REGULAR p-GROUPS

BY

AVINOAM MANN

ABSTRACT

Criteria for regularity of finite p-groups are derived. In particular, it is proved that regularity of a p-group G depends only on the sections of G of small class.

In this paper we consider finite p-groups. We recall that such a group, G, is *regular*, if for any pair of elements $a, b \in G$ we have

$$\text{(R)} \qquad (ab)^p = a^p b^p u_1^p \cdots u_n^p, \qquad u_i \in \langle a, b\rangle'.$$

The theory of regular p-groups was developed by P. Hall ([2], [3], see also [6, III. 10]). Since then, there have not been many additions to this theory. We mention the papers ([1], [8]) dealing with metabelian regular p-groups.

In this paper we give several criteria for p-groups to be regular. These criteria are proved using the concept of a minimal irregular group, i.e., an irregular p-group all of whose proper sections are regular. Our main result (Theorem 2) is a long list of properties of minimal irregular groups. The main corollaries of this list are the following (G denotes a finite p-group):

a) There exists an integer $k(p)$ (depending on p only) such that G is regular if and only if all its sections of class $k(p)$ at most are regular.

b) G is regular if all sections of exponent p^2 of $G \times G$ are regular.

Here result (a) relies on Kostrikin's solution of the restricted Burnside problem for exponent p.

In Section 2 we construct some examples of minimal irregular groups.

Notation and terminology

A group H is a *section* of a group G, if H is isomorphic to a factor group of a subgroup of G. A section H of G is *proper*, if H is not isomorphic to G. A group is

Received July 29, 1971

n-abelian for an integer n, if $(ab)^n = a^n b^n$ $(a, b \in G)$. Let G be a finite p-group. Then cl$G$ denotes the nilpotence class of G, G_n is the n-th term of the descending central series of G, $Z_n(G)$ is the n-th term of the ascending central series, $Z(G) = Z_1(G)$, $G' = G_2$ is the derived group, $\langle S \rangle$ is the subgroup of G generated by the subset S, $\Omega_i(G) = \langle a \mid a^{p^i} = 1 \rangle$, $\mho_i(G) = \langle a^{p^i} \mid a \in G \rangle$, $\Phi(G) = G' \mho_1(G)$ is the Frattini subgroup, and $M(G) = \langle u \mid (au)^p = a^p$, for each $a \in G \rangle$, $|G|$ denotes the order of G.

The author has had the pleasure and benefit of many stimulating conversations with Paul Weichsel regarding the topics of this paper.

1. Definition

A p-group P is a *minimal irregular group* if P is irregular, but all proper sections of G are regular.

We shall use the following well known result [7].

KOSTRIKIN'S THEOREM. *Among all finite p-groups of exponent p and 2 generators, there exists a unique maximal one, $G(p)$, such that all others are epimorphic images of $G(p)$.*

We let $c(p)$ be the class of $G(p)$, and $p^{n(p)}$ be its order.

THEOREM 1. *Let G be a finite p-group. If all sections of G of class at most $1 + c(p)$ are regular, then G is regular.*

PROOF. Assume that G is irregular. Then G involves some minimal irregular group, P say, and it will suffice to show cl$P \leqq 1 + c(p)$.

All proper subgroups of P are regular. Since regularity is determined by 2-generator subgroups, P can be generated by two elements. Moreover, there exists a pair of generators a, b for P such that a and b do not satisfy the regularity equation (R). Assume that P' has exponent greater than p. Then $\mho_1(P')$ is a non-trivial normal subgroup of P. Let T be a minimal normal subgroup of P such that $T \subseteq \mho_1(P')$. Then P/T is regular, so that we have $(ab)^p = a^p b^p c^p d$; where $c \in P'$ and $d \in T$. But then $c^p d \in \mho_1(P') = \mho_1(\langle a, b \rangle')$, which contradicts the choice of a, b. Thus P' has exponent p.

