Irish Math. Soc. Bulletin
Number 88, Winter 2021, 69–77
ISSN 0791-5578

On Groups whose Squares are Subgroups

HOWEN CHUAH

ABSTRACT. Let G be a group. The square of G is the set G^2 consisting of elements of the form g^2, where $g \in G$. If G^2 is a subgroup of G, we say that G has the square subgroup property. In this article, we study several conditions related to the square subgroup property, including the order of G when it is a finite group. We also provide several examples of groups with or without the square subgroup property.

1. INTRODUCTION

Let G be a group. We define the square of G by

$$G^2 = \{x^2 \ ; \ x \in G\}.$$

A natural question is whether G^2 is a subgroup of G. If this happens, we say that G has the square subgroup property. This problem has been studied in [2][4]. In particular, for G finite, [4] provides a sufficient condition as follows. Let $|G|$ be its order.

Theorem 1.1. ([4], Thms.1.1,2.1,2.5)
If $|G|$ is odd, or G is abelian or a dihedral group, then G^2 is a subgroup of G.

Theorem 1.1 does not cover the cases where $|G|$ is even, and does not provide examples where G^2 is not a subgroup. We address these issues later in Theorems 1.3 and 1.4.

A property of G^2 is provided by its comparison with the commutator subgroup, as given by the next theorem. Recall that the commutator subgroup of G is defined by

$$G' = \text{subgroup of } G \text{ generated by } \{xyx^{-1}y^{-1} \ ; \ x, y \in G\}.$$

Theorem 1.2. *If G^2 is a subgroup of G, then $G' \subset G^2$.*

While Theorem 1.1 provides examples of groups with the square subgroup property, we shall construct several examples which do not have this property. Let S_n denote the symmetric group. Let $A_n \subset S_n$ denote the alternating group, namely A_n consists of all even permutations. If q is a power of a prime number (for example $2^2, 2^3, 3^2$), up to isomorphism there is a unique finite field with q elements, and we denote it by $\mathbb{F}_q$. Let $\mathrm{SL}_n(\mathbb{F}_q)$ denote the $n \times n$ matrices with entries in $\mathbb{F}_q$ and with determinant 1.

Theorem 1.3. *If G is one of the following, then G^2 is not a subgroup of G: non-abelian simple group, $A_n (n \geq 4)$, $S_n (n \geq 6)$, $\mathrm{SL}_2(\mathbb{F}_q)(q > 3)$, $\mathrm{SL}_n(\mathbb{F}_q)(n \geq 3)$.*

Since Theorem 1.1 says that all groups of odd orders have the square subgroup property, it remains to consider the groups of even orders. This is answered by the next theorem.

Theorem 1.4. *Let $n \in \mathbb{N}$. The following conditions are equivalent:*
(a) *Every finite group of order n has the square subgroup property.*
(b) *$n \leq 8$ or 4 does not divide n.*

2020 *Mathematics Subject Classification.* 20B05, 20B07.
Key words and phrases. square of group, square subgroup property.
Received on 30-5-2021; revised 30-9-2021.
DOI:10.33232/BIMS.0088.69.77.

For any $n > 8$ divisible by 4, the proof of Theorem 1.4 constructs a group of order n which does not have the square subgroup property. However, it is still far from exhausting all such groups. Therefore, it leads to an interesting problem for future study: For any $n > 8$ divisible by 4, find all the groups of order n which do not have the square subgroup property.

While the above discussions focus on finite groups, it is natural to study this problem for infinite groups as well, and yet there has been no existing work on it. We now study some examples of infinite groups. If $G = H \times K$ is a direct product of groups, then G^2 is a subgroup of G if and only if H^2 and K^2 are respectively subgroups of H and K. With this in mind, we obtain many examples of infinite groups G such that G^2 is not a subgroup. For instance if H is any one of the groups in Theorem 1.3, and $G = H \times \mathbb{R}^n$ is the direct product, then G^2 is not a subgroup of G. Conversely, the next theorem provides an example where G^2 is a subgroup. Let $\mathrm{GL}_n(\mathbb{C})$ be the multiplicative group of all $n \times n$ invertible complex matrices.

