# SET-DIRECT FACTORIZATIONS OF GROUPS

DAN LEVY AND ATTILA MARÓTI

Abstract. We consider factorizations $G = XY$ where $G$ is a general group, $X$ and $Y$ are normal subsets of $G$ and any $g \in G$ has a unique representation $g = xy$ with $x \in X$ and $y \in Y$. This definition coincides with the customary and extensively studied definition of a direct product decomposition by subsets of a finite abelian group. Our main result states that a group $G$ has such a factorization if and only if $G$ is a central product of $\langle X\rangle$ and $\langle Y\rangle$ and the central subgroup $\langle X\rangle \cap \langle Y\rangle$ satisfies certain abelian factorization conditions. We analyze some special cases and give examples. In particular, simple groups have no non-trivial set-direct factorization.

## 1. Introduction

Factorizations of groups is an important topic in group theory that has many facets. The most basic and best studied type of factorization is the direct product factorization of a group into two normal subgroups. If $G$ is a group and $H$ and $K$ are two normal subgroups of $G$ then $G = H \times K$ if and only if each $g \in G$ has a unique representation $g = hk$ with $h \in H$ and $k \in K$. One possibility to generalize this definition is to relax the condition that both $H$ and $K$ are normal. This leads to the well-known concept of a semi-direct product of subgroups (only one of the factors is assumed to be normal) and also to the consideration of factorizations $G = HK$ where neither of the two subgroups $H$ and $K$ is normal, and even the unique representation condition is not necessarily assumed. To get a glimpse of the possibilities see the seminal classification result in [11] of maximal decompositions $G = HK$ where $G$ is a finite simple group and $H$ and $K$ are two maximal subgroups of $G$.

Another generalization arose from a geometry problem of Minkowski [13]. In 1938 Hajós [7] reformulated this problem as an equivalent factorization problem of a finite abelian group, where the factors need not be subgroups. More precisely, if $G$ is an abelian group written additively then a (set) factorization of $G$ is a representation of $G$ in the form $G = H + K$ where $H$ and $K$ are subsets of $G$ and for each $g \in G$ there is a unique pair $h \in H$ and $k \in K$ such that $g = h + k$. Four years later, Hajós [8] solved Minkowski's problem by solving the equivalent group factorization problem. This initiated the investigation of set factorizations

*Date*: September 30, 2018.

2000 *Mathematics Subject Classification.* 20K25, 20D40.

*Key words and phrases.* direct factorizations of groups, central products.

A.M. was supported by the National Research, Development and Innovation Office (NKFIH) Grant No. K115799 and Grant No. ERC_HU_15 118286, and by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences. The work of A.M. on the project leading to this application has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 741420). He also received funding from ERC 648017.

of abelian groups. The interested reader is referred to the book [14] by Szabó and Sands for a comprehensive account of problems, techniques, results and applications of this field.

In the present paper we consider set factorizations of a general group. For abelian groups our definition coincides with the one described above. Some specialized results which apply to our definition appeared in [9]. Another related concept which is studied in the literature, is the concept of a logarithmic signature. This concept found use in the search for new cryptographic algorithms which are based on finite non-abelian groups, and this application motivates the bulk of the available results. A logarithmic signature of a group $G$ is a sequence $[\alpha_1, ..., \alpha_s]$ of ordered subsets $\alpha_i \subseteq G$ (not necessarily normal) such that each $g \in G$ has a unique representation $g = g_1 \cdots g_s$ with $g_i \in \alpha_i$ for all $1 \leq i \leq s$. The first proposal for a cryptosystem which is based on logarithmic signatures can be found in [12]. Results on short logarithmic signatures can be found in [10].

**Definition 1.1.** *Let $G$ be a group, and let $X$ and $Y$ be two non-empty subsets of $G$. We shall say that the setwise product $XY$ is direct, and denote this fact by writing $X \times Y$ for the set $XY$, if both $X$ and $Y$ are normal in $G$, and if every $g \in XY$ has a unique representation $g = xy$ with $x \in X$ and $y \in Y$.*

We shall say that the group $G$ has a *set-direct factorization* (*decomposition*) or is a *set-direct product*, if $G = X \times Y$ for some $X, Y \subseteq G$. A set-direct factorization of $G$ will be called non-trivial, if and only if none of $X$ or $Y$ is a singleton consisting of a central element (whereby the second factor must be $G$). Furthermore, following [14, p.5], we shall say that a subset $X$ of a group $G$ is *normalized* if $1_G \in X$, and that the set-direct factorization $G = X \times Y$ is *normalized* if both $X$ and $Y$ are normalized. We shall show (Remark 2.10) that $Z(G) \times Z(G)$ acts on the set of all direct factorizations of $G$ and that each orbit of this action contains at least one normalized factorization.

Our main result is a necessary and sufficient condition for a group $G$ and an unordered pair $X, Y$ of normal subsets of $G$ to satisfy $G = X \times Y$. This condition involves a certain central subgroup $Z$ of $G$, and a family of set-direct factorizations of $Z$. Recall (see Section 2.2) that a group $G$ is a central product of two subgroups $M$ and $N$ if $G = MN$, and $M$ and $N$ centralize each other. In this case $M$ and $N$ are normal in $G$ and $Z := M \cap N$ is central in $G$. We write $G = M \circ_Z N$.

**Theorem 1.2.** *Let $G$ be a group and let $X, Y$ be normal subsets of $G$. Set $M = \langle X \rangle$, $N = \langle Y \rangle$, $Z := M \cap N$. For every $m \in M$ set $X_m := \left(m^{-1}X\right) \cap Z$ and for every $n \in N$ set $Y_n := \left(n^{-1}Y\right) \cap Z$. Then $G = X \times Y$ if and only if the following two conditions are met.*

(a) *$G = M \circ_Z N$.*
(b) *$Z = X_m \times Y_n$ for every $m \in M$ and $n \in N$.*

**Corollary 1.3.** *Simple groups have no non-trivial set-direct factorization.*

Condition (b) of Theorem 1.2 specifies a family of set-direct factorizations of $Z$, and the next definition characterizes the families of set-direct factorizations of $Z$ that arise in this way. Recall that if $H$ is an abelian group, and $S \subseteq H$ then the kernel of $S$ in $H$ is defined by $K_H(S) := \{h \in H | hS = S\}$ (we also write $K(S)$ if $H$ is clear from the context). One can easily check that $K_H(S)$ is a subgroup of $H$.

**Definition 1.4.** *Let $Z$ be an abelian group and let $\mathcal{M} = \{M_i\}_{i\in I}$ and $\mathcal{N} = \{N_j\}_{j\in J}$ be two multisets (i.e., repetitions allowed) of subgroups of $Z$. An $\mathcal{MN}$-direct factorization system of $Z$ is a pair of multisets $\mathcal{A} = \{A_i\}_{i\in I}$ and $\mathcal{B} = \{B_j\}_{j\in J}$ of subsets of $Z$ which satisfy for all $i \in I$ and $j \in J$*

$$Z = A_i \times B_j,\ M_i \leq K_Z(A_i),\ N_j \leq K_Z(B_j).$$

To make the connection between Condition (b) of Theorem 1.2 and Definition 1.4, we need the following fact (see Section 2.1, Lemma 2.1). Let $G$ be a group, $N \trianglelefteq G$, and $Z \leq N$ a central subgroup of $G$. Then $Z$ acts by multiplication on the set $\Omega_N$ of all conjugacy classes of $G$ contained in $N$.

