REFERENCES

1. For a review, see: P. Pincus. "Selected Topics in Physics, Astrophysics and Biophysics." *Proceedings of XIV Latin American Summer School of Physics*, Caracas, Venezuela, July 1972. Edited by E. de Laredo and Jurisic. Dordecht: D. Reidel, 1973.
2. P. J. Strebel & Z. G. Soos. *J. Chem. Phys.* 53 (1970):4077.
3. K. Huang. *Statistical Mechancis*. New York: Wiley, 1967. Chap. 8.

*****

ON GROUPS GENERATED BY THE SQUARES

H. S. SUN
California State University, Fresno, CA 93740

1. INTRODUCTION

It was known that the quaternion group and the octic group could not be generated by the squares of any group [5, pp. 193-194]. A natural question is which groups are generated by the squares of some groups. Clearly, groups of odd order and simple groups are generated by their own squares. In this paper, we show in a concrete manner that abelian groups are generated by the squares of some groups, and we show that every group is contained in the set of squares of some group. We give conditions for the dihedral and dicyclic groups to be generated by the squares of some groups. Also we show that several classes of nonabelian 2-groups cannot be generated by the squares of any group.

2. NOTATIONS AND DEFINITIONS

Throughout this paper, all groups considered are assumed to be finite. For a group G, we let G^2 denote the set of squares, $I(G)$ the group of innerautomorphisms, $A(G)$ the group of automorphisms, $Z(G)$ the center, $|G|$ the order of G, G^1 the commutator subgroup. For any subset S of G, $\langle S\rangle$ denotes the subgroup generated by S. G is called an <u>S-group</u> if it is generated by the squares of some group L; to be more precise, there is a group L such that $\langle L^2\rangle$ is isomorphic to G.

3. CLASSES OF S-GROUPS

In a group of odd order, every element is a square; therefore, it is an S-group. A simple group is also an S-group since it is generated by its own squares; for, if the set of squares generates a proper subgroup, it would be a normal subgroup with abelian quotient. We next show that an abelian group is an S-group.

Theorem 3.1: An abelian group is an S-group.

Proof: Let G be an abelian group. Then

$$G = H_1 \times H_2 \times \cdots \times H_n,$$

where the H_i are cyclic groups. Let $|H_i| = k_i$. The permutation group generated by the n circular permutations

$$(a_{11}a_{12} \cdots a_{2k_2}), \ldots, (a_{n1}a_{n2} \cdots a_{nk_n}),$$

where the a_{ij} are $|G|$ distinct symbols, is isomorphic to G. Let L be the permutation group generated by the n circular permutations

$$(a_{11}a_{12} \cdots a_{1k_1} b_{11}b_{12} \cdots b_{1k_1}),$$
$$(a_{21}a_{22} \cdots a_{2k_2} b_{21}b_{22} \cdots b_{2k_2}), \ldots,$$
$$(a_{n1}a_{n2} \cdots a_{nk_n} b_{n1}b_{n2} \cdots b_{nk_n}),$$

where the b_{ij}'s are $|G|$ distinct symbols all different from the a_{ij}'s. Then clearly $L^2 \cong G$, and G is an S-group.

Using the same technique, we can prove the following:

Theorem 3.2: Every group is contained in the set of squares of some group. (See also [9].)

Proof: Let G be a group, and let P be a permutation group on n symbols isomorphic to G. We will construct a permutation group L such that P is isomorphic to a subgroup in L^2.

Let Q be a permutation group isomorphic to P on n symbols distinct from those of P. Let i be the isomorphism of P onto Q. If each element x in P is multiplied to $i(x)$ in Q, we obtain a group

$$R = \{xi(x) \mid x \in P\}$$

isomorphic to P. Clearly, each permutation in R is the square of a permutation in $2n$ symbols. Let L be the permutation group generated by the permutations whose squares are in R. Then $R \subset L^2$.

