FINITE GROUPS WITH CENTRAL SQUARES

GHEORGHE SILBERBERG

Abstract. The present paper studies the finite groups with the following property: the square of each element in the group is central.

1. Introduction

DEFINITION 1.1. *A group G is called CS-group ("central squares") if $x^2 \in Z(G)$ for every $x \in G$.*

It is obvious that all the abelian groups are CS–gropus, therefore we restrict ourselves to the study of the non–abelian CS–groups.
Is is also obvious that all the subgroups of a CS–group are CS–groups.

The converse is not true in general. However, it may hold in some particular cases, one of them being described by the following statement.

PROPOSITION 1.1. *Let G be a finite non–abelian 2–group whose proper subgroups are abelian. Then G is a CS-group.*

PROOF. If x, y are non–trivial elements of G, then $\langle x^2, y\rangle$ is a proper subgroup of G, which implies that $[x^2, y] = 1$.

The complete description of the groups appearing in Proposition 1.1 was given by Rédei in [3] (see also [2], Aufgabe 22, p. 309):

PROPOSITION 1.2. *The only finite non–abelian 2–groups without proper non–abelian subgroups are*

a) $D_8 = \langle x, y | x^2 = y^2 = [x, y]^2 = [x, y, x] = [x, y, y] = 1\rangle$;

b) $Q_8 = \langle x, y | x^4 = 1, x^2 = y^2 = [x, y]\rangle$;

AMS (1991) subject classification: Primary 20D15

c) $G_{m,n} = \langle x, y | x^{2^m} = y^{2^n} = 1, [x, y] = x^{2^{m-1}} \rangle, m \geq 2, n \geq 1,$ $(m, n) \neq (2, 1)$;

d) $G_{m,n,1} = \langle x, y | x^{2^m} = y^{2^n} = [x, y]^2 = [x, y, x] = [x, y, y] = 1 \rangle,$ $m \geq n \geq 1, (m, n) \neq (1, 1)$.

Actually, in Rédei's classification the dihedral group D_S appears twice: as the group $G_{2,1}$ and also as the group $G_{1,1,1}$. In order to avoid such repetitions, we opted for a slightly modified classification.

In the following sections we will examine the structure of the finite CS–groups. We will see that every group of this type is closely related, in some sense, to the Rédei groups.

Al the groups in discussion will be finite. The notation is standard and follows that of [1] and [2].

2. Preliminary results

First we establish some necessary and/or sufficient conditions for a non–abelian group G to be a CS–group.

PROPOSITION 2.1. *A non–abelian group G is a CS–group iff the quotient $G/Z(G)$ has exponent 2.*

PROOF. The condition "$x^2 \in Z(G)$ for every $x \in G$" is equivalent to "each non–trivial element in $G/Z(G)$ has order 2".

COROLLLARY 2.1. *Every non–abelian CS–group is nilpotent of class 2.*

PROOF. Having exponent 2, the quotient group $G/Z(G)$ is abelian.

PROPOSITION 2.2. *A nonabelian group G is a CS–group iff $G' \subseteq Z(G)$ and* $\exp(G') = 2$.

PROOF. Suppose that G is a CS–group. By Corollary 2.1 we get $G' \subseteq Z(G)$. If $x, y \in G$, then $[x^2, y] = 1$. But $[x, y]^2 = [x^2, y]$ (see [2], Lemma 3.1.3) hence G' has exponent 2.

Conversely, suppose that $G' \subseteq Z(G)$ and $\exp(G') = 2$. If $x, y \in G$, then $[x^2, y] = [x, y]^2 = 1$.

The next result clarifies the structure of a non–abelian CS–group.

THEOREM 2.1. *A non–abelian group G is a CS–group iff its order is even and it can be expressed as a direct product $G = P \times Q$, where P is an abelian group of odd order and Q is a non–abelian CS–2–group.*

PROOF. If G is a CS–group, then G is nilpotent of class 2 and $\exp(G') = 2$. For every prime p dividing the order of G, let S_p be the Sylow p–subgroup of G. Then we have

$$G = \prod_{p\in\pi(G)} S_p \quad \text{and} \quad G' = \prod_{p\in\pi(G)} S'_p,$$

where $\pi(G)$ denotes the set of the prime divisors of $|G|$. It follows that $\exp(S'_p) \in \{1, 2\}$ for every $p \in \pi(G)$. Hence, S_p is abelian for every odd $p \in \pi(G)$ and the order of G is even.
If we put

$$P = \prod_{p\in\pi(G),p\neq 2} S_p \qquad \text{and} \qquad Q = S_2,$$

then $G = P \times Q$. Moreover, Q is a non–abelian CS–group.