Theorem 1.5. *Let $G = \mathrm{GL}_n(\mathbb{C})$. Then $G^2 = G$.*

The main theorems are proved in the sections as follows.
Section 2: Theorem 1.2
Section 3: Theorem 1.3
Section 4: Theorem 1.4
Section 5: Theorem 1.5
We also prove several other results along the way, including Proposition 4.1, Proposition 4.5, and Theorem 4.6.

Acknowledgement. The author encounters this problem while taking a course in modern algebra, and is grateful to his teacher C. Y. Chang for providing great guidance. The author also thanks the referee for providing some helpful suggestions.

2. Commutator Subgroups

In this section, we prove Theorem 1.2. Let $C = \{xyx^{-1}y^{-1} \ ; \ x, y \in G\}$ consists of the commutators of G, and it generates the commutator subgroup $G' = \langle C \rangle$. The conditions for $C = \langle C \rangle$ is more complicated than $G^2 = \langle G^2 \rangle$. Nevertheless, Theorem 1.2 says that when the latter occurs, then G' is a subgroup of G^2.

Proof of Theorem 1.2:
Suppose that G^2 is a subgroup of G. For given $g \in G$ and $x \in G^2$, we write $x = a^2$ for some $a \in G$. Then $gxg^{-1} = ga^2g^{-1} = (gag^{-1})^2 \in G^2$. This implies that G^2 is a normal subgroup of G, so G/G^2 is a group.

For $g \in G$, we let $\overline{g} \in G/G^2$ denote the corresponding quotient element. For any $\overline{g_1}, \overline{g_2} \in G/G^2$, we have $\overline{g_1}^2\overline{g_2}^2 = \overline{e}\overline{e} = (\overline{g_1 g_2})^2 = \overline{g_1 g_2 g_1 g_2}$. So $\overline{g_1 g_2} = \overline{g_2 g_1}$, which implies that G/G^2 is abelian.

Let $g_1, g_2 \in G$. Since G/G^2 is abelian, $\overline{g_1 g_2} = \overline{g_2 g_1}$, so $\overline{g_1 g_2}(\overline{g_2 g_1})^{-1} = \overline{e}$. It follows that $g_1 g_2 g_1^{-1} g_2^{-1} \in G^2$. Hence G^2 contains all the commutators of G, namely $G' \subset G^2$. □

3. Square Subgroup Property

Let G be a finite group. If the square set G^2 is a subgroup of G, we say that G has the square subgroup property. In this section, we prove Theorem 1.3, which provides several families of examples where G does not have the square subgroup property.

The next proposition shows that the square subgroup property is preserved when taking quotients and direct sums.

Proposition 3.1. [4, Thm.2.2]
(a) *Suppose that G^2 is a subgroup of G, and N is a normal subgroup of G. Then $(G/N)^2$ is a subgroup of G/N.*
(b) *Let $G = \oplus G_\alpha$ be a direct sum of groups. Then G^2 is a subgroup of G if and only if each G_α^2 is a subgroup of G_α.*

Contrary to Proposition 3.1, the square subgroup property of G is not preserved when taking a subgroup H. This is illustrated by the following example. Recall that A_n consists of the even permutations of the symmetric group S_n.

Example 3.2. Let $G = S_4$ and $H = A_4$. We shall show that G has the square subgroup property, but H does not have the square subgroup property. We first claim that

$$G^2 = H. \tag{3.1}$$

It is clear that $G^2 \subset H$. Conversely, we consider

$$H = \{e\} \cup \{(a\ b)(c\ d)\} \cup \{(a\ b\ c)\}, \tag{3.2}$$

where $\{a, b, c, d\} = \{1, 2, 3, 4\}$. If $\sigma = (a\ b)(c\ d)$, then $\sigma = (a\ c\ b\ d)^2 \in G^2$. If $\sigma = (a\ b\ c)$, then $\sigma = (\sigma^2)^2 \in G^2$. Hence $H \subset G^2$, which proves (3.1) as claimed. So G^2 is a subgroup of G.

