

2-1994

# Square Roots of Finite Groups

Kashi Abhyankar

Daniel Grossman

Advisors:

Gary Sherman

Follow this and additional works at: [http://scholar.rose-hulman.edu/math\\_mstr](http://scholar.rose-hulman.edu/math_mstr)

 Part of the [Algebra Commons](#)

---

## Recommended Citation

Abhyankar, Kashi and Grossman, Daniel, "Square Roots of Finite Groups" (1994). *Mathematical Sciences Technical Reports (MSTR)*. 123.

[http://scholar.rose-hulman.edu/math\\_mstr/123](http://scholar.rose-hulman.edu/math_mstr/123)

MSTR 94-03

This Article is brought to you for free and open access by the Mathematics at Rose-Hulman Scholar. It has been accepted for inclusion in Mathematical Sciences Technical Reports (MSTR) by an authorized administrator of Rose-Hulman Scholar. For more information, please contact [weir1@rose-hulman.edu](mailto:weir1@rose-hulman.edu).

**SQUARE ROOTS OF FINITE GROUPS**

**Kashi Abhyankar and Daniel Grossman**

**MS TR 94-03**

**February 1994**

**Department of Mathematics  
Rose-Hulman Institute of Technology  
Terre Haute, IN 47803**

**FAX(812) 877-3198**

**Phone: (812) 877-8391**

# Square Roots of Finite Groups

Kashi S. Abhyankar\* and Daniel A. Grossman\*

February 21, 1994

## Abstract

Let  $G$  be a finite group of order  $n^2$ . A perfect square root of  $G$  is a subset  $X$  of  $G$  such that  $|X| = n$  and  $X^2 = G$ . Neither generalized dihedral groups nor groups of nilpotency class two have perfect square roots.

## 1 Introduction

Let  $G$  denote a finite group and for  $X \subseteq G$  let  $X^2 = \{x_1x_2 \mid x_1, x_2 \in X\}$ .

**Definition 1**  $X \subseteq G$  is a perfect square root of  $G$  if:

- i)  $X^2 = G$ , and
- ii)  $|X|^2 = |G|$ .

We are concerned with identifying those groups  $G$  which have perfect square roots. Let  $G$  be a group with perfect square root  $X$ . Each element of  $G$  occurs exactly once in a multiplication table for  $X$ . This gives the following:

**Fact 1** *No two elements of a perfect square root commute.*

---

\*Both authors supported by the NSF grant DMS-9100509

**Corollary 1** *If  $G$  has a perfect square root, then  $G$  is non-Abelian.*

**Corollary 2** *If  $G$  has perfect square root  $X$ , then  $X$  contains no elements of the center  $Z(G)$ .*

**Lemma 1** *If  $G$  has a perfect square root, then  $|G|$  is a multiple of 4.*

PROOF: The identity element  $e$  must be the product of two elements of  $X$ . Inverse pairs always commute, so we must have  $x^2 = e$  for some  $x \in X$ . We cannot have  $x = e \in X$ , for  $e$  is in the center  $Z(G)$ , so  $x$  must have order 2, making  $|G|$  even.  $|G|$  is a multiple of 4 because it is a perfect square.  $\square$

## 2 Necessary Conditions for Perfect Square Roots

We present two necessary conditions on groups having perfect square roots.

**Lemma 2** *If  $G$  has a perfect square root, then  $|Z(G)|^2 < |G|$ .*

PROOF: If  $X$  is a perfect square root for  $G$ , then no two elements of  $X$  represent the same coset of  $Z = Z(G)$  because

$$(az_1)(az_2) = (az_2)(az_1) \text{ for } az_1, az_2 \in aZ.$$

If we let  $|G| = n^2$ , there must be at least  $n$  cosets of  $Z$  from which to choose elements of  $X$ ; i.e.,  $[G : Z] \geq n$ . The strict inequality holds because of Corollary 2.  $\square$

**Lemma 3** *Let  $G$  be a finite group with perfect square root  $X$ . Then for each  $z \in Z(G)$  there is some  $x \in X$  such that  $x^2 = z$  (i.e., each element of  $Z(G)$  occurs on the main diagonal of a multiplication table for  $X$ ).*

PROOF: Each  $z \in Z(G)$  is the product of some  $x, y \in X$ . Since  $z$  is in the center and  $xy$  and  $yx$  are conjugate, it follows that  $xy = yx$ . This contradicts Fact 1 unless  $x = y$ .  $\square$

### 3 Perfect Square Roots of Generalized Dihedral Groups

We shall show that a generalized dihedral group,

$$D(m, n) = \langle a, b \mid a^m = b^n = 1, ba = a^{-1}b \rangle; \quad m, n \geq 2 \text{ and } n \text{ even,}$$

has no perfect square roots. The following lemma establishes this result for the class of dihedral groups ( $n = 2$  in the definition above).