Unfortunately, homomorphic images of S-groups need not be S-groups. If, however, the kernel of the homomorphism is a characteristic subgroup of the S-group, then the homomorphic image is also an S-group. To prove this, we need the following lemma, which can be proved by straightforward set-inclusion.

Lemma 3.1: Let N be a normal subgroup of G which is contained in $\langle G^2 \rangle$. Then

$$\langle (G/N)^2 \rangle = \langle G^2 \rangle / N.$$

Theorem 3.3: Let G be an S-group, and let θ be a homomorphism from G onto $\overline{G}$ such that the kernel of θ is a characteristic subgroup of G. Then, $\overline{G}$ is an S-group.

Proof: Let L be a group such that $\langle L^2 \rangle = G$. Then, the kernel of θ, being a characteristic subgroup of G, is normal in L. By the lemma,

$$\langle (L/\text{kernel } \theta)^2 \rangle = \langle L^2 \rangle / \text{kernel } \theta = G/\text{kernel } \theta,$$

which is isomorphic to $\overline{G}$. Hence, $\overline{G}$ is an S-group.

As corollaries to Theorem 3.3, if G is an S-group, the quotient groups of its center, i.e., its group of inner-automorphisms, its Frattini subgroup, and its Fitting subgroup, are all S-groups.

Theorem 3.4: A nilpotent group is an S-group if and only if its Sylow 2-subgroup is an S-group.

Proof: Let G be a nilpotent group. Then $G = T \times H$, where T is a 2-group and H is a group of odd order. If T or H is trivial, then the Theorem is evident. Suppose T is an S-group, say $\langle F^2 \rangle \cong T$, letting $L = F \times H$, we have

$$\langle L^2 \rangle = G.$$

Conversely, let G be an S-group. T is a homomorphic image of G, with kernel of the homomorphism being H. Since H is a characteristic subgroup, by Theorem 3.3, T is an S-group.

4. DIHEDRAL AND DICYCLIC GROUPS

Theorem 4.1: A dihedral group D_m of order $2m$ is an S-group if and only if the congruence $t^2 \equiv -1 \pmod{m}$ has a solution.

Proof: D_m has presentation

$$a^m = b^2 = 1, \; b^{-1}ab = a^{-1}.$$

If there were a group L such that $\langle L^2 \rangle = D_m$, there would have to be elements c in L such that $c^2 = a^i b$, for some i. For $m = 2$, D_m is abelian, hence is an S-group. For $m = 4$, D_m is not an S-group. For $m \neq 1, 2, 4$, $\langle a \rangle$ is a characteristic subgroup of D_m, hence normal in L. Therefore,

$$c^{-1}ac = a^t,$$

but

$$(a^i b)^{-1} a (a^i b) = a^{-1},$$

so

$$a^{-1} = (a^i b)^{-1} a (a^i b) = c^{-1}(c^{-1}ac)c = c^{-1}(a^t)c = a^{t^2}.$$

$t^2 \equiv -1 \pmod{m}$ must have a solution.

Conversely, if $t^2 \equiv -1 \pmod{m}$ has a solution t_0, we define the group $L = \langle c,d \rangle$ as follows:

$$c^{2m} = d^4 = 1, \; d^{-1}cd = c^{t_0}.$$

Then clearly $\langle L^2 \rangle$ is isomorphic to D_m.

G. A. Miller stated [4, p. 152] that no dicyclic group can be generated by the squares of any group. The following theorem gives counterexamples to his statement [7]:

Theorem 4.2: A dicyclic group $D(m)$ of order $4m$ is an S-group if and only if $t^2 \equiv -1 \pmod{2m}$ has a solution.