Now let $x \in P$, $u \in P'$. Then $\langle x, u \rangle$ is a proper subgroup of P, therefore regular. From the properties of regular groups it follows that $(xu)^p = x^p$ (since $u^p = 1$). Thus, $u \in M(P)$, i.e., $P' \subseteq M(P)$. But then P is its own centre (mod $M(P)$). From P. Hall's permutability theorem it follows that $\mho_1(P) \subseteq Z(P)$. ([4]; direct proof: let $a, b \in P$. Then $b^{-1}a^p b = (b^{-1}ab)^p = (a \cdot a^{-1}b^{-1}ab)^p = a^p$).

Now $P/Z(P)$ is a 2-generator p-group of exponent p and having 2 generators. Therefore, its class is at most $c(p)$, and cl$P$ is at most $1 + c(p)$.

In general, minimal irregular groups have easily described structure in many senses. We collect now what we consider to be the more important properties of such groups.

THEOREM 2. *Let P be a minimal irregular group of class c and exponent e. Then*

a) *P can be generated by two elements.*

b) *P' has exponent p; P/P' is of type (p^{e-1}, p).*

c) *$Z(P) = \Omega_1(P)$ and is cyclic of order p^{e-1}; $Z_{c-1}(P) = \Phi(P)$.*

d) *$P_c = Z(P) \cap P'$ and is the only minimal normal subgroup of P.*

e) *All proper sections of P have class less than c.*

f) *P is p^2-abelian.*

g) *If $e > 2$, then for all $1 \leqq l \leqq e, \Omega_l(P)$ consists of all elements of P of order at most p^l; $\mho_l(P)$ consists of all p^l powers of elements of P; and $P/\Omega_l(P) \cong \mho_l(P)$.*

h) *$P \times P$ has an irregular section of exponent p^2.*

i) *$c \leqq 1 + c(p)$; $|P| \leqq p^{e-1+n(p)}$.*

j) *P can be generated by two elements, a and b, such that $(ab)^p = a^p b^p$.*

k) *$M(P) = P'$.*

PROOF. Parts of the theorem have been deduced already in the proof of Theorem 1. Let T be a minimal normal subgroup of P. Then P/T is regular, and its derived group is of exponent p. By (R), P/T is p-abelian. If S is another minimal normal subgroup, P/S is also p-abelian, but then P itself is p-abelian and regular. Therefore P has a unique minimal normal subgroup. This means that $Z(P)$ is cyclic. P can be generated by any two elements a, b that are independent (mod $\Phi(P)$). In particular, if $Z(P) \nsubseteq \Phi(P)$, we can choose $a \in Z(P)$, but then a and b commute, and P is abelian. Thus

$$\mho_1(P) \subseteq Z(P) \subseteq \Phi(P) = P'\mho_1(P), \; Z(P) = \mho_1(P) \; (P' \cap Z(P)).$$

Here $P' \cap Z(P) \neq 1$ is of exponent p and cyclic, therefore of order p, so it is the unique minimal normal subgroup of P. In particular, $P' \cap Z(P) \subseteq \mho_1(P)$ and $Z(P) = \mho_1(P)$. As a cyclic group generated by elements of order p^{e-1} and less, $Z(P)$ has order p^{e-1}. Next, $P/Z_{c-1}(P)$ is abelian, so $Z_{c-1}(P) \supseteq P'$, and since $Z_{c-1}(P) \supseteq Z(P) = \mho_1(P)$, we get $Z_{c-1}(P) \supseteq \Phi(P)$. But if $Z_{c-1}(P) \neq \Phi(P)$, then

$|P:Z_{c-1}(P)| \leqq p$ which implies $P = Z_{c-1}(P)$ which does not hold. Thus (c) is proved.

Let $\bar{P} = P/P'$. Then $\mho_1(\bar{P}) \cong \mho_1(P)/\mho_1(P) \cap P'$ is cyclic of order p^{e-2}. Since $\bar{P}$ is a 2-generator abelian group, it must have a type (p^{e-1}, p). Also, we have seen that $P' \cap Z(P)$ is the only minimal normal subgroup of P. But $P_c \neq 1$, and $P_c \subseteq Z(P) \cap P'$, so (d) holds.