**Theorem 1.5.** *Let $G$ be a group and let $X, Y$ be normal subsets of $G$. Set $M = \langle X\rangle$, $N = \langle Y\rangle$, $Z := M \cap N$, and assume that $G = M \circ_Z N$. For each $m \in M$ and $n \in N$ let $M_m$ and $N_n$ be, respectively, the stabilizers of the conjugacy classes of $m$ and $n$ with respect to the multiplication action of $Z$. Set $\mathcal{M} = \{M_m\}_{m\in M}$ and $\mathcal{N} = \{N_n\}_{n\in N}$. Then $G = X \times Y$ if and only if the pair of multisets $\left(\{X_m\}_{m\in M}, \{Y_n\}_{n\in N}\right)$ is an $\mathcal{MN}$-direct factorization system of $Z$, where for every $m \in M$ and for every $n \in N$, we set $X_m := \left(m^{-1}X\right) \cap Z$ and $Y_n := \left(n^{-1}Y\right) \cap Z$.*

The next theorem shows that starting from a central product $G = M \circ_Z N$ and an appropriate set-direct factorization system of $Z$, one can obtain a set-direct decomposition of $G$. We denote by $O(\Omega_M)$ and $O(\Omega_N)$ the set of all *orbits* of the multiplication action of $Z$ on $\Omega_M$ and $\Omega_N$ respectively. Note (Lemma 2.1 part 3) that the stabilizer of an orbit is the stabilizer of any conjugacy class belonging to the orbit.

**Theorem 1.6.** *Let $G = M \circ_Z N$. Set $I := O(\Omega_M)$ and $J := O(\Omega_N)$. For each $i \in I$ and $j \in J$ let $M_i$ and $N_j$ be the stabilizers of the orbits $i$ and $j$. Set $\mathcal{M} := \{M_i\}_{i\in I}$ and $\mathcal{N} := \{N_j\}_{j\in J}$. Assume that $\mathcal{A} := \{A_i\}_{i\in I}$ and $\mathcal{B} := \{B_j\}_{j\in J}$ is an $\mathcal{MN}$-direct factorization system of $Z$. For each $i \in I$ and $j \in J$ fix conjugacy classes $C_i$ and $D_j$ belonging to the orbits $i$ and $j$ respectively. Then $G = X \times Y$ is a set-direct decomposition of $G$, where*

$$X := \bigcup_{i\in I} A_iC_i \text{ and } Y := \bigcup_{j\in J} B_jD_j.$$

Thus, the set-direct factorizations of a general group $G$ can be obtained, in principle, from the knowledge of the central subgroups of $G$, the central product decompositions of $G$ in which they are involved (each central $Z \leq G$ is involved in at least one such decomposition - $G = G \circ_Z Z$), the stabilizers of their multiplication action on the set of conjugacy classes of $G$ contained in the factors of the central products, and the associated factorization systems.

Now we consider two special cases of this general observation. The first case is when one of the factors is a group (and then the second factor is a normal transversal for this group). We shall say, given a group $G$, that $z \in Z(G)$ is *semi-regular* if $zC \neq C$ for every conjugacy class $C$ of $G$. In the following $k(G)$ denotes the number of conjugacy classes of $G$.

**Theorem 1.7.** *Let $G$ be a group and let $X$ and $Y$ be normal subsets of $G$. Suppose that $X$ is a group. Set $N := \langle Y\rangle$ and $Z := X \cap N$, and for each $n \in N$ set $Y_n := \left(n^{-1}Y\right) \cap Z$. Then the following two conditions are equivalent:*

(1) $G = X \times Y$.

(2) *$G = X \circ_Z N$ and $|Y_n| = 1$ for all $n \in N$.*

*Furthermore, if either of (1) or (2) holds, $Y$ is a normal transversal of $Z$ in $N$ and $Z$ acts semi-regularly on $\Omega_N$. If $N$ is finite then $k(N) = k(Z)\,k(N/Z)$.*

**Corollary 1.8.** *Let $G := M \circ_Z N$ and suppose that $Z$ has a normal transversal $Y$ in $N$. Then $G = M \times Y$. In particular, if $N$ is an abelian group, and $Y$ is any transversal of $Z$ in $N$, then $G = M \times Y$.*

Here we prove Corollary 1.8 by showing directly how the conditions of Definition 1.1 are fulfilled. In Section 3 we give a second proof of Corollary 1.8 which relies on its connection with Theorem 1.7.

*Proof of Corollary 1.8.* Since $G = MN$, $N = ZY$ and $Z \leq M$ we get $G = MZY = MY$. If $m_1 y_1 = m_2 y_2$ for $m_1, m_2 \in M$ and $y_1, y_2 \in Y$ then $y_1 y_2^{-1} \in M$ whereby $y_1 y_2^{-1} \in M \cap N = Z$ and hence $y_1 = y_2$ and $m_1 = m_2$. This proves the unique factorization property required in Definition 1.1, and hence $G = M \times Y$. ▮

In the second special case we consider, a single set-direct factorization of an abelian group $Z$ induces a set-direct factorization of $G = M \circ_Z N$. Our non-standard commutator notation is explained in the first paragraph of Section 2.

**Theorem 1.9.** *Let $G = M \circ_Z N$ be a group, and $Z = X_0 \times Y_0$ a set-direct decomposition of $Z$. Assume that $[M, M] \cap Z \subseteq K_Z(X_0)$ and $[N, N] \cap Z \subseteq K_Z(Y_0)$. Then $G$ has a set-direct factorization $G = X \times Y$ with $X \subseteq M$, $Y \subseteq N$, $X \cap Z = X_0$ and $Y \cap Z = Y_0$.*

**Corollary 1.10.** *Let $G$ be a group with a non-trivial central element $z$ of prime power order which is not a prime. Suppose that $z$ is semi-regular. Then $G$ has a non-trivial set-direct factorization. Furthermore, if $G$ is also perfect, then $G$ has a non-trivial normalized (see Remark 2.10) set-direct factorization such that none of the factors is a group.*

Concrete examples of non-trivial set-direct factorizations of the type described by Corollary 1.10, where $G$ is a non-abelian finite quasi-simple group, are provided by the following theorem whose proof rests on the work of Blau in [3].