Conversely, let $G = P \times Q$ where P is an abelian group of odd order and Q is a non–abelian CS–group. Then

$$P = Z(P), \quad \exp(Q/Z(Q)) = 2 \quad \text{and} \quad \exp(G/Z(G)) = \exp(Q/Z(Q)) = 2.$$

The conclusion folows.

Consequently, our problem is reduced to the study of the non–abelian CS–2–groups.

3. Non–abelian CS–2–groups

We have a very simple necessary and sufficient condition for a non–abelian 2–group to be a CS–group.

PROPOSITION 3.1. *Let G be a non–abelian 2–group. The G is a CS–group iff $\Phi(G) \subseteq Z(G)$, where $\Phi(G)$ denotes the Frattini subgroup of G.*

PROOF. Obvious.

Let G be a non–abelian group of order 2^n. One says that G is d–generated if d is the smallest possible cardinal of a generating set in G. Then $|\Phi(G)| = 2^{n-d}$. If we denote by 2^z the order of $Z(G)$, a necessary condition for G being a CS–group is

$$n - d \leq z \leq n - 2.$$

Hence, the bigger is d, the more "degrees of freedom" has the order of $Z(G)$. The extreme case $d = n - 1$ puts no restrictions on $Z(G)$.

PROPOSITION 3.2. *Every $(n-1)$–generated non–abelian group of order 2^n $(n \geq 3)$ is a CS–group.*

Proof. Let G be a $(n-1)$–generated non–abelian group of order 2^n. Then $|\Phi(G)| = 2$. Becouse $\Phi(G) \triangleleft G$, it follows that $\Phi(G) \subseteq Z(G)$ and so G is a CS–group.

The other extreme case, $d = 2$, restricts considerably the order and the structure of $Z(G)$. Therefore we can easily describe all the CS–2–groups with this property.

Proposition 3.3. *Let G be a 2–generated non–abelian 2–group. Then G is a CS–group iff every proper subgroup of G is abelian.*

Proof. If G is a 2–generated CS–2–group, then $|G : \Phi(G)| = 4$ and, by Proposition 3.1, $Z(G) = \Phi(G)$.

Let H be a proper subgroup of G. There exists a maximal subgroup M if G such that $H \subseteq M$. From $M \supset \Phi(G) = Z(G)$ and $|M : Z(G)| = 2$ we get $|M : Z(M)| \leq 2$, hence M is abelian and so is H.

Conversely, if x is an element of G and M is a maximal subgroup of G containing x, then M is abelian and therefore $\Phi(G) \subseteq M \subseteq C_G(x)$. It results

$$\Phi(G) \subseteq \bigcap_{x \in G} C_G(x) = Z(G).$$

Corollary 3.1. *The only non–abelian 2–generated CS–2–groups are the Rédei groups described in Proposition 1.2.*

Corollary 3.2. *A non–abelian 2–group G is a CS–group iff every 2–generated subgroup of G is abelian or is a Rédei group.*

Proof. The statement follows from the remark that G is a CS–2–group iff every 2–generated subgroup of G is a CS–group.

The characterization of the non–abelian CS–2–groups offered by Corollary 3.2 is diffecult to use. However, it seems obvious that the structure of a non–abelian CS–2–group must be "close" to the structure of a Rédei group. This statement will be made clearer in the next section, where we will investigate the 3–generated CS–2–groups.

4. Non–abelian 3–generated CS–2–groups

Suppose G is a non–abelian 2–group.

Definition 4.1. *A pair of elements (x, y) in G is called minimal non–commutative pair if $[x, y] \neq 1$ and*

$$|x| + |y| = \min_{z,t \in G, [z,t] \neq 1} \{|z| + |t|\}.$$

DEFINITION 4.2. *An element x in G is called rational if every conjugate of x in G is a power of x.*

DEFINITION 4.3. *The group G is called*
- *rational if it contains a minimal non-commutative pair of rational elements;*
- *non-rational if each minimal non-commutative pair in G contains only non-rational elements;*
- *semi-rational in all other cases.*

When the center of G has index 4, one can provide an alternative definition of the rational elements.