If $\sigma = (a\ b)(c\ d)$, then $\sigma^2 = e$. So (3.2) implies that $H^2 = \{e\} \cup \{(a\ b\ c)^2\}$, namely $|H^2| = 1 + 8 = 9$. This is not a factor of $|H| = 12$, so by Lagrange's theorem, H^2 is not a subgroup of H.

Recall that G is said to be solvable if there exists a chain of subgroups $\{e\} = H_1 \subset ... \subset H_n = G$ such that each H_i is a normal subgroup of H_{i+1}, and H_{i+1}/H_i is abelian. We will need the following lemma.

Lemma 3.3. *Every non-trivial finite solvable simple group is a cyclic group of prime order.*

Proof. Let G be a finite solvable simple group. Let $\{e\} = H_1 \subset ... \subset H_n = G$ be the chain of subgroups described above. Replacing n by a smaller number if necessary, we may assume that $H_{n-1} \neq G$. Since G is simple, it implies that $H_{n-1} = \{e\}$, so $G \cong G/H_{n-1}$ is abelian. Since a finite abelian simple group is a cyclic group of prime order, the lemma follows. □

The next theorem illustrates many examples where G do not have the square subgroup property. They include most of the finite simple groups and alternating groups.

Theorem 3.4.
(a) *Let G be a finite simple group, and suppose that G^2 is a subgroup of G. Then G is a cyclic group of prime order.*
(b) *$(A_n)^2$ is a subgroup of A_n if and only if $n \leq 3$.*

Proof. Let G be a finite simple group, and let G^2 be a subgroup of G. For all $x = a^2 \in G^2$ and $g \in G$, we have $gxg^{-1} = ga^2g^{-1} = (gag^{-1})^2 \in G^2$, hence G^2 is a normal subgroup of G. Since G is simple, we have $G^2 = \{e\}$ or $G^2 = G$, and we discuss them separately.

Suppose that $G^2 = \{e\}$. For all $a, b \in G$, $a^2b^2 = e \cdot e = e = (ab)^2$, so $ab = ba$. Therefore, G is abelian. By Lemma 3.3, G is a cyclic group of prime order.

Next suppose that $G^2 = G$. Then the mapping $f : G \longrightarrow G$ given by $f(g) = g^2$ is surjective. Since G is finite, f is bijective. If $|G|$ is even, then by Cauchy's theorem, G has an element of order 2, which contradicts the fact that f is bijective. So $|G|$ is odd. By the Feit-Thompson theorem (see for instance [1, p.104-106 Exercise12]), this implies that G is solvable. By Lemma 3.3, G is a cyclic group of prime order. This proves Theorem 3.4(a).

Next we prove Theorem 3.4(b). For $n \geq 5$, A_n is a non-abelian finite simple group. By Theorem 3.4(a), $(A_n)^2$ is not a subgroup of A_n. For $n = 4$, by Example 3.2, $(A_4)^2$ is not a subgroup of A_4. For $n \leq 3$, it is straightforward to check that $(A_n)^2$ is a subgroup of A_n. This proves Theorem 3.4(b). □

Our next objective is to show that for n large enough, $(S_n)^2$ is not a subgroup of S_n. We first state a useful lemma. We omit its proof, which is straightforward.

Lemma 3.5. *Let $\sigma = (a_1 \ ... \ a_m) \in S_n$ be an m-cycle. Then*

$$\sigma^2 = \begin{cases} (a_1 \ a_3 \ ... \ a_m \ a_2 \ a_4 \ ... \ a_{m-1}) & \text{if } m \text{ is odd,} \\ (a_1 \ a_3 \ ... \ a_{m-1})(a_2 \ a_4 \ ... \ a_m) & \text{if } m \text{ is even.} \end{cases}$$

For $x \in \mathbb{R}$, let $\lfloor x \rfloor \in \mathbb{Z}$ denote the largest integer such that $\lfloor x \rfloor \leq x$.