**Theorem 1.11.** *Let $G$ be a finite quasi-simple group. Then $G$ has a non-trivial normalized set-direct decomposition if and only if $G/Z(G) \cong PSL(3,4)$ and $8$ divides $|Z(G)|$. Moreover, $G$ has a non-trivial normalized set-direct decomposition such that none of the two factors is a group if and only if $G/Z(G) \cong PSL(3,4)$ and $16$ divides $|Z(G)|$.*

## 2. Notation and Background Results

Let $G$ be any group. For $x \in G$ we denote the conjugacy class of $x$ in $G$ by $x^G$. For any normal subset $S$ of $G$ let $\Omega_S$ denote the set of all conjugacy classes of $G$ contained in $S$. We set $k(G) := |\Omega_G|$ in the case that $G$ is finite. For any two subsets $A$ and $B$ of $G$, we denote by $[A, B]$ the set of all commutators $[a, b] := a^{-1}b^{-1}ab$ where $a$ and $b$ vary over all elements of $A$ and $B$ respectively. Note that for subgroups $A$ and $B$ our notation differs from the common practice to denote by $[A, B]$ the subgroup generated by all $[a, b]$ with $a \in A$ and $b \in B$. If $A = \{a\}$ we may write $[a, B]$ for $[\{a\}, B]$ and similarly $[A, b] := [A, \{b\}]$.

2.1. **The action of a central subgroup on conjugacy classes.** In this subsection we summarize basic properties of the multiplication action of a central subgroup $Z \leq G$ on the conjugacy classes of $G$.

**Lemma 2.1.** *Let $G$ be a group, $N \trianglelefteq G$, and $Z \leq N$ a central subgroup of $G$.*

(1) $Z$ acts by multiplication on $\Omega_N$, namely, for any $z \in Z$ and $D \in \Omega_N$ we have $zD = Dz \in \Omega_N$. Denote this action by $\alpha$.
(2) For any $D \in \Omega_N$ denote by $Z_D \leq Z$ the stabilizer of $D$ with respect to $\alpha$. Then $z \in Z_D$ if and only if there exists some $d \in D$ such that $dz \in D$.
(3) For any $D \in \Omega_N$ denote by $O_D$ the orbit of $D$ under $\alpha$. Then for any $D_1, D_2 \in O_D$ we have $Z_{D_1} = Z_{D_2}$.
(4) Let $n \in N$ and let $D = n^G$. Then $Z_D = [n, G] \cap Z$.
(5) Let $Y$ be a normal subset of $G$ contained in $N$. Let $n \in N$ and let $D = n^G$. Set $Y_n := n^{-1}Y \cap Z$. If $Y_n$ is non-empty then $Z_D \leq K(Y_n)$ (equivalently, $Y_n$ is a union of cosets of $Z_D$ in $Z$).
(6) Suppose that $G$ is a finite group. Then $k(G/Z)$ is equal to the number of orbits of the multiplication action of $Z$ on $\Omega_G$. It follows that $Z$ acts semi-regularly on $\Omega_G$ if and only if $k(G) = k(Z)\, k(G/Z)$.

*Proof.* (1) Note that $N$ is the union of all elements of $\Omega_N$ and hence $\Omega_N \neq \emptyset$. Let $D \in \Omega_N$ and $z \in Z$. Since $Z \leq N$ we have $Dz \subseteq N$. We have to show that $Dz$ is also a conjugacy class of $G$. Let $y \in Dz$ and $g \in G$. Then there exists $d \in D$ such that $y = dz$. Using the fact that $Z$ is central, we have

$$y^g = (dz)^g = d^g z \in Dz.$$

Thus, $Dz$ is a normal subset of $G$. Now suppose that $d_1, d_2 \in D$. Then there exists $g \in G$ such that $d_2 = d_1^g$, and hence $d_2 z = (d_1 z)^g$. Thus, any two elements in $Dz$ are conjugate in $G$. This completes the proof that $Dz$ is also a conjugacy class of $G$.

(2) One direction is trivial. In the other direction let $d \in D$ be such that $dz \in D$. Then $D \cap Dz \neq \emptyset$ and since both sets are conjugacy classes this forces $Dz = D$.

(3) Since $Z$ acts transitively on $O_D$, the stabilizers $Z_{D_1}$ and $Z_{D_2}$ are conjugate in $Z$, and since $Z$ is abelian, this implies $Z_{D_1} = Z_{D_2}$.

(4) Let $z \in Z_D \leq Z$. Then $nz \in D$. This implies that there exists $x \in G$ such that $nz = x^{-1}nx$. Hence $z = n^{-1}x^{-1}nx = [n, x] \in [n, G]$. Therefore $z \in [n, G] \cap Z$. Conversely, let $z \in [n, G] \cap Z$. Then there exists $x \in G$ such that $z = [n, x] = n^{-1}x^{-1}nx$. It follows that $nz = x^{-1}nx \in D$. By part 2, this implies $z \in Z_D$.

(5) We have to show $Y_n Z_D = Y_n$. Let $\widetilde{Y}_n := nY_n = Y \cap nZ$. Set $U := Y \cap DZ$. Then, since $nZ \subseteq DZ$ we have $\widetilde{Y}_n = U \cap nZ$. On the other hand, since $Y$ is normal in $G$, we get that $U$ is a union of classes in $O_D$, and hence, by part 3, $UZ_D = U$. This together with $(nZ)\, Z_D = nZ$ implies $\widetilde{Y}_n Z_D = \widetilde{Y}_n$. Finally, this implies $Y_n Z_D = n^{-1}\widetilde{Y}_n Z_D = n^{-1}\widetilde{Y}_n = Y_n$.

(6) We first prove that $k(G/Z)$ is equal to the number of orbits of the multiplication action of $Z$ on $\Omega_G$. Let $D \in \Omega_G$. It is easy to check that the set $DZ$, viewed as a set of cosets of $Z$ in $G$ is a conjugacy class of $G/Z$. By part 1, $DZ$ can also be viewed as a disjoint union of conjugacy classes of $G$ which form one orbit under the multiplication action of $Z$. Hence if $\widetilde{D} \in \Omega_G$ then

either $\widetilde{D} \subseteq DZ$ or $\widetilde{D}Z$ is a distinct conjugacy class of $G/Z$. Moreover, every conjugacy class of $G/Z$ is of the form $DZ$ for some $D \in \Omega_G$. Therefore, $k(G/Z)$ is equal to the number of orbits of the multiplication action of $Z$ on $\Omega_G$. Now, the length of each orbit is at most $|Z|$, and $k(G)$ equals the sum of the lengths of all of the $Z$-orbits. Since the action of $Z$ is semi-regular if and only if all of the lengths equal $|Z| = k(Z)$, we get that the action is semi-regular if and only if $k(G) = k(Z)\,k(G/Z)$.

∎

**Remark 2.2.** *We make two notational remarks in relation to Lemma 2.1.*

1. *Let $G$ be a group and let $X$ be a set of conjugacy classes of $G$. In some discussions (e.g., $X$ is an orbit of $Z$) it is convenient to abuse notation and let $X$ stand also for the normal $G$-subset $\bigcup_{C \in X} C$. Conversely, if $X$ is a normal subset of $G$ we may use the same letter $X$ to denote the set of all conjugacy classes of $G$ which are contained in $X$. We trust the reader to figure out the correct interpretation from the context.*
2. *In view of the third claim of Lemma 2.1, we also write $Z_{O_C}$ instead of $Z_C$.*

2.2. **Central products and their conjugacy classes.** The following theorem is at the basis of the construction of central products of groups.

