$. Since A_i^* is rationally irreducible, it follows that $|A_i^* : A^* \cap A_i^*| < \infty$ for each i, and so $\left| \bigoplus_{i=1}^{m} A_i^* : A^* \right| < \infty$. Hence

$$\bigoplus_{i=1}^{m} A_i^{*K} \cong A^{*K}.$$

Since the same argument applies to the sum of the B_i, we conclude that

$$\bigoplus_{i=1}^{m} A_i^{*K} \cong \bigoplus_{i=1}^{n} B_i^{*K};$$

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

here the summands are KG-irreducible. Hence $m = n$ and the summands can be renumbered so that $A_i^{*K} \cong B_i^{*K}$ $(1 \leqslant i \leqslant n)$. Let

$$C_i = C_G(A_i) = C_G(A_i^*) = C_G(A_i^{*K}) = C_G(B_i^{*K}) = C_G(B_i^*) = C_G(B_i).$$

Then G/C_i is cyclic, as it is a finite irreducible abelian linear group. By the proof of Theorem 3·4, since A_i^* and B_i^* are $R[G/C_i]$-modules which become isomorphic over K, $A_i^* \cong B_i^*$. Hence $A_i \cong B_i$, as claimed.

Lemma 3·1 and Theorem 3·4 show that if G is a finite abelian group, then every divisibly irreducible $\mathbb{Z}G$-module is uniserial. We conclude this section with an example to show that (not very surprisingly) this breaks down quite quickly when non-abelian groups are considered.

PROPOSITION 3·8. *Let G be a non-abelian group of order 27 and exponent 3. Then there exists a divisibly irreducible module in* 3-$\mathrm{Divmod}_{\mathbb{Z}G}$ *having more than one minimal submodule.*

Proof. Let $G = \langle x, y\rangle$ and let $z = [x, y]$, which generates the centre of G. Let $H = \langle x, z\rangle$, which is elementary abelian of order 9 and normal in G. The matrix $\begin{pmatrix} 1 & 1 \\ -3 & -2 \end{pmatrix}$ over $\mathbb{Z}$ has multiplicative order 3, and so if R is the ring of 3-adic integers and K its field of fractions, there is an RH-lattice U with R-basis u_1, u_2 and H-action given by:

$$u_1 z = u_1 + u_2, \quad u_2 z = -3u_1 - 2u_2; \tag{2}$$

$$u_1 x = u_1, \qquad u_2 x = u_2. \tag{3}$$

By Lemma 3·3 and the remarks about irreducible modules for cyclic groups at the beginning of this section, every non-trivial irreducible $K\langle z\rangle$-module has dimension $\phi(3) = 2$, and so, by Maschke's Theorem, U^K is KH-irreducible. Let V be the induced module $U^G = U \otimes_{RH} RG$, and identify u_1 and u_2 with $u_1 \otimes 1$, $u_2 \otimes 1$ respectively. Then V has R-basis

$$u_1,\ u_1 y,\ u_1 y^2,\ u_2,\ u_2 y,\ u_2 y^2. \tag{4}$$

We claim that V^K is irreducible. For V^K is non-trivially transformed by $\langle z\rangle$, and so, by Maschke's Theorem, contains an irreducible KG-submodule W which is non-trivially transformed by z and so is faithful for G. Since H is non-cyclic, the restricted module W_H cannot be homogeneous. Hence Clifford's Theorem ((8) v. 17·3) shows that W is induced from some non-trivial irreducible KH-module W_1. The latter has dimension 2 as we have just seen. So $\dim_K W = 6$ and $W = V^K$, which is irreducible. This means that V is rationally irreducible.

Let $\overline{V} = V/3V$, and let $v \to \bar{v}$ denote the natural homomorphism of V onto $\overline{V}$. By (2), H fixes $\overline{u}_2$, and so $\overline{u}_2, \overline{u}_2 y, \overline{u}_2 y^2$ span a three-dimensional $\mathbb{F}_3 G$-submodule $\overline{T}$ of $\overline{V}$. Since G is a 3-group, $\overline{T} > [\overline{T}, G] = \langle t(g-1) : t \in \overline{T}, g \in G\rangle$. Let $s = \overline{u}_1 + \overline{u}_1 y + \overline{u}_1 y^2$, which is not in $\overline{T}$ since (4) is a basis of V. A straightforward calculation shows that $s(y-1) = 0$, $s(x-1) = \overline{u}_2 y(y-1) \in [\overline{T}, G]$. Hence $[\overline{T}, G]$, which is an $\mathbb{F}_3 G$-submodule of $\overline{V}$, contains $s(g-1)$ for all $g \in G$, and $\overline{T} \oplus \mathbb{F}_3 s$ is an $\mathbb{F}_3 G$-submodule of $\overline{V}$ having a G-trivial image of dimension 2 over $\mathbb{F}_3$. Let Y be the inverse image of $\overline{T} \oplus \mathbb{F}_3 s$ in V. Then Y has a G-trivial quotient module which is additively elementary abelian of order 9, and in particular

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

has more than one maximal submodule. Also Y is rationally irreducible; note that Y is an RG-lattice since R is a principal ideal domain. Then Y^* is clearly a divisibly irreducible $\mathbb{Z}G$-module with all the desired properties.

4. *Injective modules.* Now we return to the general notation of the Introduction. Let $U \in P\text{-Divmod}_{SG}$. The aim of the first few results in this section is to get information about the whole of U (for example, about direct summands of U) from a knowledge of

$$\Omega_1(U) = \{u \in U : uP = 0\}.$$

Most of this follows very quickly from the result of Thompson quoted as Lemma 2·3. We write $X \mid Y$ to denote that a module X is isomorphic to a direct summand of a module Y.

THEOREM 4·1. *Let G be a finite group and M be an injective $\bar{R}G$-module of finite $\bar{R}$-dimension. Then*

(i) *There exists a module $\hat{M} \in P\text{-Divmod}_{SG}$ such that $\Omega_1(\hat{M}) \cong M$.*

(ii) *$\hat{M}$ is injective in $P\text{-Divmod}_{SG}$, and is injective in the category of all SG-modules if S is Dedekind.*

(iii) *$\hat{M}$ is determined up to isomorphism by* (i).

(iv) *If $U \in P\text{-Divmod}_{SG}$, then $\hat{M} \mid U$ if and only if $M \mid \Omega_1(U)$.*

Proof. (i) Since M is injective, its dual M^* is $\bar{R}G$-projective. Writing M^* as an image of a free RG-module and using Lemma 2·3, we can find a projective RG-module X such that $X/X\pi \cong M^*$. Then X^* has the properties required of $\hat{M}$ in (i).

(ii) Since X is projective in Lat_{RG}, X^* is injective in $P\text{-Divmod}_{SG}$ (by Lemma 1·3). If S is Dedekind, then X^*, being S-divisible, is S-injective ((16), 54·19), and Lemma 2·5 shows that X^* is injective in the category of all SG-modules.

(iii) Let $\hat{M}$ denote X^*, identifying M with $\Omega_1(\hat{M})$, and let N be any module in $P\text{-Divmod}_{SG}$ with $\Omega_1(N) \cong M$. There is an isomorphism from $\Omega_1(N)$ to M, and as $\hat{M}$ is injective, this extends to a homomorphism $\psi : N \to \hat{M}$. Since $(\ker \psi) \cap \Omega_1(N) = 0$, ψ is monomorphic. Therefore the image of ψ is R-divisible and must be an R-direct summand of $\hat{M}$. But $\operatorname{im} \psi \geqslant \Omega_1(\hat{M})$, whence ψ is epimorphic. Therefore $N \cong \hat{M}$. Alternatively one can quote the dual fact.

(iv) Clearly, $\hat{M} \mid U$ implies $M = \Omega_1(\hat{M}) \mid \Omega_1(U)$. Conversely, if $M \mid \Omega_1(U)$, then M^* is a direct summand of $U^*/U^*\pi$. Since M is injective, M^* is projective, and Lemma 2·3 shows that there exists a projective RG-module Y such that $Y \mid U^*$ and $Y/Y\pi \cong M^*$. Then $Y^* \mid U$ and $\Omega_1(Y^*) \cong M$. By (iii), $Y^* \cong \hat{M}$, and so $\hat{M} \mid U$.