Each proper factor subgroup of P is a factor group of P/P_c, and thus has class less than c. On the other hand, if H is a maximal subgroup of P then $H \supseteq \Phi(P) = Z_{c-1}(P)$, so $\Phi(P) \subseteq Z_{c-1}(H)$ and $|H:Z_{c-1}(H)| \leqq p$ which implies that $H = Z_{c-1}(H)$ is of class less than c.

For (f), we notice that since P/P_c is p-abelian, we have for any elements $x, y \in P$: $(xy)^p = x^p y^p z$, $z \in P_c$. All factors on the right hand side of this equation lie in $Z(P)$ so we get

$$(xy)^{p^2} = (x^p y^p z)^p = x^{p^2} y^{p^2}.$$

The first part of (i) is just Theorem 1. The second part follows from what has been proved there together with $|\mho_1(P)| = p^{e-1}$.

For (g), consider first $S = \Omega_1$ ($P \bmod P_c$). Then $S \supseteq P'$, so $S \cap \Phi(P) = P'(S \cap \mho_1(P)) = P'\Omega_2(\mho_1(P))$ so $|P/S \cap \Phi(P)| = p^{e-1}$, while

$$|P/S| = |\mho_1(P/P_c)| = |\mho_1(P)/P_c| = p^{e-2}.$$

Let $x \in S - \Phi(P)$. Then $x^p \in P_c$. Assume $x^p \neq 1$, then we can find an element y such that $\Omega_2(\mho_1(P)) = \langle y \rangle$ and $x^p = y^p$. Since $y \in \Phi(P)$, we have $\langle x, y \rangle \neq G$ and $\langle x, y \rangle$ is regular, so that $(xy^{-1})^p = 1$. Let $z = xy^{-1}$. Then $z \in S - \Phi(P)$. From $P' \subseteq M(P)$ it follows that $\langle P', z \rangle$ has exponent p, and $|P/\langle P', z \rangle| = p^{e-1}$, so $|S/\langle P', z \rangle| = p$ and $S = \langle P', z, y \rangle$. Let $s \in S - \langle P', z \rangle$. Then $s = uy^i$, where $u \in \langle P', z \rangle$ and $i \not\equiv 0(p)$, so (using $y \in Z(P)$) $s^p = y^{ip} \neq 1$. Since $\Omega_1(P) \subseteq S$, we get that $\Omega_1(P) = \langle P', z \rangle$ has exponent p, and $|P/\Omega_1(P)| = p^{e-1} = |\mho_1(P)|$.

Moreover, $z \notin \Phi(P)$ implies that z is not a p-th power in $\bar{P} = P/P'$. The last group is of type (p^{e-1}, p), so $P/\Omega_1(P) \cong \bar{P}/\langle zP' \rangle$ is cyclic.

For $l > 1$, if $x \in P$ has order p^l then $x^p \in \mho_1(P)$, so $x^{p^{l-1}} \in P_c$. Thus $\Omega_l(P) = \Omega_{l-1}(P \bmod P_c)$, so $|P/\Omega_l(P)| = |P/P_c/\Omega_{l-1}(P/P_c)| = |\mho_{l-1}(P/P_c)| = |\mho_{l-1}(P)/P_c| = 1/p|\mho_{l-1}(P)| = |\mho_l(P)|$.

Thus, for $l \geqq 1$, $P/\mho_l(P) \cong \Omega_l(P)$, since the last two are cyclic groups of the same order.

