TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 172, October 1972

SPLIT AND MINIMAL ABELIAN EXTENSIONS OF FINITE GROUPS(1)

BY

VICTOR E. HILL

ABSTRACT. Criteria for an abelian extension of a group to split are given in terms of a Sylow decomposition of the kernel and of normal series for the Sylow subgroups. An extension is *minimal* if only the entire extension is carried onto the given group by the canonical homomorphism. Various basic results on minimal extensions are given, and the structure question is related to the case of irreducible kernels of prime exponent. It is proved that an irreducible modular representation of $SL(2, p)$ or $PSL(2, p)$ for p prime and ≥ 5 afford a minimal extension with kernel of exponent p only when the representation has degree 3, i.e., when the kernel has order p^3.

1. **Introduction.** Schur proved in 1911 that the central extensions of the unimodular group $SL(2, p^n)$ are all split (see [8]). Ashby Foote showed [4] that for an arbitrary finite group G which coincides with its own derived group, there is a central extension U of G which is universal in the sense that U admits no nonsplit central extension. In the special case $G \cong SL(k, p^n)$, U coïncides with G. No abelian extension with the property of Foote's central extension can exist because Gaschütz proved [5] that every finite group has a nonsplit abelian extension. Consequently, a useful question is how the existing nonsplit extensions may be classified.

The extensions farthest from splitting are those that H. Wielandt has called *minimal*, in which the only subgroup of E in the sequence

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1 \tag{1.1}$$

carried onto G by the canonical homomorphism is E itself. In this paper we show that in the special cases of $SL(2, p)$ and $PSL(2, p)$, if a minimal extension has an abelian kernel of exponent p which is also an irreducible KG-module (K the field of order p), that kernel must have order p^3. We also prove results on split and minimal extensions which, apart from any intrinsic interest, suggest why minimal extensions with elementary abelian kernels may be singled out for study.

Received by the editors September 22, 1971.

AMS (MOS) subject classifications (1970). Primary 20F25, 20G40; Secondary 20C20, 20K35.

Key words and phrases. Modular representations, projective modules, block of defect zero, linear groups over finite fields, generators and relations.

(1) Most of these results were included in the author's Ph. D. thesis written under the direction of Professor Charles W. Curtis at the University of Oregon.

We adopt the terminology that, in (1.1), E is an extension *of* G *by* A, E is *central* if A is in the center of E, and E is *abelian* if A is abelian. (This language conforms to that of many authors but differs, for example, from that of M. Hall [7].) If A is abelian, then E gives rise to a well-known homomorphism χ from G into the automorphism group of A such that

$$\chi(g)\colon a \longrightarrow a^g = (g')^{-1}ag' \tag{1.2}$$

where the g' come from a complete set of coset representatives for A in E, with each g' corresponding to $g \in G$ and $1'$ to $1 \in G$.

All groups will be assumed finite unless specified otherwise. The letters E, G, A will be reserved for groups with E an extension of G by A, and K or K_j will always denote the field of prime order p or p_j, respectively. Following Wielandt and others, the following notations will be used:

$C \leq B$ C is a subgroup of B,

$C < B$ C is a proper subgroup of B,

$C \trianglelefteq B$ C is a normal subgroup of B,

$C \triangleleft B$ C is a proper normal subgroup of B,

$|C|$ order of C,

$B \times C$ direct product of B and C,

$B \oplus C$ direct sum of (additive) B and C,

$\langle x, y, \cdots \rangle$ group generated by $\{x, y, \cdots\}$.

In particular, if E is an abelian extension, χ denotes the homomorphism (1.2), which makes A a G-module. Now

(1.3) A subgroup B of A is a G-submodule if and only if $B \trianglelefteq E$.

It will be useful to consider G-modules B/C where $C \leq B \leq A$ and $C, B \trianglelefteq E$; a special case is $B = A$, in which E/C is an extension of G by A/C.