If we take M to be the group algebra $\bar{R}G$, which is of course $\bar{R}G$-injective, then it follows from (iii) that $\hat{M} \cong RG \otimes_R R_0$. Specializing to the case $S = \mathbb{Z}$, we obtain

COROLLARY 4·2. *Let $U \in p\text{-Divmod}_{\mathbb{Z}G}$, where G is a finite group. Then $(\mathbb{Z}G \otimes_{\mathbb{Z}} \mathbb{Z}_{p^\infty}) \mid U$ if and only if $\mathbb{F}_p G \mid \Omega_1(U)$.*

This extends a result of Zaicev ((19), p. 103), who considered the case when G is a finite abelian p-group.

Notice that $\mathbb{F}_p G$ can be identified with the base group of the wreath product $C_p \wr G$, where C_p is cyclic of order p and the action is by conjugation, and $\mathbb{Z}G \otimes_{\mathbb{Z}} \mathbb{Z}_{p^\infty}$ with the base group of $\mathbb{Z}_{p^\infty} \wr G$.

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

5. *Groups with cyclic upper central factors.* Let G be a hypercentral p-group with upper central series $1 = Z_0 \leqslant Z_1 \leqslant \ldots$, continued transfinitely if necessary. In (2), Baumslag and Blackburn considered such groups G in which Z_{m+1}/Z_m is a non-trivial cyclic group for all finite $m \geqslant 0$. It is not hard to see that these quotients then have decreasing orders (2), and hence their orders are eventually constant. For simplicity we shall consider only the case when Z_{m+1}/Z_m is of fixed order $p^n > 1$ for all $m = 0, 1, \ldots$. Let $Z_\omega = \bigcup Z_m$ over natural numbers m. We shall eventually classify the hypercentral p-groups G such that Z_{m+1}/Z_m is cyclic of order p^n for all $m = 0, 1, \ldots$ and G/Z_ω is abelian, thus extending the work of Baumslag and Blackburn, who dealt with the case $n = 1$. It will turn out that these groups are Černikov p-groups, that G/Z_ω is finite and cyclic, and that their isomorphism classes can be parametrized in a fairly simple way.

In the results leading up to Theorem 5·6, G will denote a hypercentral p-group such that Z_{m+1}/Z_m is cyclic of order $p^n > 1$ for all finite m.

LEMMA 5·1 (2).
(i) $[G, Z_{n+1}] = Z_n$ *if* n *is finite.*
(ii) $[G, Z_\omega] = Z_\omega$.
(iii) Z_ω *is abelian.*

LEMMA 5·2. *Let K be a normal subgroup of a group H with upper central series $1 = H_0 \leqslant H_1 \leqslant \ldots$, let $K_i = K \cap H_i$, and suppose that $\bigcup_{i=1}^{\infty} K_i = K$ and $|K_{i+1}/K_i|$ is a fixed prime q for all i. Then the only normal subgroups of H contained in K are the K_i and K itself.*

Proof. Let N be a normal subgroup of H properly contained in K, and let i be the largest integer such that $K_i \leqslant N$. Such an integer exists since $\bigcup_{i=1}^{\infty} K_i = H$. If $N > K_i$, then $N \cap K_j > K_i$ for some $j > i$, which we may choose minimal. Then

$$[H, N \cap K_j] \leqslant N \cap K_{j-1} = K_i \leqslant H_i,$$

whence $N \cap K_j \leqslant H_{i+1}$. Hence $K_i < N \cap K_j \leqslant K \cap H_{i+1} = K_{i+1}$, from which

$$K_{i+1} = N \cap K_j \quad \text{as} \quad |K_{i+1}:K_i|$$

is prime, and $K_{i+1} \leqslant N$. This contradiction to the choice of i shows that $N = K_i$, as required.

Let $A = Z_\omega$.

LEMMA 5·3. *A is Černikov.*

Proof. Let $A_1 = \Omega_1(A)$. If $A_1 \leqslant Z_n$ for some n, then A_1 is finite and so A is Černikov. Suppose then that $A_1 \not\leqslant Z_n$ for all n, and write $Y_i = A_1 \cap Z_i$ $(i = 0, 1, \ldots)$. For each i, $A_1 Z_i/Z_i$ is a non-trivial normal subgroup of the hypercentral group G/Z_i, and so $A_1 Z_i/Z_i \cap Z_{i+1}/Z_i \neq 1$. Hence $A_1 \cap Z_{i+1} > A_1 \cap Z_i$ and we have

$$1 = Y_0 < Y_1 < \ldots; \quad \bigcup_{i=1}^{\infty} Y_i = A_1. \tag{1}$$

Since Y_{i+1}/Y_i has exponent p and is isomorphic to a subgroup of Z_{i+1}/Z_i, $|Y_{i+1}/Y_i| = p$. By Lemma 5·2, the subgroups (1) are the only normal subgroups of G contained in A_1.

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

Let $C = C_G(A_1)$. Then $C < G$, otherwise $A_1 \leqslant Z_1$, contrary to our assumption. Since G is hypercentral, the centre of G/C contains a non-trivial element xC, of order p. Then $C_{A_1}(x) \lhd G$, and $C_{A_1}(x) < A_1$. Hence $C_{A_1}(x)$ is one of the Y_i, which is finite.

Let ξ be the endomorphism $a \to [a, x]$ of A_1. Then $\ker \xi$ is finite, and $\xi^p = 0$. A simple induction shows that $\ker \xi^i$ is finite for all i, whence $A_1 = \ker \xi^p$ is finite. This contradiction to (1) establishes the claim.

LEMMA 5·4. *A is divisible, $A = C_G(A)$, and $|G:A| < \infty$.*

Proof. Let B be the maximal divisible subgroup of A. Then $|A/B| < \infty$, and so, as G is hypercentral, $[A, G, \ldots, G] \leqslant B$ with a sufficiently large finite number of terms G. By Lemma 5·1 (ii), $A = B$. Now let $C = C_G(A)$. Suppose that $C > A$. Using the fact G is hypercentral, we can choose an element $1 \neq xA$ lying in C/A and the centre of G/A. Then $D = \langle A, x\rangle$ is a normal abelian Černikov subgroup of G. D is a union of finite normal subgroups of G, and each of these must lie in some Z_n. Hence $D \leqslant Z_\omega = A$, a contradiction. Therefore $A = C_G(A)$. The fact that $|G:A| < \infty$ now follows since a periodic group of automorphisms of an abelian Černikov group is finite ((13), theorem 1·F·3).

We now write A additively, and think of it as a $\mathbb{Z}G$-module, or a $\mathbb{Z}[G/A]$-module, by conjugation. Then $A \in p\text{-Divmod}_{\mathbb{Z}G}$ and the resources of the preceding parts of the paper are available to us.