**Lemma 4** *The dihedral group  $D_m = \langle r, f \mid r^m = f^2 = 1, fr = r^{-1}f \rangle$  does not have a perfect square root.*

**PROOF:** Suppose  $D_m$  has perfect square root  $X$ . Then  $X$  contains at most one rotation  $r^i$  (any two rotations commute) and at most one flip  $r^i f$  (since all flips are involutions). Every element of  $D_m$  is of one of these two forms, so  $|X| \leq 2$ , and  $|D_m| \leq 4$ , a contradiction.  $\square$

Note the following:

- Every element of  $D(m, n)$  is of the form  $a^i b^j$ , with  $0 \leq i < m$ ,  $0 \leq j < n$ .
- $|D(m, n)| = mn$ .
- If  $a^i = b^j$ , then  $a^i = b^j = 1$ .

**Fact 2** *If  $m$  is even, then  $Z(D(m, n)) = \langle a^{m/2}, b^2 \rangle$ . If  $m$  is odd, then  $Z(D(m, n)) = \langle b^2 \rangle$ .*

The following computation is the basis for our work on these groups:

**Fact 3** *For  $a^i b^j \in D(m, n)$ ,  $0 \leq i < m$ ,  $0 \leq j < n$ ,*

$$(a^i b^j)^2 = \begin{cases} b^{2j} & \text{if } j \text{ is odd.} \\ a^{2i} b^{2j} & \text{if } j \text{ is even.} \end{cases}$$

**Theorem 1** *For all  $m, n \geq 2$ ,  $D(m, n)$  does not have a perfect square root.*

**Lemma 5** *If  $G = D(m, n)$  has perfect square root  $X$ , then  $n \equiv 2 \pmod{4}$ .*

PROOF: Lemma 3 and Corollary 2 require a non-central involution  $a^i b^j \in X$ . Using Fact 3, we have two cases:

1:  $j$  is odd. Then  $1 = b^{2j}$ , which can be solved for odd  $j$  only if  $n \equiv 2 \pmod{4}$ .

2:  $j$  is even. Then  $1 = a^{2i} b^{2j}$ , implying that  $1 = a^{2i}$  and  $1 = b^{2j}$ . Fact 2 implies that all solutions to this for  $i, j$  with even  $j$  are in  $Z(G)$ , contradicting Corollary 2.  $\square$

**Lemma 6** *If  $G = D(m, n)$  has perfect square root  $X$ , then 4 divides  $m$ .*

PROOF: Certainly  $m$  must be even, for otherwise  $|G| = mn$  would not be a perfect square, because  $n \equiv 2 \pmod{4}$ . Now assume  $m = 4k + 2$ . Then  $a^{m/2} = a^{2k+1} \in Z(G)$ , so there is some  $a^i b^j \in X$  with  $(a^i b^j)^2 = a^{2k+1}$ . Since  $a^{2k+1} \neq 1$ ,  $j$  is even (Fact 3), so  $j = 0$  and  $a^{2i} = a^{2k+1}$ . Now we have  $2i \equiv 2k + 1 \pmod{m}$ , which cannot be satisfied for even  $m$ .  $\square$