We shall use several times a remark due to Dedekind:

(1.4) **Lemma.** *If X and Y are subsets of a group H, if $T \leq H$, and if $YT \subseteq Y$, then $(X \cap Y)T = XT \cap YT$. In particular, if $X, Y \leq H$, then $YT \subseteq Y$ may be replaced by $T \leq Y$.*

2. **Split abelian extensions.** We begin with two results relating the splitting of certain homomorphic images of an extension E to the splitting of E itself.

(2.1) **Theorem.** *Let E be an extension of G by A, with G and A finite or infinite. Let $A = A_1 \times \cdots \times A_r$ with $A_i \trianglelefteq E$ for $1 \leq i \leq r$, and $A_i^* = \Pi_{j \neq i} A_j$. Then*

(i) *E splits over A if and only if E/A_i^* splits over A/A_i^* for all $i = 1, \cdots, r$.*

(ii) *For any $r \geq 2$, E splits over A if and only if E/A_1 and E/A_2 split over A/A_1 and A/A_2, respectively.*

Proof. (i) Let E split over A, that is, suppose there is $G^* \leq E$ with $E =$

G^*A and $G^* \cap A = 1$. For fixed i, each $A_i^* \trianglelefteq E$, E/A_i^* is an extension of G by A/A_i^*, and $G^*A_i^* \leq E$. Now by (1.4),

$$(G^*A_i^*/A_i^*) \cdot (A/A_i^*) = G^*A/A_i^* = E/A_i^*$$

and

$$(G^* A_i^*/A_i^*) \cap (A/A_i^*) = (G^* \cap A)A_i^*/A_i^* = A_i^*/A_i^*.$$

Consequently, each E/A_i^* splits over A/A_i^*.

For the converse, there are subgroups $G_1^*, \cdots, G_r^*$ of E such that, for $1 \leq i \leq r$, $A_i^* \leq G_i^*$, $(G_i^*A)/A_i^* = E/A_i^*$, and $(G_i^*/A_i^*) \cap (A/A_i^*) = A_i^*/A_i^*$. Then $G_i^*A = E$ and $G_i^* \cap A = A_i^*$, for each i. Let $G^* = G_1^* \cap \cdots \cap G_r^*$. Then by r applications of (1.4) with the observation $A_i^* \leq G_i^*$,

$$\begin{aligned} G^*A &= G^*(A_1A_1^*) = (G_2^* \cap \cdots \cap G_r^*)A_2(A_3 \cdots A_r) \\ &= \cdots = G_r^*A_r = E, \end{aligned}$$

and

$$\begin{aligned} G^* \cap A &= (G_1^* \cap \cdots \cap G_{r-1}^*) \cap A_r^* \\ &= \cdots = G_1^* \cap (A_2^* \cap \cdots \cap A_r^*) = 1. \end{aligned}$$

(ii) First, let $E = G^*A$ with $G^* \cap A = 1$. Then for $j = 1, 2$,

$$(G^*A_j/A_j) \cdot (A/A_j) = G^*A_jA/A_j = E/A_j$$

and, by (1.4),

$$(G^*A_j/A_j) \cap (A/A_j) = (G^* \cap A)A_j/A_j = A_j/A_j;$$

therefore, E/A_1 and E/A_2 split.

Conversely, let $E/A_j = G_j^* A/A_j$ with $G_j^* \cap A = A_j$, for $j = 1, 2$. Let $B = G_1^* A_3 \cdots A_r$; then $B \leq E$ and $BA_2 = E$ since $A_1 \leq G_1$ and A is a direct product. Now let $G^* = B \cap G_2^*$. Then $G^*A = E$ by (1.4) together with $BA_2 = E$, and $G^* \cap A = B \cap A_2$. Now if $x \in B \cap A_2$, then $x = ba$ for some $b \in G_1^*$ and $a \in A_3 \cdots A_r$ (by definition of B), and $ba \in A_2$. Hence $b \in A$ and thus $b \in A_1$. Consequently, $ba \in A_1(A_3 \cdots A_r) \cap A_2 = 1$, and $x = 1$, so E is split.