Theorem 3.6. *$(S_n)^2$ is a subgroup of S_n if and only if $n \leq 5$.*

Proof. Let $n \geq 6$. Assume that $(S_n)^2$ is a subgroup of S_n, and we shall derive a contradiction. There exists $k \in \mathbb{N}$ such that $\lfloor \frac{n}{2} \rfloor < 2k \leq n - 2$. Since $(S_n)^2$ is a subgroup of S_n, it is a normal subgroup, and hence it is one of $\{e\}$, A_n or S_n. But clearly $(S_n)^2$ cannot be $\{e\}$ or S_n. We obtain the remaining possibility

$$(S_n)^2 = A_n. \tag{3.3}$$

Consider $\sigma = (1 \ 2 \ ... \ 2k)(2k + 1 \ 2k + 2) \in S_n$. Note that $\sigma \in A_n$, so by (3.3), $\sigma = \tau^2$ for some $\tau \in S_n$. Let $\tau = \tau_1 \tau_2 ... \tau_s$ be a cyclic decomposition, where τ_i has length l_i. We have $(1 \ 2 \ ... \ 2k)(2k + 1 \ 2k + 2) = \sigma = \tau_1^2 ... \tau_s^2$. By Lemma 3.5, there exists j such that $l_j > 2k$, for otherwise there is no $(2k)$-cycle in τ^2, a contradiction. By Lemma 3.5, $l_j = 4k \geq 2(\lfloor \frac{n}{2} \rfloor + 1) > n$, which is a contradiction. We have shown that $(S_n)^2$ is not a subgroup of S_n for $n \geq 6$.

Next we consider $n \leq 5$. By direct computations, $(S_1)^2 = (S_2)^2 = \{e\}$, and $(S_3)^2 = A_3$. Also, Example 3.2 shows that $(S_4)^2 = A_4$. It remains to show that

$$(S_5)^2 = A_5. \tag{3.4}$$

Clearly $(S_5)^2 \subset A_5$. Conversely, pick $e \neq \sigma \in A_5$. Then σ is one of $(a \ b \ c)$, $(a \ b)(c \ d)$, $(a \ b \ c \ d \ e)$. The cases $(a \ b \ c), (a \ b)(c \ d)$ are treated in Example 3.2. If $\sigma = (a \ b \ c \ d \ e)$, then $\sigma = (\sigma^3)^2 \in (S_5)^2$. This proves (3.4). We have completed the proof of Theorem 3.6. □

Let F be a finite field. Let $\mathrm{SL}_n(F)$ be the $n \times n$ matrices with entries in F and with determinant 1, let $Z(\mathrm{SL}_n(F))$ be its center, and let

$$\mathrm{PSL}_n(F) = \mathrm{SL}_n(F)/Z(\mathrm{SL}_n(F)).$$

Recall that if q is a power of a prime number, we let $\mathbb{F}_q$ denote the unique finite field with q elements.

Lemma 3.7.
(a) $\mathrm{PSL}_2(\mathbb{F}_q)$ *is simple if and only if $q > 3$.*
(b) *If $n \geq 3$ and F is a finite field, then $\mathrm{PSL}_n(F)$ is simple.*

Proof. Lemma 3.7(a) is due to Jordan-Moore [3, Thm.8.13], and Lemma 3.7(b) is due to Jordan-Dickson [3, Thm.8.23]. □

The above lemma enables us to construct more examples of finite groups which do not have the square subgroup property.

Theorem 3.8. *Let q be a power of a prime number.*
(a) $(\mathrm{SL}_2(\mathbb{F}_q))^2$ *is not a subgroup of* $\mathrm{SL}_2(\mathbb{F}_q)$ *if* $q > 3$.
(b) *If* $n \geq 3$, *then* $(\mathrm{SL}_n(\mathbb{F}_q))^2$ *is not a subgroup of* $\mathrm{SL}_n(\mathbb{F}_q)$.
(c) $(\mathrm{GL}_n(\mathbb{F}_2))^2$ *is a subgroup of* $\mathrm{GL}_n(\mathbb{F}_2)$ *if and only if* $n \leq 2$.