LEMMA 5·5. *Let B be a divisible submodule of A of the form $B = B_1 + B_2$, where B_1 and B_2 are divisible and divisibly irreducible. Let $C_i = C_G(B_i)$. Then one of C_1 and C_2 contains the other, and if $C_1 = C_2$, then $B_1 = B_2$.*

Proof. First notice that $C_1, C_2 < G$, since Z_1 is finite. Let g be any element of G such that gC_2 is an element of order p in the centre of G/C_2. Such an element exists since G/C_2 is a finite p-group. Now $V = B_2^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a finite-dimensional irreducible $\mathbb{Q}_p[G/C_2]$-module, and by Clifford's Theorem, V is the direct sum of a number of isomorphic irreducible $\mathbb{Q}_p[\langle gC_2\rangle]$-modules, each faithful for $\langle gC_2\rangle$. If U is one of these submodules, the considerations at the beginning of section 3 show that we can identify U with $\mathbb{Q}_p(\zeta)$, where ζ is a primitive pth root of 1, with g acting as multiplication by ζ. The minimal polynomial of ζ is $1 + X + \ldots + X^{p-1}$, and so that of $\zeta - 1$ is

$$1 + (X+1) + \ldots + (X+1)^{p-1},$$

which has the form $p + Xh$ for some polynomial h. Hence $p + (g-1)h(g-1)$ annihilates B_2^*. If $b \in B_2$, then using the definition of the dual module, we have

$$(b(p + (g^{-1}-1)h(g^{-1}-1)), \phi) = (b, \phi(p + (g-1)h(g-1))) = 0$$

for all $\phi \in B_2^*$. Since B_2^* separates the points of B_2, we find that

$$b(p + (g^{-1}-1)h(g^{-1}-1)) = 0.$$

This holds for all $b \in B_2$. Evidently we may replace g by g^{-1}, and so we conclude:

There exists a polynomial $h(X) \in \mathbb{Z}[X]$ such that $p + (g-1)h(g-1)$ annihilates B_2. (*)

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

Now suppose that neither C_1 nor C_2 contains the other. Then C_1C_2/C_2 is a non-trivial normal subgroup of the finite p-group G/C_2, and hence we may choose $g \in C_1$ in the above. Let X/Y be any G-trivial factor of $B = B_1 + B_2$, and $b_1 + b_2 \in X$, with $b_i \in B_i$ $(i = 1, 2)$. Then Y contains $(b_1 + b_2)(g-1) = b_2(g-1)$, and so $b_2(g-1) \in Y \cap B_2$. Applying (*), we find that $b_2 p = -b_2(g-1)h(g-1) \in Y \cap B_2 \leqslant Y$. By symmetry, $b_1 p \in Y$ also, and so $(b_1 + b_2)p \in Y$. Therefore X/Y has exponent p.

Letting $K_i = B \cap Z_i$ $(i = 0, 1, \ldots)$, we find that each K_{i+1}/K_i is a cyclic G-trivial factor of B, and so each K_{i+1}/K_i has order p. By Lemma 5·2, the only submodules of B are the K_i and B itself. Hence $B_1 = B_2 = B$ and $C_1 = C_2$, a contradiction.

If $C_1 = C_2$ and g is chosen as at the beginning of the proof, (*) shows that

$$p + (g-1)h(g-1)$$

annihilates B, and the above argument yields $B_1 = B_2$.

In order to make more progress we have had to assume that G/A is abelian. Before doing so, however, let us summarize the information we now have:

THEOREM 5·6. *Let G be a hypercentral p-group with upper central series*

$$1 = Z_0 \leqslant Z_1 \leqslant \ldots,$$

and suppose that Z_{i+1}/Z_i is cyclic of fixed order $p^n > 1$ for all finite i. Let $A = Z_\omega$. Then

(i) *A is a divisible Černikov subgroup of finite index in G.*

(ii) *$A = C_G(A)$.*

(iii) *Viewing A as a G-module by conjugation, write $A = A_1 + \ldots + A_n$, where each A_i is divisibly irreducible and $A_1, \ldots, A_n$ are all distinct. Let $C_i = C_G(A_i)$. Then the numbering can be chosen so that $G > C_1 > \ldots > C_n = A$.*

COROLLARY 5·7. *With the hypotheses of Theorem 5·6, if G/A is abelian, then it is cyclic.*

Proof. G/C_n is finite abelian and operates faithfully on the divisibly irreducible module A_n. Lemma 3·1 shows that $G/C_n = G/A$ is cyclic.

We now consider the case when G/A is cyclic of order p^l. Our previous notational conventions no longer operate. If X is any group and M any $\mathbb{Z}X$-module, we define the *upper X-central series* of M by: $M_0 = 0$, $M_{\alpha+1}/M_\alpha$ is the set of fixed points of X in M/M_α, and $M_\mu = \bigcup_{\alpha<\mu} M_\alpha$, for ordinals α and limit ordinals μ. Suppose that

$$M \in p\text{-Divmod}_{\mathbb{Z}X}$$

for some prime p, and let $M_1^\perp$ be the annihilator of M_1 in M^*. Then from the Introduction, $M_1^* \cong M^*/M_1^\perp$, and $M_1^\perp \cong (M/M_1)^*$. Therefore $M^*/M_1^\perp$ is an X-trivial factor module of M^*, and must actually be the largest such. Thus

$$M_1^\perp = [M^*, X] = \langle \phi(x-1) : \phi \in M^*, x \in X \rangle.$$

If we define the *lower X-central series* of an X-module N by

$$[N, {}_0X] = N, \quad [N, {}_{\alpha+1}X] = [[N, {}_\alpha X], X], [N, {}_\mu X] = \bigcap_{\alpha<\mu} [N, {}_\alpha X]$$

for ordinals α and limit ordinals μ, it follows that $M_\alpha^\perp = [M^*, {}_\alpha X]$ for all α, and $(M_{\alpha+1}/M_\alpha)^* \cong [N, {}_\alpha X]/[N, {}_{\alpha+1}X]$, as additive groups.

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

LEMMA 5·8. *Let H be a cyclic group of order $p^l > 1$, let $A_1 \in p\text{-Divmod}_{\mathbb{Z}H}$, and suppose that $A = A_1 + \ldots + A_n$, where each A_i is divisibly irreducible and n is minimal. Suppose H operates non-trivially on each A_i. Then each factor in the upper H-central series of A has order p^n.*

Proof. By hypothesis, n is minimal subject to the existence of an exact sequence $\bigoplus_{i=1}^{n} A_i \to A \to 0$, where each A_i is divisibly irreducible. Hence n is minimal subject to the existence of rationally irreducible $\mathbb{Z}_p H$-lattices $B_1, \ldots, B_n$ and an exact sequence $0 \to A^* \to \bigoplus_{i=1}^{n} B_i$. Taking $B_i = A_i^*$, each B_i is non-trivially transformed by H. Clearly $A^* \cap B_i \neq 0$ for all i, otherwise A^* can be embedded in $\bigoplus_{j \neq i} B_j$. Hence $|B_j : B_j \cap A^*| < \infty$, and $\left| \bigoplus_{j=1}^{n} B_j : A^* \right| < \infty$. Write $D = A^*$. By the remarks before the statement of the lemma, what we have to prove is that $|D(h-1)^i / D(h-1)^{i+1}| = p^n$, where $H = \langle h \rangle$. Since each B_i is rationally irreducible and not H-trivial, $C_{B_i}(H) = 0$. Hence $C_D(H) = 0$. Therefore $d \to d(h-1)$ is a monomorphism, and $D(h-1)^i \cong D$ for all i. So all that is really necessary is to show that $|D/D(h-1)| = p^n$.

By the considerations of section 3, each B_i can be identified with the ring of integers R_i in the field extension of $\mathbb{Q}_p$ by a primitive p^{t_i}th root of unity ζ_i, where $0 < t_i \leqslant f$ and h acts on R_i as multiplication by ζ_i. By the proof of Lemma 3·2, $\zeta_i - 1$ is a prime element of R_i generating the maximal ideal of R_i, and $|R_i / R_i(\zeta_i - 1)| = p$, since the extension is totally ramified. In other words,

$$|B_i : B_i(h-1)| = p \quad \text{and} \quad \left| \bigoplus_{i=1}^{n} B_i : \bigoplus_{i=1}^{n} B_i(h-1) \right| = p^n.$$

Now write $C = \bigoplus_{i=1}^{n} B_i$. Since $|C:D|$ is finite and necessarily a power of p, there exists an integer i such that $C(h-1)^i \leqslant D$. We have seen that $|C(h-1)^i : C(h-1)^{i+1}| = p^n$, and so multiplication by $h-1$ induces an endomorphism of $D/C(h-1)^{i+1}$ with kernel of order at least p^n. Hence $|D : D(h-1)| \geqslant p^n$. Since $E = C(h-1)^i$ is isomorphic to C and has finite index in D, the same reasoning shows that $p^n = |E : E(h-1)| \geqslant |D : D(h-1)|$, whence we obtain the required equality.

Before proceeding with the general case of our problem on groups with cyclic upper central factors, we digress to make some remarks about the case when the factors are of order p, which is rather easier than the general case.