**Theorem 2.3** ([6], Theorem 2.5.3)**.** *Let $M, N, Z$ be groups with $Z \leq Z(M)$, and suppose that there is an isomorphism $\theta$ of $Z$ into $Z(N)$. Then, if we identify $Z$ with its image $\theta(Z)$, there exists a group $G$ of the form $G = MN$, with $Z = M \cap N \leq Z(G)$ such that $M$ centralizes $N$.*

Any group $G$ with $M, N, Z$ as in the theorem is said to be the central product of $M$ and $N$ (with respect to $Z$), and we will write $G = M \circ_Z N$.

Next we consider the structure of the conjugacy classes of a central product $G = M \circ_Z N$, and the multiplication action of $Z$ on them (see Section 2.1).

**Lemma 2.4.** *Let $G$ be a group and $M$ and $N$ normal subgroups of $G$, such that $G = M \circ_Z N$, where $Z := M \cap N$. Let $C$ be a conjugacy class of $G$. Then:*

1. *There exist a conjugacy class $C_M$ of $M$ and a conjugacy class $C_N$ of $N$ such that $C = C_M C_N$.*
2. *Let $\left\{\left(C_M^{(i)}, C_N^{(i)}\right)\right\}_{i \in I}$ be the set of all the distinct pairs of conjugacy classes $C_M^{(i)} \in \Omega_M$ and $C_N^{(i)} \in \Omega_N$ such that $C = C_M^{(i)} C_N^{(i)}$ for all $i \in I$. Then each one of $O_M := \left\{C_M^{(i)}\right\}_{i \in I}$ and $O_N := \left\{C_N^{(i)}\right\}_{i \in I}$ is a single orbit of the multiplication action of $Z$ on $\Omega_M$ and $\Omega_N$ respectively.*
3. *$O_C = O_M O_N$ and $Z_{O_C} = Z_{O_M} Z_{O_N}$.*
4. *The equality $O_C = O_M O_N$ from part 3 defines a bijection $O(\Omega_G) \to O(\Omega_M) \times O(\Omega_N)$.*

*Proof.* 1. Let $g \in C$. Then, since $G = MN$, there exist $m \in M$ and $n \in N$ such that $g = mn$. Hence:

$$C = g^G = \{(mn)^{xy} | x \in M, y \in N\} = \{m^x n^y | x \in M, y \in N\} = m^M n^N,$$

where the third equality relies on the fact that $M$ and $N$ centralize each other. Now we can take $C_M := m^M$ and $C_N := n^N$.

2. Let $C_M$ and $C_N$ be as in the first part. Note that for any $z \in Z$, $C = \left(z^{-1}C_M\right)(zC_N)$. On the other hand, suppose that $C = A_1B_1$ where $A_1 \in \Omega_M$ and $B_1 \in \Omega_N$. Then there exist $m_1 \in A_1$ and $n_1 \in B_1$ such that $g = mn = m_1n_1$. Hence $z := m_1^{-1}m = n_1n^{-1} \in Z$ and $m_1 = z^{-1}m$ while $n_1 = zn$. This implies $A_1 = z^{-1}C_M$ and $B_1 = zC_N$. We have proved:

$$(*)\ \left\{\left(C_M^{(i)}, C_N^{(i)}\right)\right\}_{i\in I} = \left\{\left(z^{-1}C_M, zC_N\right)|z \in Z\right\},$$

which implies the claim.

3. Let $C_M$ and $C_N$ be as in the first part. We have $O_M = \{z_1C_M|z_1 \in Z\}$ and $O_N = \{z_2C_N|z_2 \in Z\}$. This gives

$$\begin{aligned} O_MO_N &= \{z_1C_Mz_2C_N|z_1, z_2 \in Z\} = \{z_1z_2C_MC_N|z_1, z_2 \in Z\} \\ &= \{zC|z \in Z\} = O_C. \end{aligned}$$

For the second claim, let $z \in Z_C$. Then

$$C_MC_N = C = zC = (zC_M)\, C_N.$$

This implies that the pairs $(zC_M, C_N), (C_M, C_N) \in \Omega_M \times \Omega_N$ yield the same conjugacy class $C$. By $(*)$ there exist $z' \in Z$ such that $z'^{-1}zC_M = C_M$ and $z'C_N = C_N$. Hence $z' \in Z_{C_N}$ and $z'^{-1}z \in Z_{C_M}$, and since $z = z'\left(z'^{-1}z\right)$ we get $z \in Z_{C_M}Z_{C_N}$. This proves that $Z_C \leq Z_{C_M}Z_{C_N}$. On the other hand, for any $z_1 \in Z_{C_M}$ and $z_2 \in Z_{C_N}$ we get

$$z_1z_2C = z_1C_Mz_2C_N = C_MC_N = C.$$

This proves that $Z_{C_M}Z_{C_N} \leq Z_C$ and altogether we get $Z_C = Z_{C_M}Z_{C_N}$.

4. By part 3, $O_C = O_MO_N$ with $O_M \in O(\Omega_M)$ and $O_N \in O(\Omega_N)$. Moreover, the proofs of parts 2 and 3 show that $O_C$ uniquely determines $(O_M, O_N)$, and that each pair $(O_M, O_N)$ uniquely determines an orbit $O_C$ of $G$-conjugacy classes under the multiplication action of $Z$. ∎

The following type of subset plays an important role in the analysis of the action of a central subgroup on the conjugacy classes of central products.

**Definition 2.5.** *Let $G$ be a group, $Z$ a central subgroup of $G$ and $K \trianglelefteq G$. We set $Z_{[K]} := [K, K] \cap Z$.*

**Lemma 2.6.** *Let $G$ be a group and $M$ and $N$ normal subgroups of $G$, such that $G = M \circ_Z N$, where $Z := M \cap N$.*

(a)

$$[M, M] \cap [N, N] = Z_{[M]} \cap Z_{[N]}.$$

(b) *Let $I$ and $J$ be indexing sets such that $O(\Omega_M) := \{X_i\}_{i\in I}$ and $O(\Omega_N) = \{Y_j\}_{j\in J}$. Then:*

$$Z_{[M]} = \bigcup_{i\in I} Z_{X_i}\ ,\ Z_{[N]} = \bigcup_{j\in J} Z_{Y_j} \textit{ and } Z_{[G]} = \bigcup_{i\in I}\bigcup_{j\in J} Z_{X_iY_j} = Z_{[M]}Z_{[N]}.$$

*Proof.* (a) Since $G = M\circ_Z N$, we have $[M, M]\cap[N, N] \subseteq Z$ and hence, by Definition 2.5,

$$[M, M] \cap [N, N] = [M, M] \cap [N, N] \cap Z = Z_{[M]} \cap Z_{[N]}.$$

(b) We prove $Z_{[N]} = \bigcup_{j\in J} Z_{Y_j}$. First note that since $M$ centralizes $N$, we have, for any $n \in N$, $[n, G] = [n, N]$. Let $j \in J$. By Lemma 2.1 parts (3) and (4) and

Remark 2.2 part 2, if $n \in N$ belongs to a conjugacy class in the orbit $Y_j$ then $Z_{Y_j} = [n,G] \cap Z = [n,N] \cap Z$. Therefore

$$\bigcup_{j \in J} Z_{Y_j} = \bigcup_{n \in N} ([n,N] \cap Z) = Z \cap \bigcup_{n \in N} [n,N] = Z_{[N]}.$$

The proof that $Z_{[M]} = \bigcup_{i \in I} Z_{X_i}$ and $Z_{[G]} = \bigcup_{i \in I} \bigcup_{j \in J} Z_{X_i Y_j}$ is similar, and $Z_{[G]} = Z_{[M]} Z_{[N]}$ follows from Lemma 2.4 part (3). ▮

2.3. **Basic properties of a set-direct product.** The following lemma states several equivalent conditions for the directness of a setwise product. Although the group is not assumed to be abelian the proof is essentially the same as that of [14, Lemma 2.2], and is therefore omitted.

