A NEW TYPE OF CHARACTERISTIC SUBGROUP OF PRIME-POWER GROUPS

H. R. BRAHANA

1. Introduction. In a recent paper **(1)** the fifty-eight metabelian groups of order p^{11} that are generated by five elements and have all their elements of order p were determined and characterized in terms independent of any particular selection of the generating elements. In dealing with fifty-seven of these groups there was no occasion to distinguish between one odd prime and another, except that in exhibiting canonical forms it was necessary to select irreducible polynomials and these, of course, depended on p. The fifty-eighth group was described in two ways in terms that were independent of p, but the proof of uniqueness could not be made without taking into account properties of p. These properties distribute the primes into classes, and the properties are reflected in the groups of order p^{11} in characteristic subgroups some of which exist for one prime and not for another. It may be that examination of the groups of isomorphisms of some of the fifty-seven groups would produce characteristic subgroups for one p that would not exist for another, but the writer considers it doubtful. The doubt is made plausible by the fact that examination of some of the likeliest groups yielded no such subgroups, and by the belief that if a group is described and a canonical form obtained without making use of any special property of the prime then anything that is true for a group with one p will have an analogue for one with another. The fifty-eighth group has some characteristic subgroups pointed to by geometric differences appearing with different types of primes. It is believed this phenomenon of prime-power groups has not been brought to light before.

2. The groups. The following properties determine a group $\bar{G}$ of order p^{15} for every value of p:

1. Elements are all, except identity, of order p;
2. The group is metabelian;
3. Central and commutator subgroup coincide;[1]
4. The group has five generators.

The groups of order p^{11} are obtained by adding four conditions on commutators of this group, on commutators only because a condition that contained one of the generators explicitly would give a group that would not satisfy 3. Any four independent conditions on commutators will give a group of order p^{11}, in certain well-defined cases again violating 3.

Received June 15, 1959.

[1]Of course 3 includes 2.

To get the group we are seeking we require the four conditions to be such that G of order p^{11} satisfy:

5. G contains no abelian subgroup of order p^8;
6. G contains no subgroup of order p^{10} whose commutator subgroup is of order p^4.

G satisfying these conditions exists for every p and it is unique. In establishing the uniqueness it is necessary to make use of different arguments for different p's and this points to different characteristic subgroups of G.

Groups of order p^{11} satisfying $1, \ldots, 5$ also satisfy 6 or

6′. G contains one subgroup of order p^{10} whose commutator subgroup is of order p^4.

For purposes of comparison we shall consider this group too. Looked at geometrically the situation is not so mysterious.

Let U_1, U_2, U_3, U_4, U_5 be generators of the group $\bar{G}$ of order p^{15}; let c_{ij} be the commutator of U_i and U_j; and let $\bar{C}$ be the group generated by the c_{ij}. Every element of $\bar{G}$ is

$$c\, U_1^{x_1}\, U_2^{x_2}\, U_3^{x_3}\, U_4^{x_4}\, U_5^{x_5},$$

where c is in $\bar{C}$ and x_i is an element in $GF(p)$. The set $(x_1, x_2, x_3, x_4, x_5)$ may be taken to be a point in a projective four-space X over $\mathrm{GF}(p)$. Then every element of $\bar{G}$ not in $\bar{C}$ determines a point in X; every point in X represents a cyclic subgroup of $\bar{G}/\bar{C}$ and also an abelian subgroup of order p^{11} of $\bar{G}$. The commutator of two elements

$$c\, U_1^{x_1} \ldots U_5^{x_5} \qquad \text{and} \qquad c' U_1^{y_1} \ldots U_5^{y_5}$$

does not depend on c or c'; it is a product of the c_{ij}'s; it can be represented by a point in a projective nine-space S, over $\mathrm{GF}(p)$, which has for co-ordinates the Plücker line-co-ordinates of the line on the two points x and y in X. The points of S which represent commutators belong to V, which is a $V_6{}^5$ corresponding to the grassmannian of lines in X. Every point P of S not on V determines a three-space R in X, and the lines of R determine a five-space Σ in S, a Σ intersects V in a $V_4{}^2$; there is only one Σ in S, determined by an R in X, which contains P. A line in S which lies in a Σ is called a Σ-line; its points not on V all determine the same R in X. A line in S not a Σ-line and not intersecting V determines a unique point M on V such that the plane on M and the line is tangent to V at M. The space tangent to V at M, that is, the space consisting of all points P in S such that PM is a ruling of V or such that the five-space Σ which contains P contains M and PM meets V only at M, is six-dimensional; any plane in such a tangent space is called a τ-plane.

The four conditions on commutators which reduces $\bar{G}$ of order p^{15} to G of order p^{11} set four independent elements of $\bar{C}$ equal to identity, and hence set equal to identity all the elements in the group generated by the four. These four elements of $\bar{C}$ are represented by four independent points of S, and the points determine a three-space S_3 in S. The group G is determined by the

https://doi.org/10.4153/CJM-1960-041-8 Published online by Cambridge University Press

relation of S_3 to V. When 5 is satisfied, S_3 has no point on V; when 5 and 6 are satisfied, S_3 contains no Σ-line; when 5 and 6′ are satisfied, S_3 contains one Σ-line. These groups exist, and they are the only ones when 5 is satisfied.