Proof. Assume that $(\mathrm{SL}_2(\mathbb{F}_q))^2$ is a subgroup of $\mathrm{SL}_2(\mathbb{F}_q)$ for some $q > 3$. By Proposition 3.1(a), $(\mathrm{PSL}_2(\mathbb{F}_q))^2$ is a subgroup of $\mathrm{PSL}_2(\mathbb{F}_q)$. But by Lemma 3.7(a), $\mathrm{PSL}_2(\mathbb{F}_q)$ is a finite simple group, so by Theorem 3.4(a), it is cyclic of prime order. This is a contradiction, and we have proved Theorem 3.8(a).

Assume that $(\mathrm{SL}_n(\mathbb{F}_q))^2$ is a subgroup of $\mathrm{SL}_n(\mathbb{F}_q)$ for some $n \geq 3$. By Proposition 3.1(a), $(\mathrm{PSL}_n(\mathbb{F}_q))^2$ is a subgroup of $\mathrm{PSL}_n(\mathbb{F}_q)$. But by Lemma 3.7(b), $\mathrm{PSL}_n(\mathbb{F}_q)$ is a finite simple group, so by Theorem 3.4(a), it is cyclic of prime order. This is a contradiction, and we have proved Theorem 3.8(b).

Clearly $\mathrm{GL}_n(\mathbb{F}_2) = \mathrm{SL}_n(\mathbb{F}_2)$. For $n \geq 3$, $(\mathrm{SL}_n(\mathbb{F}_2))^2$ is not a subgroup of $\mathrm{SL}_n(\mathbb{F}_2)$ by Theorem 3.8(b). For $n = 2$, $\mathrm{SL}_2(\mathbb{F}_2) \cong S_3$, so $(\mathrm{SL}_2(\mathbb{F}_2))^2$ is a subgroup of $\mathrm{SL}_2(\mathbb{F}_2)$ by Theorem 3.6. The case of $n = 1$ is trivial. We have proved Theorem 3.8(c). □

Proof of Theorem 1.3:
We have shown that the following finite groups do not have square subgroup property.
Non-abelian simple groups: Theorem 3.4(a),
$A_n (n \geq 4)$: Theorem 3.4(b),
$S_n (n \geq 6)$: Theorem 3.6,
$\mathrm{SL}_2(\mathbb{F}_q)(q > 3)$, $\mathrm{SL}_n(\mathbb{F}_q)(n \geq 3)$: Theorem 3.8(a,b). □

4. Orders of Groups

In this section, we prove Theorem 1.4. Recall that G is said to have the square subgroup property if G^2 is a subgroup of G.

Proposition 4.1. *If* $|G| = 2k$ *where* k *is odd, then* G^2 *is a subgroup of* G.

Proof. Suppose that $|G| = 2k$, where k is odd. Then G contains a subgroup H of index 2 (see p.122, Ex.13 of [1]). We claim that

$$H = H^2 \subset G^2. \tag{4.1}$$

To obtain (4.1), the only thing to prove is $H \subset H^2$. Since $|H| = k$ is odd, we have $k + 1 = 2r$ for some $r \in \mathbb{N}$. Pick $x \in H$. We have $x = xx^k = (x^r)^2 \in H^2$. This proves that $H \subset H^2$, which implies (4.1) as claimed.

Conversely, we claim that

$$G^2 \subset H. \tag{4.2}$$

Pick $x = g^2 \in G^2$, where $g \in G$. Since H is of index 2 in G, H is normal in G, so G/H is a group. Now $xH = g^2H = (gH)^2 = eH$, so $x \in H$. This proves (4.2) as claimed. By (4.1) and (4.2), we have $G^2 = H$, so G^2 is a subgroup of G. □

Theorem 4.2. *The smallest finite group which does not have the square subgroup property has order 12.*

Proof. Suppose that G is a group, and $|G| < 12$. We consider the following two cases.
Case 1: $|G|$ *is a multiple of 4.*

If $|G| = 4$, then G is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. If $|G| = 8$, then G is isomorphic to one of the following,

$$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_8, Q_8, \tag{4.3}$$

where D_8 is the dihedral group and Q_8 is the quaternion group. Each of the above groups has the square subgroup property.