**Lemma 2.7.** *Let $G$ be a group, and let $X$ and $Y$ be two non-empty normal subsets of $G$. The following conditions are equivalent.*

(a) $XY = X \times Y$.
(b) $XX^{-1} \cap YY^{-1} = \{1_G\}$.
(c) $\{Xy | y \in Y\}$ *or* $\{xY | x \in X\}$ *is a partition of* $XY$.

*Furthermore, if $X$ and $Y$ are finite sets then $XY$ is direct if and only if $|XY| = |X| \cdot |Y|$.*

**Remark 2.8.** *Let $G$ be a group, and let $X$ and $Y$ be two non-empty normal subsets of $G$. Then $XY = X \times Y$ implies $|X \cap Y| \leq 1$. To see this observe that if $a, b \in X \cap Y$, then $ab = ba$ are two factorizations in $X \times Y$, and hence, by uniqueness of factorization, $a = b$.*

**Lemma 2.9.** *Let $G$ be a group, and let $G = X \times Y$ be a set-direct decomposition of $G$. Then:*

(a) *If $C$ is a conjugacy class of $G$ contained in $X$, and $|C| > 1$ then $Y \cap C = Y \cap C^{-1} = \emptyset$.*
(b) *There exists a central element $z$ of $G$ such that $z \in X$ and $z^{-1} \in Y$.*
(c) *If $z$ is any central element of $G$ then $G = (zX) \times Y = X \times (zY)$.*

*Proof.* (a) Since $|C| > 1$ then $C^{-1}C = CC^{-1}$ must contain non-trivial elements, and hence, if $Y$ contains $C$ or $C^{-1}$ we get a contradiction with Lemma 2.7(b).

(b) By part (a), if $C$ is a conjugacy class, $C \subseteq X$ and $C^{-1} \subseteq Y$, then $C$ must consist of a single central element. On the other hand, since $1_G \in G$, we must have at least one class $C$ such that $C \subseteq X$ and $C^{-1} \subseteq Y$.

(c) Since $z$ is central, the normality of $X$ implies the normality of $zX$ and $(zX)^{-1}(zX) = X^{-1}X$. Similar claims hold when $X$ is replaced by $Y$. Now apply Lemma 2.7. ▮

**Remark 2.10.** *In view of Lemma 2.9(c), $Z(G) \times Z(G)$ acts on the set of all direct factorizations of $G$ via $X \times Y \longmapsto (z_1 X) \times (z_2 Y)$ where $z_1, z_2 \in Z(G)$ and by Lemma 2.9(b), each orbit of this action contains at least one normalized factorization. Note that if $X \subseteq G$ is normalized and $X$ is not a subgroup of $G$ then $gX$ is not a subgroup of $G$ for any $g \in G$. For suppose by contradiction that $gX$ is a subgroup for some $g \in G$. Then, since $1_G \in X$ we get that $g \in gX$ and hence $g^{-1} \in gX$, implying $gX = g^{-1}(gX) = X$, whereby $X$ is a subgroup - a contradiction.*

**Lemma 2.11.** *Let $G$ be a group, and let $A, B, C$ be three non-empty normal subsets of $G$. Suppose that the products $AB$ and $(AB)\,C$ are direct. Then the products $BC$ and $A\,(BC)$ are also direct.*

*Proof.* First we show that $A\,(BC)$ is direct. For this we have to show that if $a_1, a_2 \in A$, $b_1, b_2 \in B$ and $c_1, c_2 \in C$ and

$$a_1\,(b_1c_1) = a_2\,(b_2c_2)\,,$$

then $a_1 = a_2$, and $b_1c_1 = b_2c_2$. By associativity, $(a_1b_1)\,c_1 = (a_2b_2)\,c_2$. Since $(AB)\,C$ is direct, we get $c_1 = c_2$ and $a_1b_1 = a_2b_2$. Since $AB$ is direct we further get $a_1 = a_2$ and $b_1 = b_2$. It follows that $b_1c_1 = b_2c_2$. Now we show that $BC$ is direct. Let $b_1, b_2 \in B$, $c_1, c_2 \in C$ and suppose that $b_1c_1 = b_2c_2$. Multiplying on the left by some $a \in A$ (recall that by assumption $A \neq \emptyset$) and using associativity, we have

$$(ab_1)\,c_1 = (ab_2)\,c_2.$$

Since $(AB)\,C$ is direct, this gives $c_1 = c_2$ and $ab_1 = ab_2$, which yields $b_1 = b_2$. ∎

## 3. Set-direct factorizations of groups

In this section we prove the various conditions stated in the Introduction for set-direct decompositions of groups. We begin by showing that if the product of two subsets of a group is direct then they must centralize each other.

**Theorem 3.1.** *Let $G$ be a group and let $X$ and $Y$ be two normal subsets of $G$. If $XY = X \times Y$ then $[X, Y] = \{1_G\}$.*

*Proof.* Let $X$ and $Y$ be two normal subsets of $G$, and assume that $XY = X \times Y$. Let $x \in X$, $y \in Y$ and $t := xy$. It is clear that $C_G\,(x) \cap C_G\,(y) \leq C_G\,(t)$. We prove that $C_G\,(t) \leq C_G\,(x) \cap C_G\,(y)$. Let $h \in C_G\,(t)$. Then $xy = t = t^h = x^hy^h$. Since $x^h \in X$ and $y^h \in Y$, we have, by uniqueness of factorization, that $x^h = x$ and $y^h = y$, implying $h \in C_G\,(x) \cap C_G\,(y)$, and $C_G\,(t) = C_G\,(x) \cap C_G\,(y)$. In particular, $t \in C_G\,(x) \cap C_G\,(y)$. Hence $t$ commutes with both $x$ and $y$. But $t = xy$ implies $y = x^{-1}t$. Using the fact that $x$ commutes with both $x^{-1}$ and $t$ we get that $x$ and $y$ commute. ∎

Using Theorem 3.1, we obtain Theorem 1.2 as a consequence of an apparently more general statement.

Let $G$ be a group and let $X$ and $Y$ be subsets of $G$. We write $G = X \times_c Y$ if every element $g \in G$ can be uniquely expressed as $g = xy$ where $x \in X$ and $y \in Y$, and if $X$ centralizes $Y$. Clearly, for an abelian $G$, $G = X \times_c Y$ and $G = X \times Y$ is the same, and, in general, $G = X \times Y$ implies $G = X \times_c Y$.