The condition that S_3 intersect V leads to a fifth-degree congruence, $f(x) \equiv 0$, mod. p. If $f(x)$ has no linear factor in GF(p), condition 5 is satisfied; conditions 6 and 6′ correspond respectively to $f(x)$ irreducible and $f(x)$ the product of an irreducible quadratic and an irreducible cubic. In the latter case the quadratic is connected with the Σ-line and the cubic with a τ-plane, both unique.

3. The characteristic subgroups. A point P in S not on V determines a three-space R in X, and R determines in $\bar{G}$ a subgroup $\bar{H}$ of index p. This subgroup is the direct product of a metabelian group of order p^{10} generated by four elements and an abelian group of order p^4. When $\bar{G}$ is reduced to G by setting equal to identity the elements of $\bar{C}$ which correspond to points of S_3 $\bar{H}$ becomes a group H of order p^{10} and its commutator subgroup remains of order p^6 if P is not in the five-space Σ determined by a point of S_3; the commutator subgroup of H will be of order p^5 if P is in the Σ determined by a point of S_3 not on a Σ-line of S_3; this commutator subgroup will be of order p^4 if P is in the Σ determined by a point of the Σ-line in S_3.

When 6′ is satisfied, the unique Σ-line in S_3 means that there is one and only one three-space R in X whose Σ in S intersects S_3 in a line. Hence G contains one subgroup only of order p^{10} with commutator subgroup of order p^4; the subgroup is therefore characteristic.

The τ-plane π, which is in S_3 when 6′ is satisfied, contains no Σ-line. Hence every point of π determines a subgroup of order p^{10} in G, whose commutator subgroup has order p^5, except for the point where π intersects the Σ-line. The τ-plane is in the space tangent to V at a point M, and from this follows that M is in the five-space Σ determined by each point of π. M is the image on V of a line m in X, and m lies in every R determined by a point of π. m determines in G a subgroup H_m of order p^8 which is non-abelian since M is not in S_3. The group H_m is characterized by the fact that it is the only group of order p^8 that is contained in every one of the $1 + p + p^2$ subgroups of order p^{10} determined by the points of π. H_m is therefore characteristic in G; it is in the characteristic subgroup of order p^{10} determined by the Σ-line.

These characteristic subgroups of orders p^8 and p^{10} together with conditions $1, \ldots, 5$ are enough to determine G, and they exist for every odd p. The subgroups are seen to be characteristic because they are uniquely defined. G has other characteristic subgroups which in number depend on p, but only on the size of p. The points of the τ-plane determine subgroups of order p^{10} of G. The vertices of the frame of reference in S_3 are completely determined if S_3 is in canonical form. (**1**, p. 699). The group of isomorphisms of G determines a group of collineations of X and this group leaves invariant every point of the τ-plane and it leaves invariant two points of the Σ-line, viz., its intersection with π and the conjugate of that point with respect to the quadratic intersection of V and the five-space Σ which contains the Σ-line. Thus every subgroup of order p^{10} determined by the points of π is characteristic.

It may be verified readily that the group of collineations of X induced by the group of isomorphisms of G is of order 2, and that the isomorphisms of G which induce the identity collineation constitute a group of order $(p - 1)p^{30}$, the $p - 1$ coming from replacing each U_i by its kth power, $k = 1, 2, \ldots, p - 1$ and the p^{30} from replacing U_i by $c_i U_i$ where the c_i's are arbitrary, independent elements of C. The order of the group of isomorphisms is therefore $2(p - 1)\, p^{30}$.

When 6 is satisfied S_3 contains no special line and no special plane. The relation of S_3 to V determines in S_3 $p^2 + 1$ "rational" cubic curves, one and only one through each point (**1**, pp. 704, 715–716). The group of collineations of X which transforms S_3 into itself is induced by the Galois group Γ of GF(p^5) relative to GF(p) and hence is of order 5. Γ transforms the cubics in sets of five and hence will leave invariant a number congruent to $p^2 + 1$, mod 5; and if a cubic is invariant it will contain $p + 1$, mod 5, invariant points.

The relation of S_3 to V, by which a point P determines a three-space R in X, serves to determine for any point A in R a quadric surface in S_3 which passes through P; by the same relation a point A in X but not in R determines a quadric in S_3 which does not pass through P. Thus the points of X determine in S_3 a four-parameter set W of quadrics. In X there is a locus J, of dimension three and order four, whose points determine in S_3 cones with one vertex; every point of S_3 is the vertex of one and only one such cone of the set W. Thus each point of S_3 determines a point in X, as well as the three-space R. Each point of J, in X, determines a plane σ in X which is the double tangent plane of J at the point, and intersects J in a conic C whose points determine the cones with vertices on one of the $p^2 + 1$ cubics; each of these $p + 1$ cones contains the cubic curve. Two of the planes σ intersect in a point which is not on J, and this point determines a non-degenerate ruled quadric which bears the two cubics corresponding to the two planes. Moreover, every point of a plane σ not on C is on another σ.