PROPOSITION 4.1. *Let G be a non-abelian 2-group such that $|G : Z(G)| = 4$. Then*
a) *$|G'| = 2$ and $G' \subseteq Z(G)$.*
b) *A non-central element $x \in G$ is rational if and only if $\langle x \rangle \supseteq G'$.*
c) *Every non-central element of order 2 in G is non-rational.*

PROOF. The first part follows from a well-known result of Wiegold (see [4]).

Statement b) is straightforward if we observe that $x^G = x \cdot G'$, where x^G denotes the conjugacy class of x in G.

c) Let x be a non-central rational element of order 2 in G. Then $\langle x \rangle \supseteq G'$ becomes an equality, which leads to the contradiction $x \in Z(G)$.

Let us classify all the Rédei 2-groups according to their "degree of rationality".

PROPOSITION 4.2. a) *D_8 is non-rational.*
b) *Q_8 is the only rational Rédei group.*
c) *$G_{m,n}$ is semi-rational for every $m \geq 2, n \geq 1, (m,n) \neq (2,1)$.*
d) *$G_{m,n,1}$ is non-rational for every $m \geq n \geq 1, (m,n) \neq (1,1)$.*

PROOF. a) Every minimal non-commutative pair in D_8 contains only elements of order 2, which are non-rational.

b) Each non-central element in Q_8 is rational, hence Q_8 itself is rational. Conversely, suppose that G is a rational Rédei 2-group and let (x, y) be a minimal non-commutative pair in G, both x and y being rational. Denote by 2^m the order of x and by 2^n the order of y. Then by Proposition 4.1, we have that $x^{2^{m-1}} = y^{2^{n-1}} = [x, y]$ is the only element of order 2 in G. Therefore G is either cyclic, or equternionic, the only possibility in our case being $G \cong Q_8$.

c) Let $m \geq 2, n \geq 1, (m,n) \neq (2,1)$,

$$G = \langle x, y | x^{2^m} = y^{2^n} = 1, [x, y] = x^{2^{m-1}} \rangle.$$

Then (x,y) is a minimal non–commutative pair, x is rational and y is non–rational. By b), it follows that G is a semi–rational group.

d) Let $m \geq n \geq 1, (m,n) \neq (1,1)$,

$$G = \langle x, y | x^{2^m} = y^{2^n} = [x,y]^2 = [x,y,x] = [x,y,y] = 1 \rangle.$$

One can check easily that $[x,y]$ cannot be a square in G. Therefore all the non–central elements of G are non–rational.

We can now tackle the case of the non–abelian 3–generated CS–2–groups. Let G be such a group. Then $|G : \Phi(G)| = 8$ and, by Proposition 3.1, $\Phi(G) \subseteq Z(G)$. There are two possibilities:

- $|Z(G) : \Phi(G)| = 2$;
- $Z(G) = \Phi(G)$.

We will study exhaustively only the first case, which implies $|G : Z(G)| = 4$.

THEOREM 4.1. *Let G be a non–abelian 3–generated CS–2–group such that $Z(G) \neq \Phi(G)$.*

a) *If G is rational, then $G \cong H \times K$, where H is a rational Rédei 2–group and K is a non–trivial cyclic 2–group.*

b) *If G is semi–rational, then $G \cong H \times K$, where H is a semi–rational Rédei 2–group and K is a non–trivial cyclic 2–group.*

c) *If G is non–rational, then G is isomorhic either to $H \times K$, or to $H \curlyvee K$, where H is a non–rational Rédei 2–group and K is a non–trivial cyclic 2–group. In the last case, the order of K is at least 4 and $H \curlyvee K$ denotes the central product of H and K where H' is identified with the unique subgroup of order 2 in K.*

PROOF. Let (x,y) be a minimal non–commutative pair in G and let z be an element of minimal order in $Z(G) \setminus \Phi(G)$. Denote by $2^m, 2^n, 2^p$ respectively the orders of x, y, z by H the subgroup generated in G by x and y, and by K the subgroup generated in G by z. Then H and K are normal subgroups of G, becouse H contains G' and K is contained in $Z(G)$. Moreover, H is a Rédei 2–group and

$$G = \langle x, y, Z(G) \rangle - \langle x, y, z, \Phi(G) \rangle = \langle x, y, z \rangle = H \cdot K.$$

a) We may assume that x and y are rational. Then H is a rational group and $x^{2^{m-1}} = y^{2^{n-1}} = [x,y]$ is the only element of order 2 in $Z(H)$.