PROPOSITION 5·9. *Let G be a Černikov p-group containing a divisible abelian normal subgroup $A = C_G(A)$, such that G/A is cyclic of order $p^l > 1$. The following conditions are equivalent*:

(i) *A has rank $\leqslant p^{l-1}(p-1)$.*

(ii) *A has rank exactly $p^{l-1}(p-1)$.*

(iii) *A is divisibly irreducible.*

(iv) *$|\zeta_{i+1}(G)/\zeta_i(G)| = p$ for all finite i*, where $1 = \zeta_0(G) \leqslant \zeta_1(G) \leqslant \ldots$ is the upper central series of G.

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

Proof. Let $H = G/A$.

(i) $\Rightarrow$ (ii). Since H operates faithfully on A, this follows from Corollary 3·6.

(ii) $\Rightarrow$ (iii). By Lemma 2·2, A contains a divisibly irreducible submodule B faithful for the cyclic group H. By Theorem 3·4, B has rank $p^{f-1}(p-1)$. Since B is additively a direct summand of A, $B = A$.

(iii) $\Rightarrow$ (iv). By Lemma 5·8, if B_i is the ith term of the upper H-central series of A, $|B_i| = p^i$. By Theorem 3·4 (iii), A/B_i is a faithful H-module, and so $C_{G/B_i}(A/B_i) = A/B_i$. It follows from this, by an easy induction, that $B_i = \zeta_i(G)$ for all finite i, yielding the claimed result.

(iv) $\Rightarrow$ (i). By Lemma 5·8, A is divisibly irreducible as H-module, and so A has rank $p^{f-1}(p-1)$ by Theorem 3·4, since it is a faithful H-module.

It is now not difficult to put together our results to show that if G is a hypercentral p-group such that $|\zeta_{i+1}(G)/\zeta_i(G)| = p$ for all finite i and $G/\zeta_\omega(G)$ is abelian, then $G/\zeta_\omega(G)$ is cyclic of order $p^f > 1$ and, for given f, G is isomorphic to one of two distinct groups according to whether G splits over $A = \zeta_\omega(G)$ or not. In this way, we can obtain the result of Baumslag and Blackburn (2) mentioned at the beginning of the section. Rather than spelling this out, however, we will press on with the general case.

Let $H = \langle h \rangle$ be a cyclic group of order $p^f > 1$ as above, and let

$$1 \leqslant r_1 < r_2 < \ldots < r_n = f$$

be integers. Let F denote the extension of $\mathbb{Q}_p$ by a primitive p^fth root of 1, ζ say, and let $R_i = \mathbb{Z}_p[\zeta^{p^{f-r_i}}]$ be the ring of integers in $\mathbb{Q}_p(\zeta^{p^{f-r_i}})$ (see Lemma 3·2). We form the external direct sum $\bigoplus_{i=1}^{n} R_i$, which we view as a $\mathbb{Z}_p H$-module by allowing h to act on R_i as multiplication by $\zeta_i = \zeta^{p^{f-r_i}}$. Let e_i denote the element of $\bigoplus_{i=1}^{n} R_i$ which has the component 1 in the ith place and zero elsewhere, let $U(r_1, \ldots, r_n)$ be the $\mathbb{Z}_p H$-submodule of $\bigoplus_{i=1}^{n} R_i$ generated by $e = \sum_{i=1}^{n} e_i$, and let $A(r_1, \ldots, r_n) = U(r_1, \ldots, r_n)^*$. Then we have

THEOREM 5·10. (i) *The factors of the upper H-central series of $A(r_1, \ldots, r_n)$ are cyclic of order p^n.*

(ii) *If $A \in p\text{-Divmod}_{\mathbb{Z}H}$, A is faithful for H and the H-centre of A is cyclic of order p^n, then $n \leqslant f$ and $A \cong A(r_1, \ldots, r_n)$ for some choice of $r_1, \ldots, r_n$ as above.*

This result is given by Zaicev ((19), section 6), who proves it by working entirely within p-Divmod$_{\mathbb{Z}H}$. We feel that the present less direct treatment is more transparent.

Proof. (i) For brevity, write $U = U(r_1, \ldots, r_n)$. By the remarks preceding Lemma 5·8, we have to show that $U(h-1)^i/U(h-1)^{i+1}$ is cyclic of order p^n, for all i. Since multiplication by $(h-1)^i$ induces a monomorphism on each R_i it induces one on U, and so all we need to show is that $U/U(h-1)$ is cyclic of order p^n. Since U is a cyclic $\mathbb{Z}_p H$-module, $U/U(h-1)$ is clearly a cyclic group, and by the last part of the proof of Lemma 5·8, its order will be correct if we can show that $\left| \bigoplus_{i=1}^{n} R_i : U \right| < \infty$.

For any j, U contains $eh^j = \sum_{i=1}^{n} e_i \zeta_i^j$. Let Tr denote the trace map from $F = \mathbb{Q}_p(\zeta)$ to

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

$\mathbb{Q}_p$, and let $S = \{j \in \mathbb{Z} : 1 \leqslant j < p^f, (j,p) = 1\}$. Then, for any integer $k \geqslant 0$, $\mathrm{Tr}(\zeta^k) = \sum_{j \in S} \zeta^{jk}$; also $\mathrm{Tr}(\zeta^{p^l}) = 0$ if $0 \leqslant l < f-1$, and $\mathrm{Tr}(\zeta^{p^{f-1}}) = -p^{f-1}$. This is because the minimal polynomial of ζ^{p^l} over $\mathbb{Q}_p$ is

$$1 + X^{p^{f-1-l}} + X^{2p^{f-1-l}} + \ldots + X^{(p-1)p^{f-1-l}}$$

and

$$(F : \mathbb{Q}_p(\zeta^{p^{f-1}})) = p^{f-1}.$$

Now U contains

$$\sum_{j \in S} eh^{jp^{r_1-1}} = \sum_{j \in S} \sum_{i=1}^{n} e_i \zeta^{jp^{f-r_i+r_1-1}} = \sum_{i=1}^{n} e_i \mathrm{Tr}(\zeta^{p^{f-r_i+r_1-1}}) = -e_1 p^{f-1}.$$

Since U also contains ep^{f-1}, it contains $\left(\sum_{i=2}^{n} e_i\right) p^{f-1}$. Operating on this element with $\sum_{j \in S} h^{jp^{r_1-1}}$ and arguing similarly, we find that U contains $e_2 p^{2(f-1)}$. Proceeding, we see that $p^{i(f-1)} e_i \in U$ for any i with $1 \leqslant i \leqslant n$. Hence $U \geqslant \left(\bigoplus_{i=1}^{n} R_i\right) p^{n(f-1)}$, and so U has finite index in $\bigoplus_{i=1}^{n} R_i$. This establishes (i).

(ii) Now let $A \in p\text{-Divmod}_{\mathbb{Z}H}$ be such that the H-centre of A is cyclic of order p^n. If we write A as a sum of divisibly irreducible submodules, then each is non-trivially transformed by H. By Lemma 5·8, the number of summands in a minimal such decomposition is n. Therefore $A = A_1 + \ldots + A_n$, where each A_i is divisibly irreducible and non-trivially transformed by H. Let $C_i = C_H(A_i)$. By Theorem 5·6, the A_i can be numbered so that

$$H > C_1 > \ldots > C_n = 1.$$

Let $H = \langle h \rangle$ and $C_i = \langle h^{p^{r_i}} \rangle$ $(1 \leqslant i \leqslant n)$. Then

$$1 \leqslant r_1 < \ldots < r_n = f.$$

By the proof of Lemma 5·8, A^* is isomorphic to a $\mathbb{Z}_p H$-submodule of finite index in $\bigoplus_{i=1}^{n} A_i^*$, which we can identify with $\bigoplus_{i=1}^{n} R_i$ in the above notation, by the considerations of section 3.

Since the H-centre of A is cyclic, $A^*/A^*(h-1)$ is cyclic, generated by the coset of an element x say. Thus $A^* = A^*(h-1) + B$, where $B = x.\mathbb{Z}_p H$. If A^*/B is non-zero, then it has a non-zero factor module annihilated by p, and hence a non-zero factor module annihilated by $h-1$. This contradicts the fact that $A^* = A^*(h-1) + B$. Therefore $B = A^*$, which is cyclic.