(2.2) **Corollary.** *Let E be an extension of a finite or infinite group G by a finite nilpotent group A, let $A = A_1 \times \cdots \times A_r$ be a Sylow decomposition of A, and let $A_i^* = \prod_{j \neq i} A_j$ for $i = 1, \cdots, r$. Then*

(i) *E splits over A if and only if E/A_i^* splits over A/A_i^* for all $i = 1, \cdots, r$;*

(ii) *E splits over A if and only if E/A_j splits over A/A_j for two distinct $j \in \{1, \cdots, r\}$.*

Proof. The result follows immediately from (2.1) since a nilpotent group has a Sylow decomposition of the required form, where the A_i are characteristic subgroups of A.

This corollary suggests that splitting of abelian extensions may be approached through splitting of extensions by the Sylow subgroups of the kernels (where $A/A_i^* \cong A_i$). The next result shows that abelian kernels of prime exponent p and irreducible representations over the field K of order p are appropriate to be singled out for study.

(2.3) **Proposition.** *Let E be an extension of a (possibly infinite) group G by a finite abelian p-group A, let χ be as in* (1.2), *and let*

$$A = A_0 \rhd A_1 \rhd \cdots \rhd A_r = 1$$

be a χ-composition series for A (in the sense of (1.3)). *Then each factor A_{i-1}/A_i $(1 \leq i \leq r)$ is an abelian group of exponent p, affording an irreducible representation of G over the $K = \mathrm{GF}(p)$.*

Proof. Let $|A| = p^n$. Then A has a subgroup of order p^{n-1}, and the corresponding factor group is elementary abelian. Since A is finite, it has a proper normal subgroup A^* of smallest possible order such that A/A^* is elementary. It is easily shown that A^* is contained in every other subgroup of A yielding an elementary factor group and, moreover, that A^* is a characteristic subgroup of A. Hence $A^* \trianglelefteq E$ and, by (1.3), A^* is χ-invariant. Repeating this argument yields a series

$$A \rhd A^* \rhd A^{**} \rhd \cdots \rhd 1 \tag{2.4}$$

consisting of subgroups of A invariant under χ, which series can be refined to a χ-composition series for A in which each factor group is elementary abelian.

Now χ acts on A_{i-1}/A_i by restriction, and if A_{i-1}/A_i is written additively as a K-module, then χ is a representation of G over K afforded by the KG-module A_{i-1}/A_i. If this module were χ-reducible there would be a χ-invariant subgroup C/A_i which, by (1.3), would introduce a new term into the series (2.4). Hence A_{i-1}/A_i affords an irreducible K-representation, and the proof of (2.3) is complete.

Arguments similar to those in the proof of (2.1) yield

(2.5) Let E be an extension of G by A (with G and A finite or infinite). If A has a series

$$A = A_0 \rhd \cdots \rhd A_r = 1$$

such that $A_i \trianglelefteq E$ for each $i = 0, 1, \cdots, r$, and if there are subgroups $B_1, \cdots, B_r$ of E such that $E = B_1 A$ and $B_1 \cap A = A_1$ and, for each i, $B_i = B_{i+1} A_i$ and $B_{i+1} \cap A_i = A_{i+1}$, then E splits as $B_r A$.

Now the proof of a theorem of Marshall Hall may be applied to the special case of elementary abelian kernels to yield

(2.6) **Theorem** (see [7, Theorem 15.5.1]). *If E is an extension of G by A, A is an abelian group of prime exponent p, χ is as in* (1.2), *and A is a free KG-module affording χ, then E is split.*

This result may be generalized by (2.5) to obtain the following stronger result:

(2.7) **Theorem.** *If E is an extension of G by an abelian p-group A with χ: $G \longrightarrow \mathrm{Aut}(A)$ as in* (1.2), *and if $A = A_0 \rhd \cdots \rhd A_r = 1$ is a χ-normal series for A such that each factor is a free KG-module, then E is split.*

Proof. Since $A_i \trianglelefteq E$ (from the proof of (2.3)) E/A_1 is an extension of G by A/A_1, where A/A_1 affords a restriction of χ. By the hypothesis together with (2.6), E/A_1 splits as $(B_1/A_1)(A/A_1)$. The same argument applies to $A_2 \trianglelefteq B_1$ and the module A_1/A_2. Repetitions yield $B_1, \cdots, B_r$ satisfying the hypotheses of (2.5).