**Theorem 3.2.** *Let $G$ be a group and let $X$ and $Y$ be subsets of $G$. Set $M := \langle X \rangle$, $N := \langle Y \rangle$ and $Z := M \cap N$. For every $m \in M$ and $n \in N$ set $X_m := \left(m^{-1}X\right) \cap Z$ and $Y_n := \left(n^{-1}Y\right) \cap Z$. Then $G = X \times_c Y$ if and only if*

(a) *$G = M \circ_Z N$; and*
(b) *$Z = X_m \times Y_n$ for every $m \in M$ and $n \in N$.*

*Proof.* Assume that $G = X \times_c Y$. Then $M$ is centralized by $Y$ and hence $M \trianglelefteq G$. Similarly, $N \trianglelefteq G$. Furthermore, $M$ centralizes $N$. Thus (a) follows.

Now we prove (b). From $G = X \times_c Y$ and by (a) we have $G = XY = M \circ_Z N$. Furthermore, $G = X \times_c Y$ and $N = \langle Y \rangle$ imply that $n$ centralizes $X$ for all $n \in N$. Similarly $m$ centralizes $Y$ for all $m \in M$. Hence, for all $m \in M$ and $n \in N$ we have

$$G = m^{-1}n^{-1}XY = m^{-1}Xn^{-1}Y,$$

and this implies $G = \left(m^{-1}X\right) \times_c \left(n^{-1}Y\right)$ for all $m \in M$ and $n \in N$ (note that uniqueness of factorization follows from that of $G = X \times_c Y$). In particular, for all $z \in Z$ there exist unique $x \in X$ and $y \in Y$ such that $z = \left(m^{-1}x\right)\left(n^{-1}y\right)$. This gives $m^{-1}x = y^{-1}nz$. As the l.h.s. is in $M$ and the r.h.s. is in $N$ we get $m^{-1}x \in \left(m^{-1}X\right) \cap Z = X_m$ and similarly, $n^{-1}y \in Y_n$. This proves $Z = X_m \times Y_n$.

Conversely, assume that conditions (a) and (b) hold true. By (a) we get that $X \subseteq M$ centralizes $Y \subseteq N$. Let $g \in G$. By (a) there exist $m \in M$ and $n \in N$ such that $g = mn$. Using (b) and the fact that $X_m$ and $Y_n$ are central we get:

$$gZ = (mn)\,X_mY_n = (mX_m)\,(nY_n) = (X \cap mZ)\,(Y \cap nZ) \subseteq XY.$$

Since $g \in gZ$ this implies the existence of $x \in X$ and $y \in Y$ such that $g = xy$. It remains to prove uniqueness of representation. Suppose that we also have $x_1 \in X$ and $y_1 \in Y$ such that $g = x_1y_1$. Then $xy = x_1y_1$ implying $x_1^{-1}xy = y_1$. Since $x_1^{-1}x \in M$ and $y \in N$, this implies $yx_1^{-1}x = y_1$ from which $x_1^{-1}x = y^{-1}y_1$ follows. Since the l.h.s. of the last equality is in $M$ and the r.h.s. is in $N$ we get $x_1^{-1}x = y^{-1}y_1 \in Z$. It now follows that $x_1^{-1}x \in X_{x_1}$ and $y^{-1}y_1 \in Y_y$, hence $x_1^{-1}x = y^{-1}y_1 \in X_{x_1} \cap Y_y$. Now, since $x_1 \in X$ we have $1_G \in X_{x_1}$ and similarly $1_G \in Y_y$. Therefore $1_G \in X_{x_1} \cap Y_y$. By (b), the product $X_{x_1}Y_y$ is direct, therefore, by Remark 2.8, $X_{x_1} \cap Y_y = \{1_G\}$. This implies $x_1 = x$ and $y_1 = y$. ∎

*Proof of Theorem 1.2.* Combine Theorems 3.1 and 3.2. ∎

*Proof of Theorem 1.5.* Since condition (a) of Theorem 1.2 holds by assumption, we have that $G = X \times Y$ if and only if $Z = X_m \times Y_n$ for every $m \in M$ and $n \in N$. Hence, by Definition 1.4, it remains to show that for any $m \in M$ and $n \in N$ we have $M_m \leq K\left(X_m\right)$ and $N_n \leq K\left(Y_n\right)$. This is immediate from Lemma 2.1 (5). ∎

**Remark 3.3.** *There is a considerable redundancy in the description of the factorization system $\left(\{X_m\}_{m\in M}, \{Y_n\}_{n\in N}\right)$ of $Z$ used in Theorem 1.5. First of all, since $Z$ is central we get that $X_{m_1} = X_{m_2}$ for any two conjugate $m_1, m_2 \in M$, or equivalently, $X_m$ depends only on the conjugacy class of $m$ in $G$. Furthermore, suppose that $C_1$ and $C_2$ are two conjugacy classes of $M$ which belong to the same $Z$-orbit. Let $m_i \in C_i$ for $i = 1, 2$ and let $c_{12} \in Z$ be such that $C_2 = c_{12}C_1$. Then by Lemma 2.1 (3) we have $M_{m_1} = M_{m_2}$. Furthermore, we have $X_{m_2} = c_{12}^{-1}X_{m_1}$. Since similar claims hold true for the $Y_n$ it follows that one can replace the indexing sets $M$ and $N$ by, respectively, the set of orbits of the multiplication action of $Z$ on $\Omega_M$ and on $\Omega_N$, and replace $\left(\{X_m\}_{m\in M}, \{Y_n\}_{n\in N}\right)$ by a "trimmed" factorization system.*

**Theorem 3.4.** *Let $Z$ be an abelian group and let $\mathcal{M} = \{M_i\}_{i\in I}$ and $\mathcal{N} = \{N_j\}_{j\in J}$ be two multisets of subgroups of $Z$. Let $(\mathcal{A}, \mathcal{B})$ be an $\mathcal{MN}$-direct factorization system of $Z$ where $\mathcal{A} = \{A_i\}_{i\in I}$ and $\mathcal{B} = \{B_j\}_{j\in J}$. Then:*

(a) *For any $i \in I$ and $j \in J$, any two distinct elements $a_1, a_2 \in A_i$ belong to distinct cosets of $N_j$ in $Z$ and any two distinct elements $b_1, b_2 \in B_j$ belong to distinct cosets of $M_i$ in $Z$.*

(b) *Suppose that $Z$ is finite. Then $(\mathcal{A},\mathcal{B})$ has to satisfy the following arithmetical conditions:*

$$|Z| = |A_i|\,|B_j|\,,\ \forall 1 \leq i \leq r,\ \forall 1 \leq j \leq s, \tag{3.1}$$

*which imply*

$$|A_1| = \cdots = |A_r|\,,\ |B_1| = \cdots = |B_s|\,, \tag{3.2}$$

*and also*

$$\operatorname{lcm}(|M_1|,...,|M_r|) \text{ divides } |A_1| \text{ and } \operatorname{lcm}(|N_1|,...,|N_s|) \text{ divides } |B_1|\,. \tag{3.3}$$

*Proof.* (a) We prove the first part of the claim. The proof of the second part is essentially the same. Suppose, by contradiction, that there exist $i \in I$ and $j \in J$, and two elements $a_1 \neq a_2 \in A_i$ which belong to the same coset of $N_j$ in $Z$. Then $a_1 = n_1x$ and $a_2 = n_2x$, where $n_1 \neq n_2$ are elements of $N_j$ and $x \in Z$. Since $B_j$ is a non-empty union of cosets of $N_j$, there exists some $y \in Z$, such that $N_jy \subseteq B_j$. Hence $b_1 := n_1y$ and $b_2 := n_2y$ belong to $B_j$ and $a_1b_2 = a_2b_1$ are two distinct factorizations in $A_i \times B_j$ of the same element - a contradiction.