Case 2: $|G|$ is not a multiple of 4.

In this case by Theorem 1.1 and Proposition 4.1, G has the square subgroup property.

We have shown that if $|G| < 12$, then G has the square subgroup property. On the other hand $|A_4| = 12$, and by Example 3.2, A_4 does not have the square subgroup property. This proves the theorem. □

As an application of our study on square subgroup property, it leads to the following well-known result in finite group theory.

Corollary 4.3. *If G is a non-abelian finite simple group, then $|G|$ is a multiple of 4.*

Proof. Since G is nonabelian, it cannot be cyclic. By Theorem 4.1(a), G does not have the square subgroup property. By Theorem 1.1 and Proposition 3.4, 4 divides $|G|$. □

In view of Theorem 1.1 and Proposition 3.4, it remains to consider groups of order divisible by 4. We focus on such groups for the rest of this section.

Proposition 4.4. *There exists a finite group G of order 16 which does not have the square subgroup property.*

Proof. Let $G = \langle a, b \ ; \ a^4 = b^4 = e, ba = a^{-1}b \rangle$. Here G is a nonabelian group of order 16, and $G \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_4$.

We claim that

$$G^2 = \{e, a^2, b^2\}. \tag{4.4}$$

It is clear that $\{e, a^2, b^2\} \subset G^2$, and it remains to prove the opposite inclusion. From $ba = a^{-1}b$, we have $ba^i = a^{-i}b$ for all $i \in \mathbb{Z}$. By induction,

$$b^j a^i = a^{(-1)^j i} b^j \tag{4.5}$$

for all $i, j \in \mathbb{Z}$. Suppose that $x \in G^2$. Then $x = g^2$ for some $g \in G$. Assume that $g = a^r b^s$ for some $r, s \in \mathbb{Z}$. By (4.5),

$$x = g^2 = (a^r b^s)^2 = a^r b^s a^r b^s = a^r a^{(-1)^s r} b^s b^s = a^{r+(-1)^s r} b^{2s} = \begin{cases} a^{2r} & \text{if } s \text{ is even,} \\ b^{2s} & \text{if } s \text{ is odd.} \end{cases}$$

Hence $x \in \{e, a^2, b^2\}$, which proves (4.4). By (4.4), $|G^2| = 3$, which is not a factor of 16. So G^2 is not a subgroup of G. □

The finite 2-groups form a family of groups whose orders are divisible by 4. The next proposition constructs finite 2-groups that do not have the square subgroup property.

Proposition 4.5. *For any $n \geq 4$, there exists a finite group G of order 2^n such that G^2 is not a subgroup of G.*

Proof. Let $n \geq 4$. Let H be the group of order 16 constructed in Proposition 4.4. Let $G = H \times \mathbb{Z}_{2^{n-4}}$. By Proposition 3.1(b), G^2 is not a subgroup of G. □

We note that Proposition 4.5 fails for $n = 3$. Up to isomorphism, there are exactly five groups of order $2^3 = 8$ (see (4.3)), and they all have the square subgroup property. Therefore, the smallest 2-group which does not have the square subgroup property has order 16.

Let $n \geq 2$. We define the dicyclic group of order $4n$ by

$$\mathrm{Dic}_n = \langle a, x \ ; \ a^{2n} = e, x^2 = a^n, x^{-1}ax = a^{-1} \rangle.$$

Every element of Dic_n is uniquely of the form $a^k x^j$, where $k = 0, 1, ...2n-1$ and $j = 0, 1$.