When $p = 5t + 1$, then both $p^2 + 1$ and $p + 1$ are congruent to 2, nod 5, and hence S_3 contains four points fixed under Γ. These four points determine four fixed points on J, the points which determine cones with vertices at the fixed points of S_3. Moreover, X contains a fifth fixed point, the point not on J which determines the non-degenerate ruled quadric containing the two fixed cubics. These five fixed points in X determine five abelian subgroups of order p^7 in G, and these subgroups are characteristic. They are contained in sets of two, three, four in subgroups of order p^8, p^9, and p^{10}, respectively, necessarily characteristic also.

This use of the five fixed points indiscriminately does not make full use of the geometry. Four of the fixed points in X are on J and one is not. Let the fixed point not on J be A_2. A_2 is on σ_1 and σ_2, the double tangent planes of J determined by the fixed cubics K_1 and K_2 in S_3. In σ_1 and σ_2 are conics C_1 and C_2, intersections of the planes with J. C_1 and C_2 are fixed under Γ and so are the polars l_1 and l_2 of A_2 with respect to C_1 and C_2. The other four fixed points, necessarily on J, are A_3 and A_5 on l_1 and C_1, and A_1 and A_4 on l_2 and C_2.

Distinctions can be made among the ten characteristic subgroups of order p^8 of G. We recall that each of the $1 + p + p^2 + p^3$ points of S_3 determines a unique three-space R of X and a subgroup of order p^{10} of G whose commutator subgroup has order p^5. A line in S_3 determines a line in X and also a set of $p + 1$ three-spaces in X, and a set of $p + 1$ subgroups of order p^{10} in G. Of the ten lines in X on pairs of the five points fixed under Γ, six are imaged on points of V at which the spaces tangent to V cut S_3 in lines; the remaining four do not have this property. Thus each of six of the characteristic subgroups of order p^8 is in $p + 1$ subgroups of order p^{10} whose commutator subgroups are of order p^5; each of the other four characteristic subgroups of order p^8 is in only one such group of order p^{10}.

Similar distinctions can be made among characteristic subgroups of orders p^9 and p^{10}; we will let one further example suffice. Every one of the characteristic subgroups of order p^{10} contains six of the characteristic subgroups of order p^8. The one given by $A_1 A_3 A_4 A_5$ contains the four subgroups of order p^8 described at the end of the last paragraph; each of the other four characteristic subgroups of order p^{10} contains only two of these.

When $p = 5t - 1$, S_3 contains two cubics fixed under Γ, but contains no fixed points. The cubics determine the planes σ_1 and σ_2 in X, and the intersection of σ_1 and σ_2 is a fixed point A_2. A_2 determines a characteristic subgroup of order p^7 which is abelian and the only characteristic subgroup of its order. σ_1 and σ_2 contain conics C_1 and C_2, on J, and the polars l_1 and l_2 of A_2 with respect to them. l_1 and l_2 determine characteristic subgroups of order p^8 of G. A_2 with l_1 and l_2 separately determines characteristic subgroups of order p^9, and l_1 and l_2 determine a characteristic subgroup of order p^{10}.

When $p = 5t \pm 2$, S_3 contains no fixed cubic and no fixed point. However, $1 + p + p^2 + p^3 + p^4 \equiv 1$, mod 5, and hence X contains one fixed point and one fixed three-space. Thus G contains one characteristic subgroup of each of orders p^7 and p^{10}; G contains no characteristic subgroup of order p^8 or p^9.

Thus a group of order p^{11} satisfying $1, \ldots, 6$ has characteristic subgroups in numbers and orders as follows:

	p^7	p^8	p^9	p^{10}
$p = 5t + 1$	5	10	10	5
$p = 5t - 1$	1	2	2	1
$p = 5t \pm 2$	1	0	0	1

4. Concluding remarks. The study of finite groups conformal with the abelian groups of orders p^n and type $1, 1, \ldots, 1$ immediately singles out the prime 2, since no such non-abelian group exists for $p = 2$. The maximum value of the class of a group whose elements are all of order p depends on the size of p, and so differentiates among primes; when the groups are restricted to be metabelian, that is, of class 2, this last distinction is lost. When the metabelian groups are ordered according to the number of generators, there is no occasion to distinguish one odd prime from another until this group of order p^{11} is reached. Because of a duality in the geometry, the determination in the paper cited of all the groups of order p^{α}, $\alpha \geqslant 11$, brings with it a determination of all of those for $\alpha \leqslant 9$. There remain to be examined the groups of order p^{10}. It is certain that many of the groups of order p^{10} will require different treatment for different primes.

Reference

1. H. R. Brahana, *Metabelian p-groups with five generators and orders p^{12} and p^{11}*, Illinois J. Math., *2* (1958), 641–717.

University of Illinois