A principal result of this section is

(2.8) **Theorem.** *Let E be an extension of G by an abelian group A, let χ: $G \longrightarrow \mathrm{Aut}(A)$ as in* (1.2), *and let $A = A^1 \times \cdots \times A^s$ be a Sylow decomposition of A, where A^j corresponds to the prime p_j, $1 \le j \le s$. If for each p_j dividing $|G|$, each factor of some χ-normal series for A^j is a projective K_jG-module, then E is split.*

Proof. We consider first the special case in which A is an abelian p-group, that is, $s = 1$. Let $A = A_0 \rhd A_1 \rhd \cdots \rhd A_r = 1$ be a χ-normal series with projective factors, and let X be an arbitrary Sylow p-subgroup of G. Since A_{i-1}/A_i is projective, it is a direct sum of principal indecomposable modules of G, each of which, when viewed as a KX-module, is isomorphic to a direct sum of copies of the (right) regular KX-module KX (by a theorem of Green [6], see [3, (65.16)]). Hence A_{i-1}/A_i is isomorphic to a direct sum of copies of the regular KX-module and so is a free KX-module, for $1 \le i \le r$. Now let X^* be the restriction of E to X (i.e., X^* is the subgroup of E corresponding to X under the canonical homomorphism); then X^* is an extension of X by A, and A affords the restriction of χ to X. By (2.7), X^* splits over A. But p is the only prime dividing both $|A|$ and $|G|$. Moreover, by the Schur-Zassenhaus Theorem we have the fact that, for every prime $q \neq p$ dividing $|G|$, the restriction of E to some Sylow q-subgroup Q of G splits when regarded as an extension of Q by A. Hence (see [7, Theorem 15.8.6]) E splits over A.

To complete the proof of (2.8), let $A^j_* = \Pi_{k \neq j} A^k$. By (2.1), E splits if and only if E/A^j_* splits over A/A^j_* for $j = 1, \cdots, s$. Now A/A^j_* is χ-isomorphic to A^j, so E/A^j_* is an extension of G by an abelian p_j-group. If p_j divides $|G|$, then E/A^j_* splits by the special case above because the property of being a projective K_jG-module is carried over from the χ-normal factors of A^j to those of A/A^j_* by χ-isomorphism. If p_j does not divide $|G|$, then E/A^j_* splits by the Schur-Zassenhaus Theorem. Therefore, E splits.

In the terminology of modular representation theorv, we have

(2.9) **Corollary.** *Let E be an extension of G by an abelian group A, let χ be as in* (1.2), *and let $A = A^1 \times \cdots \times A^s$ be a Sylow decomposition of A, where A^j corresponds to the prime p_j, $1 \leq j \leq s$. If for each p_j dividing $|G|$, each factor of some χ-normal series for A^j, viewed as a K_jG-module, belongs to a block of defect* 0, *then E is split.*

Proof. By a result of Brauer and Nesbitt [2] (see [3, (86.3)]), each factor of the χ-normal series is a principal indecomposable K_jG-module. Hence by [3, (56.6)] each factor is projective. Thus if p_j divides $|G|$, then E/A^j_* splits, and with this one modification the proof of (2.8) applies.

This corollary shows that the application of modular representation theory to finding nonsplit abelian extensions entails the use of modules from blocks of defect greater than zero. If E is an abelian extension of G by A which does not split, then A must have a Sylow p-subgroup A^j for some p_j dividing $|G|$ such that A^j has a χ-normal factor which (viewed as a K_jG-module) belongs to a block of defect greater than zero.