Now $U(r_1, \ldots, r_n)$ is also a cyclic submodule of finite index in $\bigoplus_{i=1}^{n} R_i$, as we have seen. If we can show that any two cyclic submodules of finite index of $\bigoplus_{i=1}^{n} R_i$ are isomorphic, it will follow that $A^* \cong U(r_1, \ldots, r_n)$, whence $A \cong A(r_1, \ldots, r_n)$. But if $Y = y.\mathbb{Z}_p H$ and $Z = z.\mathbb{Z}_p H$ are two such submodules, we can choose m such that $Yp^m \leqslant Z$. Then the annihilator $\mathrm{ann}\, z$ of z in $\mathbb{Z}_p H$ is contained in $\mathrm{ann}\, y$ (as $\mathbb{Z}_p H$ is commutative). By symmetry, $\mathrm{ann}\, y = \mathrm{ann}\, z$. Using the commutativity of $\mathbb{Z}_p H$ again, we obtain

$$Y \cong \mathbb{Z}_p H/\mathrm{ann}\, y = \mathbb{Z}_p H/\mathrm{ann}\, z \cong Z,$$

concluding the proof.

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

Continuing with the above notation, let A denote one of the modules $A(r_1, \ldots, r_n)$, and let $\langle a \rangle$ be its H-centre, which is cyclic of order p^n. Choose an integer m with $0 \leqslant m \leqslant n$, let $\langle g \rangle$ be a cyclic group of order p^{f+n-m}, and form the split extension $A\langle g \rangle$ of A by $\langle g \rangle$, allowing g to act on A like h and writing A multiplicatively. Then $\langle a, g^{p^f} \rangle$ lies in the centre of $A\langle g \rangle$. Let

$$G(f, r_1, \ldots, r_n, m) = A\langle g \rangle / \langle a^{p^m} g^{-p^f} \rangle.$$

Clearly this is independent, up to isomorphism, of the choice of the generator a. Now we can state our main theorem.

THEOREM 5·11. (i) *Let $f \geqslant 1$ be an integer and $n, r_1, \ldots, r_n, m$ be integers satisfying $1 \leqslant n \leqslant f$, $1 \leqslant r_1 < \ldots < r_n = f$, $0 \leqslant m \leqslant n$. Then $G = G(f, r_1, \ldots, r_n, m)$ is a hypercentral p-group such that $\zeta_{i+1}(G)/\zeta_i(G)$ is cyclic of order p^n for all finite i, and $G/\zeta_\omega(G)$ is cyclic of order p^f.*

(ii) *Let $e, k, s_1, \ldots, s_k, l$ be integers satisfying $e \geqslant 1$, $1 \leqslant k \leqslant e$, $1 \leqslant s_1 < \ldots < s_k = e$, $0 \leqslant l \leqslant k$. Then $G(f, r_1, \ldots, r_n, m) \cong G(e, s_1, \ldots, s_k, l)$ if and only if $f = e$, $n = k$, $m = l$, and $r_i = s_i$ $(1 \leqslant i \leqslant n)$.*

(iii) *If E is any hypercentral p-group such that $\zeta_{i+1}(E)/\zeta_i(E)$ is cyclic of order $p^n > 1$ for all finite i and $E/\zeta_\omega(E)$ is abelian, then $E/\zeta_\omega(E)$ is cyclic of order p^f for some $f > 1$ and $E \cong G(f, r_1, \ldots, r_n, m)$ for some integers $f, r_1, \ldots, r_n, m$ satisfying the conditions of* (i).

This gives us a parametrization of the groups in which we are interested in this section.

Proof. (i) Let $G = G(f, r_1, \ldots, r_n, m) = L/K$ in the above notation, where $L = A\langle g \rangle$ and $K = \langle a^{p^m} g^{-p^f} \rangle$. Then $A \cap K = 1$. If $C/K = C_G(AK/K)$, then $[C, A] \leqslant A \cap K = 1$, from which we easily find that $C = C_L(A) = \langle A, g^{p^f} \rangle = A \times K$. Let $\{Z_\alpha/K\}$ be the upper central series of G, $\{A_i\}$ be the upper $\langle h \rangle$-central series of A, and suppose we already know that $Z_i = A_i K$ and

$$C_L(A/A_i) = \langle A, g^{p^f} \rangle = A \times K$$

for some finite i. (This is certainly the case when $i = 0$.) Then

$$[Z_{i+1}, A] \leqslant Z_i \cap A = A_i K \cap A = A_i(K \cap A) = A_i,$$

and so $Z_{i+1} \leqslant A \times K$. Hence $Z_{i+1} = (Z_{i+1} \cap A) \times K$. Since $[Z_{i+1} \cap A, L] \leqslant Z_i \cap A = A_i$, we have $Z_{i+1} \cap A \leqslant A_{i+1}$, which gives $Z_{i+1} \leqslant A_{i+1} \times K$. The reverse is clear, so

$$Z_{i+1} = A_{i+1} \times K.$$

Clearly $C_L(A/A_{i+1}) \geqslant A \times K$. Strict inequality would imply that $g_1 = g^{p^{f-1}}$ centralizes A/A_{i+1}, whence $A(g_1 - 1)$ is finite and divisible. Then $A(g_1 - 1) = 0$, contradicting the fact that A is faithful for $\langle h \rangle$.

We now know that $Z_i = A_i K$ for all finite i. Hence Z_{i+1}/Z_i is cyclic of order p^n, from Theorem 5·10. We have $\zeta_\omega(G) = AK/K$, whence $G/\zeta_\omega(G)$ is clearly cyclic of order p^f.

(ii) Let $G = G(f, r_1, \ldots, r_n, m)$. We show how to determine $f, r_1, \ldots, r_n$ and m in terms of the structure of G. By (i), $|G/\zeta_\omega(G)| = p^f$ and $|\zeta_1(G)| = p^n$, so f and n are uniquely determined.

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

We have $G = L/K$, where $L = A\langle g\rangle$ as before, $A = A(r_1, \ldots, r_n) = A_1 + \ldots + A_n$, where A_i is a divisible and divisibly irreducible $\mathbb{Z}\langle g\rangle$-submodule of A such that $g^{p^{r_i}}$ generates $C_{\langle g\rangle}(A_i)$, and the decomposition is irredundant. This follows by reversing the argument at the beginning of the proof of Theorem 3·7. Let x be any element of G which generates G modulo $\zeta_\omega(G) = B$, and let $\psi: L \to G$ be the natural homomorphism. Then $x \equiv (g\psi)^s = (g^s)\psi \bmod B$ for some integer s with $(s, p) = 1$. View B as a $\mathbb{Z}\langle x\rangle$-module by conjugation. Then ψ determines a group isomorphism from A to B such that $(ag^s)\psi = (a\psi)\, x\, (a \in A)$. Let $B_i = A_i\psi\ (1 \leqslant i \leqslant n)$. Then $B = B_1 + \ldots + B_n$, the decomposition is irredundant, and since $\langle g^s\rangle = \langle g\rangle$, each B_i is divisible and divisibly irreducible under $\langle x\rangle$. Also, $x^{p^{r_i}}$ generates $C_{\langle x\rangle}(B_i)$.

By Theorem 3·7, if we take any irredundant decomposition $B = C_1 + \ldots + C_t$ of B (as $\mathbb{Z}\langle x\rangle$-module) into divisible and divisibly irreducible $\mathbb{Z}\langle x\rangle$-submodules, then $t = n$, and the C_i can be numbered so that $C_{\langle x\rangle}(C_i) = C_{\langle x\rangle}(B_i) = \langle x^{p^{r_i}}\rangle$. Therefore $r_1, \ldots, r_n$ are determined by choosing an arbitrary element x generating G modulo B, writing B as an irredundant sum of divisibly irreducible $\langle x\rangle$-submodules in any way, and calculating the centralizers of these submodules.