Suppose $H \cap K \neq 1$. Then necessarily $z^{2^{p-1}} = x^{2^{m-1}}$. If $m > p$, then $x^{2^{m-p}} \cdot z$ would be an be an element of order less that 2^p in $Z(G) \setminus \Phi(G)$. If $m \leq p$, then $(x \cdot z^{2^{p-m}}, y)$ would be a non–commutative pair in G with $|x \cdot z^{2^{p-m}}| + |y| < 2^m + 2^n$. Either way we get a contradiction. Therefore $H \cap K = 1$ and hence $G \cong H \times K$.

b) We may assume that x is rational and y is non–rational. Then H is a semi–rational group and $x^{2^{m-1}} = [x,y] \neq y^{2^{n-1}}$.

Suppose $H \cap K \neq 1$. Then $z^{2^{p-1}}$ must coincide with an element of order 2 in $Z(H)$, these elements being $x^{2^{m-1}} = [x,y], y^{2^{n-1}}, x^{2^{m-1}} \cdot y^{2^{n-1}}$ (or only $x^{2^{m-1}}$ if $n = 1$).
The equalities $z^{2^{p-1}} = x^{2^{m-1}}, z^{2^{p-1}} = y^{2^{n-1}}$ can be excluded as in the previous case.
If $m > n$, then $x^{2^{m-1}} \cdot y^{2^{n-1}} = (x^{2^{m-n}} \cdot y)^{2^{n-1}}$ and $(x, x^{2^{m-1}} \cdot y)$ is a minimal non–commutative pair.
If $m < n$, then $x^{2^{m-1}} \cdot y^{2^{n-1}} = (x \cdot y^{2^{m-n}})^{2^{m-1}}$ and $(x \cdot y^{2^{n-m}}, y)$ is a minimal non–commutative pair.
If $m = n \geq 3$, then $x^{2^{m-1}} \cdot y^{2^{n-1}} = (x \cdot y)^{2^{m-1}}$ and $(x, x \cdot y)$ is a minimal non–commutative pair. All the last three cases are leading to contradictions.
Finally, if $m = n = 2$ the equality $z^{2^{p-1}} = x^2 \cdot y^2$ implies $(x \cdot y \cdot z^{2^{p-2}})^2 = [x,y]$, hence $(x, x \cdot y \cdot z^{2^{p-2}})$ is a minimal non–commutative pair in G containing two rational elements, in contradiction with the hypothesis.

Consequently, $H \cap K = 1$ and $G \cong H \times K$.

c) H, x and y are non–rational and the only elements of order 2 in $Z(H)$ are $x^{2^{m-1}}, y^{2^{n-1}}, x^{2^{m-1}} \cdot y^{2^{n-1}}, [x,y], x^{2^{m-1}} \cdot [x,y], y^{2^{n-1}} \cdot [x,y], x^{2^{m-1}} \cdot y^{2^{n-1}} \cdot [x,y]$ (or less elements).
Suppose first that $H \cap K = 1$. Then $G \cong H \times K$.
Suppose that $H \cap K \neq 1$. Then $z^{2^{p-1}}$ must coincide with one of the elements above. We know already that $z^{2^{p-1}}$ cannot coincide with either of the first three elements in the list.

If $z^{2^{p-1}} = [x,y]$, then $H \cap K \supseteq H'$. The inclusion cannot be strict, because it would follow that $[x,y]$ would be a square in the non–rational Rédei 2–group H and this is not possible according to the proof of Proposition 4.2 d). It results that $H \cap K = H'$ and then $G \cong HYK$.