3. **Minimal abelian extensions.** Let E be an extension of G by A (with G and A finite or infinite) and π: $E \to G$ the canonical homomorphism. Helmut Wielandt (in some unpublished work: see footnote 4 of [5]) has called E *minimal* if whenever $T \leq G$ and $\pi(T) = G$, it follows that $T = E$.

Equivalently, E is minimal if and only if $T \leq E$ with $TA = E$ implies $T = E$. Thus minimality may be regarded as the strongest sort of nonsplitting. Another useful characterization is

(3.1) E is a minimal extension of G by A if and only if A is contained in the Frattini subgroup of E.

This result was proved by H. Bechtell in [1] and was used earlier by Gaschütz in [5].

That not every nonsplit extension is minimal is clear from the quaternion group of order 8, regarded as an extension of a cyclic group of order 2 by one of order 4. However, under certain conditions it is true that every nonsplit extension is minimal. For example, the following result will be useful later:

(3.2) If E is an extension of G by an abelian group A of prime exponent p, and if A is an irreducible KG-module affording χ: $G \to \mathrm{Aut}(A)$, then E is either split or minimal.

Proof. If E is not minimal, then there is $T < E$ such that $TA = E$. Now $T \cap A < A$ since A is not contained in T. Moreover, $T \cap A \trianglelefteq T$ and $T \cap A \trianglelefteq A$ since A is abelian. Hence $T \cap A \trianglelefteq E$ and, by (1.3), $T \cap A$ is a proper KG-submodule of A. But A is irreducible, so E is split.

Three easy consequences are

(3.3) If E is an extension of a (possibly infinite) group G by a cyclic group of prime order, then either E is split or E is minimal.

(3.4) The only minimal extension of a finite cyclic group G is again a cyclic group.

(3.5) Let E be a minimal extension of G by A (with G and A finite or infinite), and let $B \leq A$ with $B \trianglelefteq E$. Then E/B is a minimal extension of G by A/B.

Proof. The first result follows immediately from (3.2). For the second, let $G = \langle g\colon g^n = 1\rangle$ and let E be a minimal extension of G by a finite A. Let g^* be a representative in E for the coset corresponding to g under the canonical homomorphism π. Then π carries $T = \langle g^* \rangle$ onto G, and $T = E$. For (3.5), if E/B is not minimal, then there exists $T < E$ with $B \leq T$ such that $(T/B)(A/B) = E/B$. But then $TA/B = E/B$ and $TA = E$, which contradicts the minimality of E.

Gaschütz has proved [5] that an arbitrary finite group G has a minimal extension $H^{(p)}$ of largest possible (finite) order such that the kernel H_p is abelian of exponent p (p a prime dividing $|G|$) and that $H^{(p)}$ is unique up to equivalence of extensions. Let B_p be a maximal proper KG-submodule of H_p; then H_p/B_p is an irreducible KG-module, and by (3.5), $H^{(p)}/B_p$ is a minimal extension of G by H_p/B_p. In fact, if E is any minimal extension of G by an abelian group A of exponent p, and if B is a maximal proper KG-submodule of A, then E/B is a minimal extension of G by A/B, and A/B is an irreducible KG-module. Consequently, a knowledge of the minimal extensions of G with irreducible kernels of exponent p is important for the investigation of minimal extensions.

(3.6) **Theorem.** *Let p be a prime ≥ 5 and let $G \cong \mathrm{SL}(2, p)$ or $\mathrm{PSL}(2, p)$. If an irreducible modular representation of G over $K = \mathrm{GF}(p)$ affords a minimal extension of G, then the representation has K-degree 3. Hence, if E is a minimal extension of G by a finite abelian group A of exponent p, then A is of order p^3.*

Proof.[2] Let A be an irreducible KG-module and $G \cong \mathrm{SL}(2, p)$. If A is faithful, then E is split since, if C is the centralizer in E of a coset representative corresponding to the central element of G, then $E = CA$ and $C \cap A = 1$. Hence we may assume that A is not faithful or that $G \cong \mathrm{PSL}(2, p)$; in either event, A is a $\mathrm{PSL}(2, p)$ module, and thus we may assume $G \cong \mathrm{PSL}(2, p)$.