Now we shall calculate the order of x, showing that it is p^{f+n-m}. From this it will follow that m is determined by G. In the above notation, $x \equiv g^s\psi \bmod B$, where $(s, p) = 1$. We can choose an integer u prime to p such that $x^u \equiv g\psi \bmod B$, and since x and x^u have the same order, we may suppose that $x \equiv g\psi \bmod B$, that is, $x = gaK$ with $a \in A$. Now $1 + g + \ldots + g^{p^f-1}$ annihilates the $\langle g\rangle$-module A, since $A^* = U(r_1 \ldots, r_n)$ is a submodule of $\bigoplus_{i=1}^{n} R_i$, g acts on R_i as multiplication by ζ_i, and the minimal polynomial of ζ_i divides $1 + X + \ldots + X^{p^f-1}$. Hence

$$x^{p^f} = g^{p^f} a^{1+g+\ldots+g^{p^f-1}} K = g^{p^f} K.$$

Since $K \cap \langle g\rangle = 1$ and g has order p^{f+n-m}, it follows that $g^{p^f}K$ has order p^{n-m}, and x has order p^{f+n-m}. The proof of (ii) is now complete.

(iii) Let E be as given, and $B = \zeta_\omega(E)$. By Theorem 5·6 and Corollary 5·7, E is Černikov, B is its unique minimal subgroup of finite index, $B = C_E(B)$, and E/B is cyclic of some order $p^f > 1$. Let $E/B = \langle h\rangle$, where $h = gB$. Then B is a faithful $\langle h\rangle$-module by conjugation in E. Clearly the centre of E lies in B, so it coincides with the $\langle h\rangle$-centre of B and is cyclic of order p^n. By Theorem 5·10, $B \cong A(r_1, \ldots, r_n)$ for some choice of $r_1, \ldots, r_n$ with $1 \leqslant r_1 < \ldots < r_n = f$, and since g^{p^f} lies in the centre of E, it is clear that $E \cong G(f, r_1, \ldots, r_n, m)$ where p^{f+n-m} is the order of g.

To conclude this section, we mention an example to show that $G/\zeta_\omega(G)$ need not be abelian if G is a hypercentral p-group in which $|\zeta_{i+1}(G)/\zeta_i(G)| = p$ for all finite i. The possibilities for $G/\zeta_\omega(G)$ are probably rather numerous.

PROPOSITION 5·12. *Let H_1 be a cyclic group of order p, and recursively define*

$$H_n = H_{n-1} \wr H_1 \quad \text{for} \quad n > 1.$$

For $n \geqslant 1$, there exists a module $A_n \in p\text{-Divmod}_{\mathbb{Z}H_n}$ such that A_n is faithful for H_n and the factors of the upper H_n-central series of A_n all have order p. The split extension $G_n = A_n H_n$ is a Černikov p-group with $|\zeta_i(G_n)| = p^i$ for all $i \geqslant 0$, and $\zeta_\omega(G_n) = A_n$.

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

Proof. We begin by showing inductively that H_n has a faithful irreducible representation of degree $\phi(p^n) = p^{n-1}(p-1)$ over $\mathbb{Q}_p$ ($n \geqslant 1$). For $n = 1$, this follows for example from the argument of Theorem 3·4. Suppose that $n \geqslant 1$ and V is an irreducible $\mathbb{Q}_p H_n$-module faithful for H_n and of dimension $\phi(p^n)$ over $\mathbb{Q}_p$. We have $H_{n+1} \cong BH_1$, $B \lhd H_{n+1}$, $B \cap H_1 = 1$, where B, the base group, is a direct product of p copies of H_n cyclically permuted under conjugation by H_1. One of these copies will be identified with H_n, and H_n^* will denote the direct product of the rest.

We view V as a $\mathbb{Q}_p B$-module by allowing H_n^* to act trivially, and form the induced module $W = V^{H_{n+1}}$. Then $C_{H_{n+1}}(W) = 1$, and W is faithful. Also,

$$\dim_{\mathbb{Q}_p} W = p \dim_{\mathbb{Q}_p} V = \phi(p^{n+1}).$$

Now it is easy to show by induction that H_n contains an element of order p^n. In fact, if $x \in H_n$ has order p^n and $H_1 = \langle h \rangle$, then $(hx)^p = x^{h^{p-1}} x^{h^{p-2}} \dots x^h x$, which has order p^n, so hx has order p^{n+1}. Let y denote any element of order p^{n+1} in H_{n+1}. By Theorem 3·4, every irreducible $\mathbb{Q}_p\langle y \rangle$-module faithful for $\langle y \rangle$ has dimension $\phi(p^{n+1})$. Hence, and by Maschke's Theorem, W is irreducible when restricted to $\langle y \rangle$, and is *a fortiori* irreducible as $\mathbb{Q}_p H_{n+1}$-module. This completes the inductive proof.

Now let V_n denote any irreducible $\mathbb{Q}_p H_n$-module of dimension $\phi(p^n)$ and faithful for H_n, let $0 \neq v \in V_n$, and let U_n be the $\mathbb{Z}_p$-module spanned by the vh ($h \in H$). Then U_n is a rationally irreducible $\mathbb{Z}_p H_n$-lattice. Let $A_n = U_n^* \in p\text{-Divmod}_{\mathbb{Z}H_n}$. Then A_n is faithful for H_n. Let $x \in H_n$ have order p^n. Then by Lemmas 3·6 and 5·8, if B_i is the ith term of the upper $\langle x \rangle$-central series of A_n, $|B_i| = p^i$. Let C_i be the ith term of the upper H_n-central series of A_n. Then $0 < C_1 < C_2 < \dots$ as H_n is a finite p-group, while $C_i \leqslant B_i$, clearly. Hence $C_i = B_i$, and $|C_{i+1}/C_i| = p$, for all finite i. Notice also that A_n/C_i is a faithful H_n-module, for any finite i, as if $A_n(h-1) \leqslant C_i$ with $h \in H$, then $A_n(h-1)$ is both finite and divisible and so is zero.

It is now easy to show by induction that, if $G_n = A_n H_n$, then $\zeta_i(G_n) = C_i$ for all finite i. For

$$\zeta_{i+1}(G_n) \leqslant C_{G_n}(A_n/\zeta_i(G_n)) = C_{G_n}(A_n/C_i) = A_n,$$

whence $\zeta_{i+1}(G_n) \leqslant C_{i+1}$; the reverse is obvious.

6. *Elementwise divisibly irreducible groups of automorphisms.* Let G be a Černikov group with a divisible abelian subgroup A of finite index, and let $C = C_G(A)$, $H = G/C$. In studying certain finiteness conditions on locally finite groups, one encounters the situation where $A \neq 1$, $G \neq C$, and $N_G(B) = C$ for every infinite subgroup B of A (see **(4)**, **(14)**). Clearly A is then a divisible p-group for some prime p. The problem is to determine the possibilities for H. Thinking of A as a faithful H-module in the usual way, we see that $A \in p\text{-Divmod}_{\mathbb{Z}H}$, and A is divisibly irreducible when restricted to any non-trivial subgroup of H. In particular, this holds for the cyclic subgroups, so we say that A is elementwise divisibly irreducible, or that H operates elementwise divisibly irreducibly on A. We shall prove:

THEOREM 6·1. *Let H be a finite elementwise divisibly irreducible group of automorphisms of a non-trivial divisible Černikov p-group. Then H is cyclic, and either $|H| = p$, or $(|H|, p) = 1$.*

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

Special cases of this result have been obtained by Černikov (4), R. E. Phillips (14) and V. L. Phillips (15).