For (h) we may assume $e > 2$. Let $P = \langle a, b \rangle$, where $b^p \in P'$, so $b^{p^2} = 1$. If $x \in P$, then $x = a^i b^j c$, where $c \in P'$, so $x^p = (a^i b^j)^p$. Since P is not p-abelian, we must have $(a^i b^j)^p \neq a^{ip} b^{jp}$ for some pair (i, j), and may as well assume $(a\, b)^p \neq a^p b^p$. By (g), a has order p^e.
Also

$$(ab)^p = a^p b^p t, \ t \in P_c, \quad t \neq 1.$$

Let P_i be isomorphic to P $(i = 1,2)$ under an isomorphism sending $x \in P$ to $x_i \in P_i$. Consider in $P_1 \times P_2$, $H = \langle (a_1, a_2), (b_1, u_2) \rangle$, where $u \in P'$. Then

$$\text{(A)} \qquad ((a_1, a_2)(b_1, u_2))^p = (a_1 b_1, a_2 u_2)^p = (a_1^p b_1^p t_1, a_2^p u_2^p)$$
$$= (a_1, a_2)^p (b_1, u_2)^p (t_1, 1).$$

With P, H is p^2-abelian, so $h \to h^{p^2}$ is an epimorphism from H onto $\mho_2(H)$. Therefore,

$$\mho_2(H) = \langle (a_1, a_2)^{p^2}, (b_1, u_2)^{p^2} \rangle = \langle (a_1^{p^2}, a_2^{p^2}) \rangle$$

and $(t_1, 1) \notin \mho_2(H)$. Thus, (A) shows that $H/\mho_2(H)$ is not p-abelian. Since $H/\mho_2(H)$ with P, has a derived group of exponent p, it is not regular.

A result of Hobby's [5] implies (j) since minimal irregular groups are certainly nearly regular in the sense of [5]. (Hobby also gives an example of a non-regular nearly regular group which is not minimal irregular.)

Lastly for (k) We have already seen in the proof of Theorem 1 that $P' \subseteq M(P)$. Assume $c \in M(P) - P'$. Then c has order p, and $c \notin \Phi(P)$. Let $P = \langle a, b \rangle$. We may assume that $a \notin M(P)\Phi(P)$, and then $P = \langle a, c \rangle$. In particular, we have $b = a^i c^j uz$, $u \in P'$, $z \in Z(P)$. Let $d = c^j u \in M(G)$. Then

$$a^p b^p = a^p (a^i dz)^p = a^p a^{ip} z^p$$

$$(ab)^p = (a^{i+1} dz)^p = a^{(i+1)p} z^p$$

$$\text{(B)} \qquad (ab)^p = a^p b^p$$

Equation (B) holds if $P \neq \langle a, b \rangle$, by Eq. (R) and the fact that P' has exponent p. Thus P is p-abelian and regular, a contradiction.

COROLLARY 1. *Let G be a finite p-group. If all sections of exponent p^2 of $G \times G$ are regular, then G is regular.*

REMARK Groups in which all sections of exponent p^2 are regular are called *weakly regular*. (This notion, discussed by P. Hall, was brought to my attention by P. M. Weichsel.) Most of (g) above follows immediately from properties of weakly regular groups.

For $e = 2$, (g) does not hold. Any irregular group of order p^{p+1} is minimal irregular of exponent p^2, in which $\mho_1(P)$ has order p and consists of p-th power [6, III.14.14]. One such group is the wreath product of two groups of order p, in which $\Omega_1(P) = P$ and thus $\Omega_1(P)$ contains elements of order p^2. Another such group was constructed by Blackburn. In it, $\Omega_1(P)$ contains only elements of order p, but has index p^2 [6, III,10.15].

The condition of Corollary 1 is not necessary for G to be regular. Thus, Weichsel [8] has constructed regular p-groups of exponent p^2, whose direct square is not regular.

Also, there does not hold any result of the form "If all sections of exponent at most p^e (where $e = e(p)$ depends on p only) are regular, then G is regular". This we show by constructing, in the next section, a minimal irregular group of exponent p^e, for each $e > 1$.

To conclude this section, we mention one more result, which is, in a sense, a generalization of the well-known criterion of P. Hall, "If $|G/\mho_1(G)| < p^p$, then G is regular".