Theorem 4.6. *Let $n \geq 2$. Then Dic_n has the square subgroup property if and only if n is even.*

Proof. Let $G = \mathrm{Dic}_n$. We first claim that

$$G^2 = \{a^{2m} \ ; \ m = 0, 1, ..., n-1\} \cup \{a^n\}. \tag{4.6}$$

Let $T = \{a^{2m} \ ; \ m = 0, 1, ..., n-1\} \cup \{a^n\}$. Clearly $a^{2m} \in G^2$ for all $m = 0, 1, ..., n-1$. Also, $a^n = x^2 \in G^2$. Hence $T \subset G^2$. Conversely, we consider $g^2 \in G^2$. Write $g = a^k x^j$, where $k = 0, 1, ..., 2n-1$ and $j = 0, 1$. If $j = 0$, then $g^2 = a^{2k} \in T$. If $j = 1$, then $g^2 = a^k x a^k x = a^k a^{-k} x^2 = x^2 = a^n \in T$. Hence $G^2 \subset T$. This proves (4.6) as claimed.

If n is even, then by (4.6), $(\mathrm{Dic}_n)^2 = \langle a^2 \rangle$, so $(\mathrm{Dic}_n)^2$ is a subgroup of Dic_n.

Suppose that n is odd. Let $n = 2k+1$. By (4.6), $a^{2k}, a^n \in (\mathrm{Dic}_n)^2$, but $a^n (a^{2k})^{-1} = a \notin (\mathrm{Dic}_n)^2$. Hence $(\mathrm{Dic}_n)^2$ is not a subgroup of Dic_n. □

Proof of Theorem 1.4:

We want to show that conditions (a) and (b) of Theorem 1.4 are equivalent. We first show that (b) implies (a). Suppose that $n \leq 8$ or 4 does not divide n. If $n \leq 8$, then by Theorem 4.2, every group of order n has the square subgroup property. If 4 does not divide n, then by Theorems 1.1 and 4.1, every group of order n has the square subgroup property.

Next we show that (a) implies (b). Suppose that $n > 8$ and 4 divides n. Then $n = 4k$ for some $k \geq 3$. We want to construct a group G of order $4k$ and does not have the square subgroup property. For $k = 3$, we let $G = A_4$, see Example 3.2. For $k = 4$, we let G be the group constructed in Proposition 4.4. For $k \geq 5$ and odd, we take $G = \mathrm{Dic}_k$ and apply Theorem 4.6. For $k \geq 5$ and even, we write

$$k = 2^t r \ , \ t, r \in \mathbb{N} \text{ and } r \text{ is odd.}$$

If $r = 1$, we let G be the group in Proposition 4.5. If $r > 1$, we let $G = \mathrm{Dic}_r \times \mathbb{Z}_{2^t}$. By Proposition 3.1(b) and Theorem 4.6, $G = \mathrm{Dic}_r \times \mathbb{Z}_{2^t}$ does not have the square subgroup property. This proves Theorem 1.4. □

5. General Linear Groups

In this section, we prove Theorem 1.5. For any square matrix A, we let A_{ij} denote its (i, j)-th entry. We make the convention that empty spots in a matrix denote the entry 0.

Lemma 5.1. *Let A be an $n \times n$ upper-triangular complex matrix with entries 1 along the diagonal, and $A_{ij} = x_{j-i}$ for all $i < j$, namely*

$$A = \begin{pmatrix} x_0 & x_1 & x_2 & \dots & x_{n-2} & x_{n-1} \\ & x_0 & x_1 & \dots & x_{n-3} & x_{n-2} \\ & & x_0 & & \vdots & \vdots \\ & & & \ddots & x_1 & x_2 \\ & & & & x_0 & x_1 \\ & & & & & x_0 \end{pmatrix}. \tag{5.1}$$

Then $(A^2)_{ij} = \begin{cases} \sum_{k=i}^{j} x_{k-i} x_{j-k} & \text{for } i \leq j \\ 0 & \text{for } i > j. \end{cases}$

Proof. For $i > j$, it is clear that $(A^2)_{ij} = 0$. For $i \leq j$, we have $(A^2)_{ij} = \sum_{k=1}^{n} A_{ik} A_{kj} = \sum_{k=i}^{j} x_{k-i} x_{j-k}$. □

Recall that a Jordan block is a square matrix with diagonal entries $\lambda \in \mathbb{C}$, entries 1 above the diagonal, and 0 elsewhere. Let $\mathbb{C}^\times$ denote the multiplicative group consisting of nonzero complex numbers.