In keeping with the spirit of this paper, we prove Theorem 6·1 by considering instead the dual situation. If A is an elementwise divisibly irreducible module in p-Divmod$_{\mathbb{Z}H}$, then the restricted module A_E is divisibly irreducible for every non-trivial cyclic subgroup E of H, and so $A_E^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is an irreducible $\mathbb{Q}_p E$-module. Letting

$$V = A^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

we have that H is a finite group of linear transformations of V and is elementwise irreducible in the obvious sense. Conversely, if U is any finite-dimensional elementwise irreducible $\mathbb{Q}_p H$-module, faithful for H, then H leaves invariant and operates faithfully on some $\mathbb{Z}_p$ H-lattice U, and clearly U^* is an elementwise divisibly irreducible module in p-Divmod$_{\mathbb{Z}H}$ and is faithful for H. So our problem is really one about elementwise irreducible $\mathbb{Q}_p$-linear groups, and Theorem 6·1 follows from

THEOREM 6·2. *Let k be any field and H be a finite elementwise irreducible group of linear transformations of a finite dimensional k-space V. Then H is cyclic. If $k = \mathbb{Q}_p$, then either $|H| = p$ or $(|H|, p) = 1$.*

Proof. We first prove that H is cyclic by supposing this false and considering a counterexample of minimal order. We establish a number of properties of H.

(1) *Every proper subgroup of H is cyclic.*

(2) *$|H|$ is odd.* For if $2||G|$, then an element of order 2 operates irreducibly on V. Then $\dim_k V = 1$ and H, being isomorphic to a finite subgroup of the multiplicative group of k, is cyclic.

(3) *The Sylow subgroups of H are cyclic.* For let Q be a Sylow q-subgroup of H, where q is a prime divisor of $|H|$. Every abelian subgroup of Q is a finite irreducible abelian k-linear group, and so is cyclic. Hence, since q is odd by (2), Q is cyclic ((8), III·7·6).

(4) *H is not of prime power order.*

(5) *$H = QR$, where $Q \lhd H$, $|Q| = q$, R is a cyclic r-group, $|R/C_R(Q)| = r$, and q, r are distinct primes.* This follows by routine arguments. Let r be the smallest prime divisor of $|H|$ and R be a Sylow r-subgroup of H. Burnside's Theorem on normal complements shows that R has a normal complement Q which, being proper, must be cyclic. R is also cyclic, and so $[Q, R] \neq 1$. If follows that $[Q_0, R] \neq 1$ for some subgroup Q_0, of prime order q say, of Q. Then $Q_0 R$ is non-cyclic, whence $Q_0 = Q$. If R_1 is the maximal subgroup of R, then QR_1 is cyclic, and so $R_1 \leqslant C_R(Q)$. Finally, $R_1 = C_R(Q)$ since $H = QR$ is not cyclic.

Let $n = \dim_k V$.

(6) $n \leqslant r - 1$. To see this, notice first that both q and r are different from the characteristic of k, since an element of order equal to the characteristic of k cannot operate faithfully and irreducibly on V. Hence, by the considerations at the beginning of section 3, the dimension of a faithful irreducible module for a cyclic group of order r over k is $(k(\zeta):k)$, where ζ is a primitive rth root of 1. Since $1 + \zeta + \ldots + \zeta^{r-1} = 0$, $n = (k(\zeta):k) \leqslant r - 1$.

Now let E be the subring of End$_k$ V generated by k and Q, where we have identified k and H with their images in End$_k$ V in the obvious way. By Schur's Lemma, End$_{kQ}$ V

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

is a division ring, and clearly E is a k-subalgebra of the centre of $\mathrm{End}_{kQ} V$ algebraic over k. Hence E is a field, and since every E-subspace of V is kQ-invariant, $\dim_E V = 1$. Hence $\dim_k E = n$.

Since R normalizes Q, conjugation with elements of R (inside $\mathrm{End}_k V$) leaves E invariant and induces on it elements of the Galois group Γ of E over k. In fact, $R/C_R(Q)$ is isomorphic to a subgroup of Γ. Hence, from (5),

$$r = |R/C_R(Q)| \leqslant |\Gamma| \leqslant n.$$

This contradicts (6) and proves that G is cyclic.

Now we consider the case $k = \mathbb{Q}_p$. We may assume that $p \mid |H|$ and have to prove that $|H| = p$. Write $|H| = p^d l$, where $d \geqslant 1$ and $(p, l) = 1$. Suppose first that $l > 1$. Then V is irreducible when restricted to the subgroups of orders p and l respectively of H, and Lemma 3·3 and the remarks at the beginning of section 3 give

$$n = p - 1 = p^{d-1}(p-1)\, o(p,l) = o(p,l).$$

The last equation gives $p = 2$ and $d = 1$, whence $o(p, l) = 1$. This implies that $l \mid p - 1$, and since $p = 2$, that $l = 1$. We also have $p - 1 = p^{d-1}(p-1)$, whence $d = 1$. Hence $|H| = p$.

7. *A construction.* Let G be a Černikov group with maximal divisible abelian subgroup B, and let A be the Sylow p-subgroup of B. Then $\Omega_1(A)$ is a module by conjugation for the finite group $H = G/B$, and is in fact an $\mathbb{F}_p H$-module. We consider the question: given H, which $\mathbb{F}_p H$-modules can occur as $\Omega_1(A)$ in the above situation? In the notation of the Introduction, with $S = \mathbb{Z}$ and $R = \mathbb{Z}_p$, we have $\Omega_1(A)^* \cong A^*/A^*p$ as $\mathbb{Z}_p H$-modules. Thus, if V is an $\mathbb{F}_p H$-module of finite $\mathbb{F}_p$-dimension, $V \cong \Omega_1(A)$ for some $A \in p\text{-Divmod}_{\mathbb{Z}H}$ if and only if $V^* \cong C/Cp$ for some $C \in \mathrm{Lat}_{\mathbb{Z}_p H}$. We are immediately reminded of the well-known Fong–Swan Theorem about lifting modular representations to representations in characteristic zero ((6), theorem 72·1), but the version of that result usually given involves working over splitting fields. However, a version of the Fong–Swan Theorem which involves no splitting field hypotheses and is valid for $p \neq 2$ can be deduced from Isaacs' work on lifting Brauer characters (9), and this is exactly what we need. The results and arguments from this point on are all entirely due to I. M. Isaacs (unpublished), and I am most grateful for his permission to include them here.

THEOREM 7·1. *Let p be an odd prime, H a finite p-soluble group, and V an irreducible $\mathbb{F}_p H$-module. Then there exists $A \in p\text{-Divmod}_{\mathbb{Z}H}$ such that $\Omega_1(A) \cong V$.*

As we have explained above, this follows by taking $R = \mathbb{Z}_p$ in the following theorem:

THEOREM 7·2 (Isaacs). *Let R be a complete discrete valuation ring of characteristic zero with maximal ideal $P = \pi R$ and residue class field $\bar{R} = R/P$ of characteristic $p > 0$, let H be a finite p-soluble group, and let V be an irreducible $\bar{R}H$-module. Suppose that $p > 2$. Then there exists $U \in \mathrm{Lat}_{RH}$ such that $U/U\pi \cong V$ as $\bar{R}H$-module.*

The main result of Isaacs' paper (9) gives Theorem 7·2 with the added hypothesis that the field of fractions K of R is a splitting field for H and its subgroups, and yields a U which is unique subject to satisfying certain additional requirements. It is the absence of a uniqueness statement which prevents the proof given below from working

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

when $p = 2$, but Theorem 7·2 may nevertheless hold when $p = 2$ as far as we are aware. The deduction of Theorem 7·2 involves some fairly detailed change of field and Schur index considerations for ordinary and modular representations. The first lemma may be of independent interest. Throughout, ordinary irreducible characters are always understood to be absolutely irreducible.

LEMMA 7·3. *Let $R, P, \bar{R}, K$ be as above, and H be any finite group. Let χ be an ordinary irreducible character of H. Suppose that $K = K(\chi)$, and the restriction of χ to the set of p-regular elements of H is an irreducible Brauer character of H. Then χ is the character of an irreducible K-representation of H.*

For general facts about Brauer characters, see (5) or (6).

Proof. Let m be the exponent of H, $L = K(\sqrt[m]{1})$. Then by a well-known result of Brauer, L is a splitting field for H and all its subgroups. Let ν be the exponential valuation of K defined by $\nu(0) = \infty$, $\nu(u\pi^n) = n$ for any unit $u \in R$ and $n \in \mathbb{Z}$. Since K is complete with respect to ν, the latter can be uniquely extended to an exponential valuation of L, also denoted by ν ((18), 2-2-10). Let S be the ring of integers in L (with respect to ν), Q the maximal ideal of S, $\bar{S} = S/Q$. Since $Q \cap R = P$, $\bar{R}$ can be canonically identified with a subfield of $\bar{S}$, and since $\bar{S}$ contains every mth root of 1, it also is a splitting field for H and its subgroups.