COROLLARY 2. *Let G be a finite p-group. If for each 2-generator subgroup H, we have* $\mathrm{cl}\, H/\Omega_1(H) \leqq p - 2$, *then G is regular.*

Indeed, the restriction on the class would hold also for all 2-generator sections of G. If G is irregular, it has a minimal irregular section P, which has two generators and satisfies $\mho_1(P) = Z(P)$ and thus $\mathrm{cl} P \leqq p - 1$, a contradiction.

2. We begin by constructing the examples mentioned in the preceding section. For each p and each $e > 1$ we construct a minimal irregular group, which is metabelian, has class p and exponent p^e. The method is standard.

Let H be the abelian group $\langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \langle a_{p-1} \rangle$, where a_1 has order p^e and a_i has order p $(i > 1)$. Denote $a_p = a^{p^{e-1}}$. Let P be the splitting extension $H\langle b \rangle$, where $b^p = 1$ and $b^{-1}a_i b = a_i a_{i+1}$, for $1 \leqq i \leqq p - 1$. Then $P_k = \langle a_k, a_{k+1}, \cdots, a_p \rangle$, so $\mathrm{cl} P = p$. Since P has an abelian maximal subgroup, it is irregular [6, III.10.10]. Now $\langle a_i^p \rangle \subseteq Z(P)$, and $|P : \langle a_i^p \rangle| = p^p$, so if $Z(P) \neq \langle a_i^p \rangle$, then $\mathrm{cl} p < p$. Thus, $Z(P) = \langle a_i^p \rangle$ is cyclic, P has the unique minimal normal subgroup $\langle a_p \rangle = P_p$, so all proper factor groups of P are regular of class less than p. Next, $\Phi(P) = \langle a_1^p, a_2, \cdots, a_{p-1} \rangle$, so if K is a maximal subgroup of P, then $K = \langle a_1^p, a_2, \cdots, a_{p-1}, c \rangle$, for some c, and if $K \neq H$, then c must induce on H the same automorphism as b^i, for some i, so $K_k = P_{k+1}$ and K has class $p-1$. Thus P is minimal irregular with the required properties.

For $p = 2$, "regular" is the same as "abelian", so the minimal irregular groups are just the minimal non-abelian groups, which are well known.

Let P be a minimal irregular 3-group. Let $T = P_c$ be its minimal normal subgroup. Then P/T is a 2-generator regular 3-group. Therefore, P'/T is cyclic [6, III.10.3], and as it has exponent 3, $|P'/T| = 3$ and P' is elementary abelian of order 9. Let $K = C_p(P')$, then $|P:K| = 3$. Since K has $\Phi(P) = P'Z(P)$ as a central subgroup of index 3, K is an abelian maximal subgroup of P. Moreover, we have $|\mho_1(P)| = p^{e-1}$, so $|\Phi(P)| = p^e$ and $|P| = p^{e+2}$, so P has a normal cyclic subgroup of index p^2. It is now routine to describe all minimal irregular 3-groups.

References

1. W. Brisley and I. D. MacDonald, *Two classes of metabelian p-groups*, Math. Z. **112** (1969), 5–12.
2. P. Hall, *A contribution to the theory of groups of prime power orders*, Proc. London Math. Soc. **36** (1933), 29–95.
3. P. Hall, *On a theorem of Frobenius*, Proc. London Math. Soc. **40** (1936), 468–507.
4. P. Hall, *Verbal and marginal subgroups*, J. Math. **182** (1940), 156–157.
5. C. R. Hobby, *Nearly regular p-groups*, Canad. J. Math. **19** (1967), 520–522.
6. B. Huppert, *Endliche Gruppen I.*, Grud. Math. **134**, Berlin, 1967.
7. A. I. Kostrikin, *The Burnside problem*, Izv. Akad. Nauk SSSR Ser. Mat. **23** (1959), 3–34 (Russian) [English translation, Amer. Math. Soc. Transl. **36** (1964), 63–99].
8. P. M. Weichsel, *Regular p-groups and varieties*, Math. Z. **95** (1967), 223–231.

The Hebrew University of Jerusalem