Proof: For $m = 2$, $D(m)$ is not an S-group. For $m > 2$, let $D(m)$ have presentation

$$a^{2m} = b^4 = 1, \; b^2 = a^m, \; b^{-1}ab = a^{-1}.$$

If there were a group L such that $\langle L^2 \rangle = D(m)$, there would have to be an element c in L with $c^2 = a^i b$ for some $i = 0, 1, 2, \ldots, 2m - 1$. $\langle a \rangle$ is a characteristic subgroup of $D(m)$, hence normal in L. $c^{-1}ac = a^t$, for some t, but $(a^i b)^{-1} a (a^i b) = a^{-1}$; therefore,

$$a^{-1} = (a^i b)^{-1} a (a^i b) = c^{-1}(c^{-1}ac)c = c^{-1}a^t c = a^{t^2}.$$

Thus, $t^2 \equiv -1 \pmod{2m}$ must have a solution.

Conversely, if $t^2 \equiv -1 \pmod{2m}$ has a solution t_0, we define the group $L = \langle c,d \rangle$ by

$$d^4 = c^{2m},\ c^{4m} = d^8 = 1,\ d^{-1}cd = c^{t_0}.$$

Then clearly $\langle L^2 \rangle$ is isomorphic to $D(m)$.

5. 2-GROUPS

Since a nilpotent group is an S-group if and only if its Sylow 2-subgroup is an S-group, 2-groups are particularly important in the determination of S-groups.

Lemma 5.1: Let G be a 2-group, and let N be a normal subgroup of order 4. Then the index of the centralizer of N, $[G:C(N)]$, is at most 2.

Proof: Since N is normal, for a in N, every conjugate of a is also in N. The number of conjugates is either 1 or 2, because at least two of the elements of N are in $Z(G)$. This means that, for every a in N, the index of its centralizer, $[G:C(a)]$, is at most 2. If N is cyclic, let a be its generator, then $C(a) = C(N)$. If N is not cyclic,

$$N = \langle a \rangle \times \langle b \rangle, \text{ where } |a| = |b| = 2.$$

Let $a \in Z(G)$. If $b \notin Z(G)$, then $C(N) = C(b)$, so $[G:C(N)]$ is at most 2. If $b \in Z(G)$ also, then $C(N) = G$.

Lemma 5.2: Let G be a 2-group, let N be an abelian normal subgroup of order 8 contained in $\langle G^2 \rangle$. If $N = \langle a \rangle \times \langle b \rangle$, where a is an element of order 4 in $Z(\langle G^2 \rangle)$, then $N \subset Z(\langle G^2 \rangle)$.

Proof: Let M be a subgroup of N of order 2 contained in $Z(G)$. If M is not contained in $\langle a \rangle$, then

$$N = \langle a,M \rangle \subset Z(G) \cap \langle G^2 \rangle \subset Z(\langle G^2 \rangle).$$

If $M = \langle a^2 \rangle$, then b, an element of order 2 in N, can only be conjugate to b and ba^2, and the index of $C(b)$ is equal to the number of conjugates of b, so $[G:C(b)]$ is at most 2. Since $C(b)$ contains $\langle G^2 \rangle$, b is in $Z(\langle G^2 \rangle)$.

Theorem 5.1: A nonabelian 2-group with cyclic center is not an S-group.

Proof: By induction on the order of G; it is true for $|G| = 2^3$ [5, pp. 193-194]. Suppose that G is a group of lowest order with cyclic center and that there exists a 2-group L such that $\langle L^2 \rangle = G$. Let $\langle c \rangle$ be a subgroup of order 2 contained in $G \cap Z(L)$. Then, by Lemma 3.1, $\langle (L/\langle c \rangle)^2 \rangle = G/\langle c \rangle$. $Z(G/\langle c \rangle)$ cannot be cyclic if $G/\langle c \rangle$ is nonabelian. If $G/\langle c \rangle$ is abelian, then $G/\langle c \rangle = Z(G/\langle c \rangle)$. Since $\langle c \rangle$ is contained in $Z(G)$, $G/Z(G)$ is a homomorphic image of $G/\langle c \rangle$. $G/Z(G)$ is never cyclic, so $G/\langle c \rangle$ is not cyclic. Thus, in any case, $Z(G/\langle c \rangle)$ is not cyclic.