(b) Equation 3.1 is immediate from Lemma 2.7. For Equation 3.3 note that $|K(A)|$ divides $|A|$ for any finite, non-empty $A$. Hence, by Definition 1.4, $|M_i|$ divides $|A_i|$ for all $1 \leq i \leq r$. Similarly, $|N_j|$ divides $|B_j|$ for all $1 \leq j \leq s$. Now Equation 3.3 follows from Equation 3.2.

∎

*Proof of Theorem 1.6.* Fix arbitrary $i \in I$ and $j \in J$. Since $M_i \leq K(A_i)$ we get that $A_i$ is a union of cosets of $M_i$, and similarly, $B_j$ is a union of cosets of $N_j$. Therefore we can write $A_i = \bigcup\limits_s a_{is}M_i$ where the $a_{is} \in Z$ represent distinct cosets of $M_i$ and similarly $B_j = \bigcup\limits_t b_{jt}N_j$, with $b_{jt}$ representing distinct cosets of $N_j$. Hence all the $M$-conjugacy classes $a_{is}C_i$, which are contained in $A_iC_i$, are distinct for distinct values of $s$, and similarly, the $N$-conjugacy classes $b_{jt}D_j$ which are contained in $B_jD_j$ are distinct for distinct values of $t$. We claim that $\bigcup\limits_{s,t}\{a_{is}b_{jt}\}$ is a transversal of $Z_{ij}$ in $Z$, where $ij$ is the unique $Z$-orbit formed by the product of $i$ and $j$ (see Lemma 2.4 (3)). In the first place, using $Z_{ij} = M_iN_j$ (Lemma 2.4 (3)), we get

$$\left(\bigcup_{s,t}\{a_{is}b_{jt}\}\right)Z_{ij} = \left(\bigcup_s a_{is}M_i\right)\left(\bigcup_t b_{jt}N_j\right) = A_iB_j = Z.$$

Next, suppose that $a_{is}b_{jt}Z_{ij} = a_{is'}b_{jt'}Z_{ij}$. This yields $a_{is}b_{jt} \in (a_{is'}M_i)(b_{jt'}N_j)$ which implies the existence of $z_1 \in M_i$ and $z_2 \in N_j$ such that $a_{is}b_{jt} = (a_{is'}z_1)(b_{jt'}z_2)$. Observe that $a_{is'}z_1 \in A_i$ and $b_{jt'}z_2 \in B_j$. By uniqueness of factorization in $A_i \times B_j$ we get $a_{is} = a_{is'}z_1$ and $b_{jt} = b_{jt'}z_2$. If $s \neq s'$, we have, by our choice, that $a_{is}$ and $a_{is'}$ belong to distinct $M_i$ cosets in contradiction to $a_{is} = a_{is'}z_1$. Hence $s = s'$ and similarly $t = t'$. Now it follows that $a_{is}b_{jt}C_iD_j$ are distinct conjugacy classes for distinct pairs $(s,t)$, and $\bigcup\limits_{s,t}\{a_{is}b_{jt}\}C_iD_j = ij$. This shows that $G = X \times Y$. ∎

The next theorem is needed for the proof of Theorem 1.7.

**Theorem 3.5.** *Let $N$ be a group and $Z$ a central subgroup of $N$. Then the following conditions are equivalent:*

(1) *$Z$ has a normal transversal $Y$ in $N$.*

(2) *$Z$ acts semi-regularly on $\Omega_N$.*

*Furthermore, if $N$ is finite then each one of (1) and (2) is equivalent to $k(N) = k(Z)\,k(N/Z)$.*

*Proof.* Suppose that $Z$ has a normal transversal $Y$ in $N$. Then every element of $Y$ meets every coset of $Z$ in $N$ in precisely one element which is equivalent to $|Y_n| = 1$ for every $n \in N$. Let $D \in \Omega_N$. By Lemma 2.1 (5) we have $Z_D \leq K(Y_n)$, where $n \in D$. Since $|Y_n| = 1$, we get that $K(Y_n) = \{1_Z\}$ and therefore $Z_D = \{1_Z\}$ for all $D \in \Omega_N$ which is the claim of (2).

Conversely, assume (2). Let $J$ denote the set of all distinct orbits of the multiplication action of $Z$ on $\Omega_N$. For each $j \in J$ let $D_j$ be a conjugacy class belonging to the orbit $j$. We claim that $T := \bigcup_{j\in J} D_j$ is a normal transversal of $Z$ in $N$. The normality of $T$ in $N$ is clear as it is a union of conjugacy classes. Since $Z$ acts transitively by multiplication on each orbit we have $ZD_j = j$ and hence $ZT = N$. Now suppose that $t_1, t_2 \in T$ satisfy $Zt_1 = Zt_2$. Then there exist $z \in Z$ such that $t_2 = zt_1$. If $z \neq 1$ then, by the semi-regularity assumption, $t_1$ and $t_2$ belong to two distinct conjugacy classes of $N$, say $D_1$ and $D_2$ respectively, but, on the other hand, $D_1$ and $D_2$ belong to the same $Z$-multiplication orbit. This contradicts the construction of $T$. Hence $z = 1$ and $t_2 = t_1$.

Finally, the last claim of the theorem follows from Lemma 2.1 (6). ∎

*Proof of Theorem 1.7.* By assumption, $M := \langle X\rangle = X$. Suppose that $G = X \times Y$. Then $G = X \circ_Z N$ follows from Theorem 1.2(a). By Theorem 1.2(b) we have $Z = X_m \times Y_n$ for every $m \in M$ and $n \in N$. Since $M = X$ we have $Z \subseteq X$ and $mZ \subseteq X$ for every $m \in M$ and hence $X_m = Z$. By uniqueness of representation in the set-direct product $Z = X_m \times Y_n$, this forces $|Y_n| = 1$ for all $n \in N$.

Conversely, assume condition (2). Let $m \in M$ and $n \in N$. Then $X_m = Z$ and $|Y_n| = 1$ implies $Z = X_m \times Y_n$. Now (1) follows by Theorem 1.2.