PROOF OF THEOREM: Suppose  $G = D(m, n)$  has perfect square root  $X$ . By the previous two Lemmas, let  $m = 4x$ ,  $n = 4y + 2$ . Note that for  $0 \leq k \leq y$ ,  $a^{2x} b^{4k} \in Z(G)$ , and for some  $a^i b^j \in X$ , we have  $(a^i b^j)^2 = a^{2x} b^{4k}$ . If  $j$  is odd, then  $b^{2j} = a^{2x} b^{4k}$ , by Fact 3, which is impossible. So  $j$  is even, and we have  $b^{2j} = b^{4k}$ , which implies that

$$2j \equiv 4k \pmod{4y + 2}. \text{ Dividing,}$$

$$j \equiv 2k \pmod{2y + 1}, \text{ so}$$

$$j - 2k = t(2y + 1)$$

for some integer  $t$ . But  $j$  is even, so  $t$  must be even as well, and we get

$$j \equiv 2k \pmod{4y + 2}, \text{ i.e.,}$$

$$j = 2k.$$

So for every  $k = 0, 1, \dots, y$ ,  $X$  contains an element of the form  $a^h b^{2k}$ . All elements of this form commute with each other, because  $b^2 \in Z(G)$ . In the cases of  $k = 0$  and  $k = 1$  we have the commuting pair  $a^h b^0$  and  $a^{h'} b^2$  in  $X$ , which is a contradiction. The only exception is the case  $y = 0$ , i.e.,  $G$  is a standard dihedral group. This was addressed in Lemma 4.  $\square$

## 4 Facts about Groups of Nilpotency Class 2

It is our goal to show that groups of nilpotency class 2 cannot have perfect square roots. Throughout this section, assume  $G$  is of nilpotency class 2.

**Fact 4** *The derived subgroup  $G'$  is contained in the center  $Z(G)$ .*

**Corollary 3**  $[x, yz] = [x, y][x, z]$  and  $[xy, z] = [x, z][y, z]$  for all  $x, y, z \in G$ .

**Corollary 4**  $[x^m, y^n] = [x, y]^{mn}$  for all  $x, y \in G$ .

We now study the set  $Q(G) = \{q \in G \mid q^2 \in Z(G)\}$ .

**Fact 5**  $Q = Q(G)$  is a normal subgroup of  $G$ .

PROOF: Let  $q_1, q_2 \in Q$ . Then

$$(q_1 q_2^{-1})^2 = q_1^2 q_2^{-1} [q_2^{-1}, q_1] q_2^{-1} = q_1^2 q_2^{-2} [q_2^{-1}, q_1] \in Z(G),$$

which implies  $Q \leq G$ . The normality of  $Q$  follows because for  $x \in G$ ,

$$(x^{-1} q_1 x)^2 = x^{-1} q_1^2 x = q_1^2 \in Z(G). \square$$

**Lemma 7** *For  $k \in Q(G)$ , every commutator  $[k, g]$  has order 1 or 2.*

PROOF: By Corollary 4,  $[k, g]^2 = [k^2, g] = 1$ , since  $k^2 \in Z(G)$ .  $\square$

## 5 Perfect Square Roots in Groups of Nilpotency Class 2

Throughout this section, assume  $G$  is of nilpotency class 2 with perfect square root  $X$ .

**Definition 2**  $M(G) \subseteq G$  contains  $g \in G$  if  $g$  can be written as a product  $g_1 g_2 \dots g_n$  in such a way that each factor  $g_i$  occurs an even number of times, with occurrences of  $g_i^{-1}$  counted together with occurrences of  $g_i$ .

It is easy to see that  $M = M(G)$  is a normal subgroup of  $G$ .

**Lemma 8**  $G/M$  is an elementary Abelian two-group.

PROOF: If  $gM \in G/M$ , then

$$(gM)^2 = g^2 M = M. \square$$

**Lemma 9** Let  $C_G(Q)$  denote the centralizer in  $G$  of the subgroup  $Q = Q(G)$ . Then  $M \leq C_G(Q)$ .

PROOF: For  $q \in Q, m \in M$ , consider the commutator  $[q, m]$ . By the defining property of  $M$ , we can write

$$[q, m] = [q, g_1 g_2 \dots g_n] = [q, g_1][q, g_2] \dots [q, g_n]$$

(see Corollary 3) with each distinct  $g_i$  occurring an even number of times. All of these commutators are in the center  $Z(G)$ , so by Lemma 7, we can delete all pairs  $[q, g_i]^2$ . All that remains are products of commutators of the form  $[q, g_i][q, g_i^{-1}]$ . By Corollary 3 these each have product 1. So  $[q, m] = 1. \square$

Lemma 9 implies that no element of the perfect square root  $X$  is contained in  $M$ . Otherwise, such an element would commute with the elements of  $Q(G) \cap X$ , which is non-empty by Lemma 3, and contains at least two elements because a nilpotent group has a non-trivial center.