Assume $z^{2^{p-1}} = x^{2^{m-1}} \cdot [x,y]$. If $m \leq p$, then $(x \cdot z^{2^{p-m}}, y)$ is a minimal non–commutative pair in G and $x \cdot z^{2^{p-m}}$ is rational, a contradiction. If $m > p$, then we can replace z by $z' = x^{2^{m-p}} \cdot z$ and we will arrive to the already discussed case $(z')^{2^{p-1}} = [x,y]$.

The same argument applies if $z^{2^{p-1}} = y^{2^{n-1}} \cdot [x,y]$ or if $z^{2^{p-1}} = x^{2^{m-1}} \cdot y^{2^{n-1}} \cdot [x,y]$ and $x^{2^{m-1}} \cdot y^{2^{n-1}}$ is a power of a component of a minimal non–commutative pair. The proof of b) shows that the letter is actually the case if $m \neq n$ or if $m = n \geq 3$. It remains only $m = n = 2$ and $z^{2^{p-1}} = x^2 \cdot y^2 \cdot [x,y]$, but then $(x, x \cdot y \cdot z^{2^{p-2}})$ is a non–commutative pair with $|x| + |x \cdot y \cdot z^{2^{p-2}}| = 4 + 2 < |x| + |y|$, which contradicts the hypothesis.

In conclusion, the assumption $H \cap K \neq 1$ leads to $H \cap K = H'$ and to $G \cong HYK$.

A complete list of the non–abelian 3–generated CS–2–groups G with $Z(G) \neq \Phi(G)$ can be presented.

THEOREM 4.2. *Let G be a non–abelian 3–generated CS–2–group such that $Z(G) \neq \Phi(G)$. Then G is isomorphic to one of the following groups:*

a) $Q_8 \times \mathbf{Z}_{2^p}$ $(p \geq 1)$ *if G is rational;*

b) $G_{m,n} \times \mathbf{Z}_{2^p}$ $(m \geq 2, n, p \geq 1, (m,n) \neq (2,1))$ *if G is semi–rational;*

c) $D_8 \times \mathbf{Z}_{2^p}$ $(p \geq 1)$ *or*
$D_8 Y \mathbf{Z}_{2^p}$ $(p \geq 2)$ *or*
$G_{m,n,1} \times \mathbf{Z}_{2^p}$ $(m \geq n \geq 1, (m,n) \neq (1,1), p \geq 1)$ *or*
$G_{m,n,1} Y \mathbf{Z}_{2^p}$ $(m \geq n \geq 1, (m,n) \neq (1,1), p \geq 2)$
if G is non–rational.

PROOF. All the statements are following from Theorem 4.1 and Proposition 4.2.

We may wonder why are not appearing in this list the groups of the type $Q_8 Y \mathbf{Z}_{2^p}$ and $G_{m,n} Y \mathbf{Z}_{2^p}$. The explanation is the following: they actually appear, but they are isomorphic to other groups in the list. More precisely, for every $p \geq 2$ we have

$$Q_8 Y \mathbf{Z}_{2^p} \cong D_S Y \mathbf{Z}_{2^p}$$

$$G_{m,n} Y \mathbf{Z}_{2^p} \cong \begin{cases} G_{m-1,n,1} Y \mathbf{Z}_{2^p} & \text{if} \quad n < m \leq p \\ G_{n,m-1,1} Y \mathbf{Z}_{2^p} & \text{if} \quad m \leq n, m \leq p \\ G_{m,n} Y \mathbf{Z}_{2^{p-1}} & \text{if} \quad m > p \end{cases} .$$

On the other hand, the groups in Theorem 4.2 are pairwise non–isomorphic.

REFERENCES

[1] Gorenstein, *Finite groups*, Harper and Row, New York–Evanston–London 1968.

[2] Huppert, *Endliche Gruppen I*, Springer–Verlag, Berlin–Heidelberg–New York 1967.

[3] Rédei, *Das schiefe Produkt in der Gruppentheorie*, Commenta. Math. Helvetici **20**(1947), 225–267.

[4] Wiegold, *Multiplicators and groups with finite central factor–groups*, Mathematische Zeitschrift **89**(1965), 345–347.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TIMIŞOARA
BD. V. PÂRVAN NR. 4
1900 TIMIŞOARA
ROMANIA

e-mail: c98sig01@student.ceu.hu