Lemma 5.2. *Let $\lambda \in \mathbb{C}^\times$, and consider the $n \times n$ Jordan block*

$$J = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \lambda & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix}.$$

There exists an $n \times n$ complex matrix B such that $B^2 = J$.

Proof. Pick $\alpha \in \mathbb{C}$ such that $\alpha^2 = \lambda$. Then $J = \alpha^2 M$, where

$$M = \begin{pmatrix} 1 & \frac{1}{\lambda} & & & \\ & 1 & \frac{1}{\lambda} & & \\ & & 1 & \ddots & \\ & & & \ddots & \frac{1}{\lambda} \\ & & & & 1 \end{pmatrix}.$$

Let A be the matrix in (5.1). By Lemma 5.1, $A^2 = M$ holds if

$$2x_1 = \frac{1}{\lambda} \text{ and } \sum_{k=0}^{j} x_k x_{j-k} = 0 \text{ for all } j = 2, ..., n-1. \tag{5.2}$$

We note that (5.2) has a unique solution for $x_1, x_2, ..., x_{n-1}$. It starts with $x_1 = \frac{1}{2\lambda}$, then inductively with $x_2 = -\frac{1}{2}x_1^2 = -\frac{1}{8\lambda^2}$, $x_3 = -\frac{1}{2}(x_1x_2 + x_2x_1) = \frac{1}{16\lambda^3}$, and more generally

$$x_j = -\frac{1}{2}\sum_{k=1}^{j-1} x_k x_{j-k} \text{ for all } j = 2, ..., n-1.$$

In this way, $A^2 = M$.

Let $B = \alpha A$. Then $J = \alpha^2 M = \alpha^2 A^2 = B^2$. This proves the lemma. □

Recall that $\mathrm{GL}_n(\mathbb{C})$ is the multiplicative group of all $n \times n$ nonsingular complex matrices. We now show that $(\mathrm{GL}_n(\mathbb{C}))^2 = \mathrm{GL}_n(\mathbb{C})$.

Proof of Theorem 1.5:

Let $X \in \mathrm{GL}_n(\mathbb{C})$. There exists $P \in \mathrm{GL}_n(\mathbb{C})$ such that $J = PXP^{-1}$ is the Jordan form of X, namely

$$J = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_r \end{pmatrix}$$

where each J_i is a Jordan block. By Lemma 5.2, there exist $B_1, ..., B_r$ such that $B_i^2 = J_i$ for all $i = 1, ..., r$. Let

$$B = \begin{pmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_r \end{pmatrix}$$

Clearly $B^2 = J$. Then

$$X = P^{-1}JP = P^{-1}B^2P = (P^{-1}BP)^2 \in (\mathrm{GL}_n(\mathbb{C}))^2.$$

This proves the theorem. □

References

[1] D. S. Dummit and R. M. Foote: *Abstract Algebra, 3rd. edition*, John Wiley & Son, 2004.
[2] M. Haugh and D. MacHale: *The subgroup generated by the squares*, Proc. Royal Irish Acad. A: Math. and Phys. Sci. 97 (1997), 123–129.
[3] J. J. Rotman: *An Introduction to the Theory of Groups, 4th. edition*, Springer-Verlag, 1994.
[4] H. S. Sun: *On groups whose squares form a group*, Bull. Inst. Math. Acad. Sinica 9 (1980), 381–388.

Howen Chuah is a mathematics graduate student at the National Tsing Hua University, Taiwan. He intends to pursue research in mathematics.

Department of Mathematics, National Tsing Hua University, Hsinchu 300, Taiwan.
E-mail address: howen@gapp.nthu.edu.tw