Let E be the largest elementary abelian 2-group contained in $Z(G/\langle c \rangle)$. Since $Z(G/\langle c \rangle)$ is not cyclic, $|E|$ is at least 4. E is a characteristic subgroup of $G/\langle c \rangle$, therefore normal in $L/\langle c \rangle$. There exist normal subgroups $\overline{M}$, $\overline{N}$ of $L/\langle c \rangle$ of orders 2 and 4, respectively, such that $\overline{M} \subset \overline{N} \subset E$. Let M and N be the normal subgroups of L which are the preimages of $\overline{M}$ and $\overline{N}$ under the natural homorphism of L onto $L/\langle c \rangle$. Then,

$$|M| = 4,\ |N| = 8, \text{ and } \langle c \rangle \subset M \subset N.$$

By Lemma 5.1, $[L:C(M)]$ is at most 2, which means

$$G = \langle L^2 \rangle \subset C(M), \text{ or } M \subset Z(G),$$

which is cylcic. Now N is abelian, $N \subset G\overline{N} \subset E$, which is noncyclic, so N is noncyclic; $M \subset N$, if M is cyclic, by Lemma 5.2, $N \subset Z(G)$, which contradicts the assumption that $Z(G)$ is cyclic.

Theorem 5.2: Let G be a nonabelian 2-group with commutator subgroup of index 4. Then G is not an S-group.

Proof: Suppose L is a 2-group with $\langle L^2 \rangle = G$, G' nontrivial, and $[G:G'] = 4$. Let N be a normal subgroup of L contained in G', with $[G':N] = 2$ [3, p. 127]. Then L/N is a 2-group such that $\langle (L/N)^2 \rangle = G/N$, by Lemma 3.1. But, $(G/N)' = G'/N$ is nontrivial, and the order of G/N,

$$[G:N] = [G:G'][G':N] = 8.$$

Thus, G/N is a nonabelian group of order 8 which cannot be an S-group. This contradiction shows that G is not an S-group.

Theorem 5.3: Let G be a nonabelian 2-group with $\langle G^2 \rangle$ cyclic and $[G:\langle G^2 \rangle] = 4$. Then G is not an S-group.

Proof: Use induction on the order of G. It is true for $|G| = 2^3$. Assuming the theorem for all 2-groups of order less than 2 , let G be a nonabelian group of order 2^n, and let $[G:\langle G^2 \rangle] = 4$ with $\langle G^2 \rangle$ cyclic. Suppose there is an L with $\langle L^2 \rangle = G$. We consider two cases with $|G'| = 2$ and $|G'| > 2$.

Let $|G'| = 2$. Then every noncentral element has just two conjugates, i.e., for every x in G, $[G:C(x)] \leq 2$. Hence,

$$\bigcap_{x \in G} C(x) = Z(G) \supseteq \langle G^2 \rangle.$$

Since $[G:Z(G)] \geq 4$, $Z(G) = \langle G^2 \rangle$. By Theorem 5.1, G is not an S-group.

Now suppose $|G'| > 2$. Since $\langle G^2 \rangle$ is cyclic, let $\langle G^2 \rangle = \langle c \rangle$. Then $|c| = 2^{n-2}$. Let a be the 2^{n-1}th power of c. Then $\langle a \rangle$ is a characteristic subgroup of order 2 in G, thus normal in L. Now $\langle (L/\langle a \rangle)^2 \rangle = G/\langle a \rangle$. Since $|G'| > 2$, G' is not contained in $\langle a \rangle$, so $G/\langle a \rangle$ is nonabelian. Moreover,

$$[G/\langle a \rangle : \langle (G/\langle a \rangle)^2 \rangle] = [G:\langle G^2 \rangle] = 4.$$

Therefore, $G/\langle a \rangle$ is a nonabelian 2-group of order 2^{n-1} with cyclic $\langle (G/\langle a \rangle)^2 \rangle$ of index 4. This contradicts the induction hypothesis.