(2) The author expresses his appreciation to the referee, who provided this shorter method of proof.

By (3.2), it suffices to prove that if the degree k of A is not 3, then E splits over A.

Let x^* be an element of order p in G, and let $y^* \in G$ be of order $(p-1)/2$ with $y^{*-1}x^*y^* = x^{*\lambda}$, where λ is a primitive $(p-1)/2$th root of 1 in K. Brauer and Nesbitt proved [2] that $\dim A = 2m+1 \leq p$ for some integer m, and A has a basis $\{a_i : -m \leq i \leq m\}$ with $a_i y^* = \lambda^i a_i$. Moreover, a_m spans the unique one-dimensional subspace of A which is invariant under the action of x^*. If $\dim A = p$, then by [2], A is projective, and, by (2.8), E is split. Hence we have $m < (p-1)/2$. A calculation performed on the representations in [2] shows that, for such m and for any $a \in A$,

$$\sum_{i=1}^{p} a x^{*\lambda i} = 0. \tag{3.7}$$

Let x be a p-element of E which maps to $x^* \in G$ and y be an element of order $(p-1)/2$ which maps to y^*. If we write A multiplicatively, the relations of the preceding paragraph become

$$y^{-1}a_i y = a_i^{\lambda^i}, \qquad x^{-1}a_m x = a_m,$$

and $\langle a_m \rangle$ is the center of the Sylow p-subgroup of E containing x. Hence there is some $c \in K$ such that

$$x^p = a_m^c. \tag{3.8}$$

Moreover, if $a \in A$, then $\prod_{i=1}^{p} x^{-\lambda i} a x^{\lambda i} = 1$, and $y^{-1}xy = x^{\lambda}b$ for some $b \in A$. Hence

$$\begin{aligned} y^{-1}x^p y = (y^{-1}xy)^p = (x^{\lambda}b)^p &= x^{p\lambda}\prod_{i=1}^{p} x^{-\lambda i} b x^{\lambda i} \\ &= a_m^{c\lambda} \quad \text{by (3.7) and (3.8).} \end{aligned}$$

But then

$$a_m^{c\lambda} = y^{-1}x^p y = y^{-1}a_m^c y = a_m^{c\lambda^m},$$

so $c(\lambda - \lambda^m) = 0$ in K. Thus either $c = 0$ or $\lambda = \lambda^m$. If $c = 0$, then $x^p = 1$ and the Sylow p-subgroup of E containing x splits over A. But then (see [7, Theorem 15.8.6]) E splits over A. Hence $\lambda = \lambda^m$ and $m = 1$, so $\dim A = 2m+1 = 3$.

The question of whether SL (2, p) or PSL (2, p) has more than one inequivalent minimal extension by an abelian group of type (p, p, p) has not yet been answered.

REFERENCES

1. H. F. Bechtell, *Reduced partial products*, Amer. Math. Monthly 72 (1965), 881–882. MR 32 #4185.

2. R. Brauer and C. Nesbitt, *On the modular characters of groups*, Ann. of Math. (2) 42 (1941), 556–590. MR 2, 309.

3. C. W. Curtis and I. Riener, *Representation theory of finite groups and associative algebras*, Pure and Appl. Math., vol. XI, Interscience, New York, 1962. MR 26 #2519.

4. S. A. Foote, *Universal central extensions of groups*, Ph. D. Thesis, University of Wisconsin, Madison, Wis., 1965.

5. W. Gaschütz, *Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden*, Math. Z. 60 (1954), 274–286. MR 16, 446.

6. J. A. Green, *On the indecomposable representations of a finite group*, Math. Z. 70 (1958/59), 430–445. MR 24 #A1304.

7. M. Hall, Jr., *The theory of groups*, Macmillan, New York, 1959. MR 21 #1996.

8. I. Schur, *Über die Darstellungen der symmetrischen und der alternierenden Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. 139 (1911), 155–250.

DEPARTMENT OF MATHEMATICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MASSACHUSETTS 01267