**Theorem 2** *If  $G$  has nilpotency class 2, then  $G$  has no perfect square root.*

PROOF OF THEOREM: We study the occurrences of elements of  $M$  in the multiplication table for a perfect square root  $X$ . Let  $\bar{X}$  denote the image of  $X$  in the quotient group  $G/M$ . Regard  $\bar{X}$  as a multiset rather than a set, because distinct elements of  $X$  may be contained in the same coset of  $M$ .

We obtain a lower bound on the number of occurrences of the identity  $1 \in G/M$  in the multiplication table for  $\bar{X}$ , corresponding to occurrences of elements of  $M$  in the multiplication table for  $X$ . Let the *distinct* elements of  $\bar{X}$  (the distinct cosets of  $M$  that are represented in  $X$ ) be  $a_0, a_1, \dots, a_{k-1}$ , and let  $|\bar{X}| = n = qk + r$ , with  $0 \leq r < k$ . List the elements of the multiset  $\bar{X}$  in the following order  $b_0, b_1, \dots, b_{n-1}$ :

- Let  $b_0 = a_0$ .
- Suppose  $b_i = a_j$ . Then let

$$b_{i+1} = \begin{cases} a_{j+1} & \text{if } j < k-1, \\ a_0 & \text{if } j = k-1, \end{cases}$$

unless all occurrences of  $a_{j+1}$  (or  $a_0$ , if appropriate) in  $\bar{X}$  have already been incorporated into the ordering, in which case we use the next  $a_m$  not already exhausted. Partition the multiset  $\bar{X}$  into submultisets  $S_0, S_1, \dots, S_{q-1}$  of cardinality  $k$  and submultiset  $S_q$  (possibly empty) of cardinality  $r$  as follows:

- For  $i < q$ ,  $S_i$  contains  $b_{ik}, b_{ik+1}, \dots, b_{ik+(k-1)}$ .
- $S_q$  contains  $b_{qk}, b_{qk+1}, \dots, b_{qk+(r-1)}$ .

It is clear that the elements of  $S_0$  are the distinct elements  $a_0, a_1, \dots, a_{k-1}$ . Note that the set of distinct elements of  $S_i$  is a subset of the set of distinct elements of  $S_{i-1}$ , because  $S_i$  contains at least one of each  $a_j$  that has not been exhausted in  $S_0, S_1, \dots, S_{i-1}$ .

We can now consider the multiplication table for  $\bar{X}$  as a union of tables  $S_i S_j$ , with  $0 \leq i, j \leq q$ . In the table  $S_i S_j$ , the number of occurrences of 1 is at least  $\min\{|S_i|, |S_j|\}$ , because if we assume  $i \leq j$ , then each element of  $S_j$  is present in  $S_i$ , and the square of any element of  $G/M$  is equal to 1 (by Lemma 8). Thus each row of the table  $S_i S_j$  contains an occurrence of 1. Clearly,

$$\min\{|S_i|, |S_j|\} = \begin{cases} k & \text{if } i, j < q. \\ r & \text{otherwise.} \end{cases}$$

Therefore the number of occurrences of 1 in the table for  $\bar{X}$ , which equals  $|M|$ , is bounded by the following:

$$|M| \geq \sum_{i=0}^q \sum_{j=0}^q \min\{|S_i|, |S_j|\} = kq^2 + 2qr + r.$$

We also have the following:

$$|G| = |X|^2 = (qk + r)^2 = k^2q^2 + 2kqr + r^2.$$

Consequently,

$$\begin{aligned} [G : M] &\leq \frac{k^2q^2 + 2kqr + r^2}{kq^2 + 2qr + r} \\ &= k \frac{k^2q^2 + 2kqr + r^2}{k^2q^2 + 2kqr + kr} \\ &\leq k, \end{aligned}$$

since  $r < k$ . Recall that  $a_0, a_1, \dots, a_{k-1}$  are distinct elements of  $G/M$ , and since the coset  $M$  cannot contain any elements of  $X$  (by Lemma 9), we have  $[G : M] > k$ , which is a contradiction.  $\square$