Since L is a splitting field for H, there is an irreducible LH-module V with character χ. There is an SH-lattice U with $0 \neq U \leqslant V$.

Let χ^* denote the restriction of χ to the set of p-regular elements of H. The fact that χ^* is an irreducible Brauer character means precisely that U/UQ is an irreducible $\bar{S}H$-module. The values of the modular character of U/UQ (as distinct from the Brauer character) are obtained on p-regular elements by taking the values of the Brauer character χ^* modulo Q. Since $K = K(\chi)$, these all lie in $\bar{R}$. Therefore there exists an irreducible $\bar{R}G$-module T such that $T \otimes_{\bar{R}} \bar{S} \cong U/UQ$ ((10), theorem 9·14).

Let W be a projective indecomposable RH-module such that $W/WJ(RH) \cong T$, where $J(\ )$ denotes the Jacobson radical. For the existence of W, see (6), corollary 45·8. Since $T \otimes_{\bar{R}} \bar{S} \cong U/UQ$, T is an absolutely irreducible $\bar{R}G$-module, so $\mathrm{End}_{RH} T \cong \bar{R}$. By (6), lemmas 45·9 and 49·6, W is an absolutely indecomposable RH-module, so that $W \otimes_R S$ is an indecomposable SH-module. Clearly $W \otimes_R S$ is SH-projective and $\mathrm{Hom}_{SH}(W \otimes_R S, U/UQ) \neq 0$, so $W \otimes_R S$ is the unique projective indecomposable SH-module having U/UQ as its irreducible image. By (6), lemma 60·1, since χ^* is the Brauer character of U/UQ, the character Φ of $W \otimes_R S$ is given by

$$\Phi = \sum_{\theta} d_{\theta\chi^*}\theta,$$

where the $d_{\theta\phi}$ are the decomposition numbers of the ordinary irreducible characters θ of H with respect to the irreducible Brauer characters ϕ. By hypothesis, $d_{\chi\chi^*} = 1$, that is, χ has multiplicity one in Φ.

There is therefore an irreducible KH-submodule X of W^K such that the character of X involves χ with multiplicity exactly one. Since all the irreducible constituents of the character of X are Galois conjugate to χ over K ((10), theorem 9·21), while $K = K(\chi)$, it follows that χ is the character of X. This proves Lemma 7·3.

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

Proof of Theorem 7·2. We have an odd prime p, a finite p-soluble group H, and an irreducible $\bar{R}H$-module V. Let L, S, Q, $\bar{S}$ be as in the proof of Lemma 7·3. By (10), theorem 9·21, the modular character of V has the form $\sum_{\alpha \in \mathscr{G}} \theta^\alpha$, where θ is some absolutely irreducible character of H over $\bar{S}$ and $\mathscr{G}$ is the Galois group of $\bar{R}(\theta)$ over $\bar{R}$.

Let ϕ be the Brauer character associated to θ, $K_1 = K(\phi)$, $S_1 = S \cap K_1$. Since the values of ϕ are sums of roots of unity of order prime to p, K_1 is an unramified extension of K ((18), proposition 3-2-6). The Galois group $\mathscr{H}$ of K_1 over K fixes S_1 and $Q_1 = Q \cap S_1$ and is mapped isomorphically to the Galois group of $\bar{S}_1$ over $\bar{R}$ in the obvious way. Now an element of $\mathscr{H}$ which fixes θ also fixes ϕ. Hence $\bar{S}_1 = \bar{R}(\theta)$, and we can identify $\mathscr{H}$ and $\mathscr{G}$. It follows that the Brauer character of V is $\sum_{\alpha \in \mathscr{H}} \phi^\alpha$.

By Isaacs' Theorem (9), there exists an ordinary irreducible character χ of H which coincides with ϕ on the p-regular elements of H, and is uniquely determined by the condition that its values lie in a field generated over $\mathbb{Q}$ by a root of unity of order prime to p. Clearly $K_1 = K(\phi) \leqslant K(\chi)$. Unless $K(\phi) = K(\chi)$, there is an automorphism of $K(\chi)$ fixing ϕ but not χ, which would contradict the uniqueness of χ. Therefore $K_1 = K(\chi)$. We may apply Lemma 7·3 to conclude that χ is the character of an irreducible K_1-representation of H. Letting W be an irreducible KH-module whose character involves χ, we can conclude from (10), theorem 9·21, that the character of W is $\sum_{\alpha \in \mathscr{H}} \chi^\alpha$. Let U be a non-zero RH-lattice in W. Then the Brauer character of $U/U\pi$ is $\sum_{\alpha \in \mathscr{H}} \phi^\alpha$, the same as that of V. Therefore, by the fundamental theorem on Brauer characters, V and $U/U\pi$ have the same set of composition factors. Since V is irreducible, it follows that $V \cong U/U\pi$.

REFERENCES

(1) AZUMAYA, GORÔ. On generalized semi-primary rings and Krull–Remak–Schmidt's Theorem. *Japan J. Math.* **19** (1948), 525–547.

(2) BAUMSLAG, G. and BLACKBURN, N. Groups with cyclic upper central factors. *Proc. London Math. Soc.* (3), **10** (1960), 531–544.

(3) BERMAN, S. D. Representations of finite groups over an arbitrary field and rings of integers. *Izv. Akad. Nauk SSSR, Ser. Mat.* **30** (1966), 69–132 (Russian); *Amer. Math. Soc. Transl.* (*Series* 2) **64**, 147–215.

(4) ČERNIKOV, S. N. Groups with given properties of systems of infinite subgroups. *Ukrain. Mat. Z.* **19** (1967), 111–131 (Russian); *Ukrainian Math. J.* **19** (1967), 715–731.

(5) CURTIS, C. W. and REINER, I. *Representation theory of finite groups and associative algebras* (New York: Interscience, 1962).

(6) DORNHOFF, L. *Group representation theory, Part B* (New York: Marcel Dekker, 1972).

(7) HARTLEY, B. and MCDOUGALL, D. Injective modules and soluble groups satisfying the minimal condition for normal subgroups. *Bull. Australian Math. Soc.* **4** (1971), 113–135.

(8) HUPPERT, B. *Endliche Gruppen I* (Berlin: Springer-Verlag, 1967).

(9) ISAACS, I. M. Lifting Brauer characters of p-solvable groups. *Pacific J. Math.* **53** (1974), 171–188.

(10) ISAACS, I. M. *Character theory of finite groups* (New York: Academic Press, 1976).

(11) KAPLANSKY, I. Dual modules over a valuation ring I. *Proc. Amer. Math. Soc.* **4** (1953), 213–219.

(12) KAPLANSKY, I. *Infinite abelian groups* (University of Michigan Press, 1954).

(13) KEGEL, OTTO H. and WEHRFRITZ, BERTRAM A. F. *Locally finite groups* (Amsterdam: North Holland, 1973).

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press

(14) PHILLIPS, R. E. Infinite groups with normality conditions on infinite subgroups. *Rocky Mountain J. Math.* **7** (1977), 19–30.
(15) PHILLIPS, V. L. (to appear).
(16) ROTMAN, J. J. *Notes on homological algebra* (New York: van Nostrand Reinhold, 1968).
(17) THOMPSON, J. G. Vertices and sources, *J. Algebra* **6** (1967), 1–6.
(18) WEISS, EDWIN. *Algebraic number theory* (New York: McGraw-Hill, 1963).
(19) ZAICEV, D. I. The complementation of subgroups in extremal groups. Investigations of groups with prescribed properties of subgroups. *Mathematics Institute of the Academy of Sciences of the Ukrainian SSSR, Kiev*, 1974 (Russian).

https://doi.org/10.1017/S0305004100053834 Published online by Cambridge University Press