Applying Theorems 5.1-5.3, we obtain the following theorems.

Theorem 5.4: Let G be a nonabelian 2-group whose center

$$Z(G) = \langle a \rangle \times \langle b \rangle, \text{ where } |a| = 2^n, \ |b| = 2.$$

If $Z(G)$ contains exactly one element which is not a square and is not in the commutator subgroup, then G is not an S-group.

Proof: Let c be the central element which is neither a square nor a commutator. Then $c = b$ or $a^i b$ for some i, so $Z(G)/\langle c \rangle = Z(G/\langle c \rangle)$ is cyclic. $\langle c \rangle$ is a characteristic subgroup of G. Since $c \notin G'$, $G/\langle c \rangle$ is nonabelian. By Theorem 5.1 $G/\langle c \rangle$ is not an S-group; by Theorem 3.3 G is not an S-group.

An example of this is the group of order 16 with presentation $a^4 = b^4 = 1$, $b^{-1}ab = a^{-1}$. Here, $a^2 b^2$ is a central element which is not in G' and is not a square, so the group is not an S-group [1, p. 146].

Theorem 5.5: Let G be a nonabelian 2-group with

$$\langle G^2 \rangle = \langle a \rangle \times \langle b \rangle, \text{ where } |a| = {}^n, \ |b| = 2.$$

Suppose $\langle G^2 \rangle$ contains exactly one element c which is not a square; also suppose that either $c \notin G'$ or $|G'| > 2$, and $[G:G'] = 4$. G is not an S-group.

The proof of this theorem is similar to that for Theorem 5.4. An example is the group G of order 3_2 with presentation

$$a^4 = b^2 = c^2 = d^2 = 1, \ d^{-1}ad = a,$$

$$d^{-1}cd = eb, \ c^{-1}ac = a^{-1},$$

where a^2 and b are central elements. Here

$$G' = \langle G^2 \rangle = \langle a^2, b \rangle,$$

and the element a^2b is not a square. By Theorem 5.5 G is not an S-group.

REFERENCES

1. W. Burnside. *Theory of Groups of Finite Order*. Dover, 1955.
2. W. Burnside. "On Some Properties of Groups Whose Orders are Powers of Primes." *Proc. Lond. Math. Soc.* (2), 11 (1912):225-245.
3. R. D. Carmichael. *Introduction to the Theory of Groups of Finite Order*. Dover, 1956.
4. G. A. Miller. *Collected Works*, V. University of Illinois, 1959.
5. W. R. Scott. *Group Theory*. Prentice-Hall, 1964.
6. H. S. Sun. "Embedding a Set into a Group." Unpublished doctoral dissertation, University of New Brunswick, 1969.
7. H. S. Sun. "A Group Whose Squares Generate a Dicyclic Group." *American Math. Monthly* 78, No. 9 (1971).
8. H. S. Sun. "Embedding a Semigroup in a Ring." *The Fibonacci Quarterly* 13, No. 1 (1975):50.
9. H. S. Sun. "Embedding a Group in the pth Powers." *The Fibonacci Quarterly* 16, No. 1 (1978):4.

*****

A PRIMER ON STERN'S DIATOMIC SEQUENCE—II

CHRISTINE GIULI

University of Santa Clara, Santa Clara, CA 95053

and

ROBERT GIULI

University of California, Santa Cruz, CA 96050

PART II: SPECIAL PROPERTIES

In 1929, D. H. Lehmer, at Brown University, presented a summary [1] of discovered results concerning Stern's sequence. Also, in July 1967, some additional results were reported by D. A. Lind [2]. In order to standardize the results, we will define Stern's sequence to be $s(i,j)$ where

(1) $s(i,0) = 1$, for $i = 0, 1, 2, \ldots$

(2) $s(0,j) = 0$, for $j = 1, 2, 3, \ldots$