The condition that for any $n \in N$ we have $|Y_n| = 1$, is equivalent to the statement that $Y$ intersects every coset of $Z$ in $N$ in precisely one element, which is equivalent to $Y$ being a transversal of $Z$ in $N$. The remaining claims follow from Theorem 3.5. ∎

*Second proof of Corollary 1.8.* Let $Y$ be a normal transversal of $Z$ in $N$. Set $N_1 = \langle Y\rangle$. Clearly $N_1 \leq N$ is a normal subgroup of $G$ and $Z_1 := M \cap N_1$ is a subgroup of $Z$. We have $G = MN = MZY = MY$ and hence $G = MN_1$ implying $G = M \circ_{Z_1} N_1$. Now, since $Y$ is a normal transversal of $Z$ in $N$ it follows that $|Y_n| = 1$ for all $n \in N$ (see last paragraph of the proof of Theorem 1.7) and hence for all $n \in N_1$. Furthermore, $Z_1 \leq M$ and hence, setting $X := M$, we get $X_m = \left(m^{-1}X\right) \cap Z_1 = Z_1$ for all $m \in M$. Thus, condition (2) of Theorem 1.7 is satisfied when substituting $N_1$ for $N$ and $Z_1$ for $Z$. Consequently $G = M \times Y$. ∎

In order to prove Theorem 1.9 we need the following result.

**Lemma 3.6.** *Let $Z$ be an abelian group and let $\mathcal{M} := \{M_i\}_{i\in I}$ and $\mathcal{N} := \{N_j\}_{j\in J}$ be two multisets of subgroups of $Z$. If there exists an $\mathcal{M}\mathcal{N}$-direct factorization system of $Z$, then $M_i \cap N_j = \{1_G\}$ for any $i \in I$ and $j \in J$.*

*Proof.* Let $\mathcal{A} := \{A_i\}_{i\in I}$ and $\mathcal{B} := \{B_j\}_{j\in J}$ be an $\mathcal{M}\mathcal{N}$-direct factorization system of $Z$. Let $i \in I$ and $j \in J$ be arbitrary. Let $g \in M_i \cap N_j$, $a \in A_i$ and $b \in B_j$.

By definition of an $\mathcal{MN}$-direct factorization system of $Z$, $g \in K(A_i) \cap K(B_j)$ and therefore $(ga)\,b = a\,(gb)$ are two factorizations of an element of $Z$ in $A_i \times B_j$. By uniqueness $ga = a$ implying $g = 1_Z$. This proves $M_i \cap N_j = \{1_G\}$. ∎

*Proof of Theorem 1.9.* Apply the notation of Lemma 2.6(b). Set $\mathcal{M} = \{M_i\}_{i\in I}$ where $M_i := Z_{X_i}$ for all $i \in I$, and $\mathcal{N} = \{N_j\}_{j\in J}$ where $N_j := Z_{Y_j}$ for all $j \in J$. Let $\mathcal{A} = \{A_i\}_{i\in I}$ where $A_i = X_0$ for all $i \in I$, and $\mathcal{B} = \{B_j\}_{j\in J}$ where $B_j = Y_0$ for all $j \in J$. By Lemma 2.6(b), $M_i \subseteq Z_{[M]} = [M,M] \cap Z$, and by assumption of the theorem, $Z_{[M]} \subseteq K_Z(X_0)$ so $M_i \leq K(A_i)$ for each $i \in I$. Similarly, $N_j \leq K(B_j)$ for all $j \in J$. Hence, by Definition 1.4, $(\mathcal{A}, \mathcal{B})$ is an $\mathcal{MN}$-direct factorization system of $Z$. Now apply Theorem 1.6. Note that $Z$ itself is an orbit of conjugacy classes in both $M$ and $N$. Using the notation of Theorem 1.6, let $i \in I$ and $j \in J$ be the labels of $Z$ as an orbit of conjugacy classes. Choose in the proof of that theorem $C_i = D_j = \{1_G\}$. This choice ensures that $X_0 = X \cap Z$ and $Y_0 = Y \cap Z$. ∎

**Proposition 3.7.** *Let $G$ be a group and $M$ and $N$ normal subgroups of $G$, such that $G = M \circ_Z N$. Let $G = X \times Y$ such that $X \subseteq M$ and $Y \subseteq N$. Then*

$$M = X \times (Y \cap Z) \text{ and } N = Y \times (X \cap Z),$$

*and*

$$[M,M] \cap [N,N] = Z_{[M]} \cap Z_{[N]} = \{1_G\}.$$

*Proof.* Clearly, $X$ and $(Y \cap Z)$ are normal subsets of $M$. Since $G = X \times Y$ any $m \in M$ has a unique factorization $m = xy$ with $x \in X \subseteq M$ and $y \in Y \subseteq N$. This implies $y = x^{-1}m \in M$ so $y \in Z$. Thus we have proved that every $m \in M$ has a unique factorization $m = xy$ with $x \in X$ and $y \in Y \cap Z$, so $M = X \times (Y \cap Z)$. The proof that $N = Y \times (X \cap Z)$ is similar.

For the proof of the second claim we use the first claim:

$$\begin{aligned} Z_{[M]} \cap Z_{[N]} &\subseteq [M,M] \cap [N,N] \\ &= [X \times (Y \cap Z), X \times (Y \cap Z)] \cap [Y \times (X \cap Z), Y \times (X \cap Z)] \\ &= [X,X] \cap [Y,Y] \subseteq \left(XX^{-1}\right) \cap \left(YY^{-1}\right) = \{1_G\}, \end{aligned}$$

where $[X \times (Y \cap Z), X \times (Y \cap Z)] = [X,X]$ since $Y \cap Z$ is central in $G$, $[X,X] \subseteq \left(XX^{-1}\right)$ since $X$ is normal, and the last equality follows from Lemma 2.7. ∎

*Proof of Corollary 1.10.* Set $M := G$ and $N := Z := \langle z \rangle$. Then $G = M \circ_Z N$ and by assumption $o(z) = p^k$ where $p$ is a prime and $k \geq 2$ an integer. Let $X_0 = \langle z^p \rangle$ and $Y_0 = \left\{1_Z, z, z^2, ..., z^{p-1}\right\}$. Then $X_0$ is a subgroup of $Z$ of order $p^{k-1}$ and $Y_0$ is a transversal of $X_0$ in $Z$ whereby $Z = X_0 \times Y_0$. It is immediate to check that $K_Z(X_0) = X_0$ and $K_Z(Y_0) = \{1_Z\}$. Consider the multiplication action of $Z$ on $\Omega_G$. Since $z$ is semi-regular, the stabilizer of any conjugacy class is proper in $Z$. But $X_0$ is the unique maximal subgroup of $Z$ and hence it contains all of the point stabilizers. By Lemma 2.6(b) this implies $Z_{[M]} = [M,M] \cap Z \subseteq X_0 = K_Z(X_0)$. The condition $[N,N] \cap Z \subseteq K_Z(Y_0)$ is immediate to verify. Thus all the conditions of Theorem 1.9 are satisfied and we can deduce the existence of a set-direct factorization $G = X \times Y$ with $X \subseteq M$, $Y \subseteq N$, $X \cap Z = X_0$ and $Y \cap Z = Y_0$, which is non-trivial since $Z = X_0 \times Y_0$ is non-trivial. Observe that both $Y = Y_0$ and $X$ are normalized, and that $Y$ is not a group. Now assume that $G$ is perfect. We will show that under this assumption also $X$ is not a group. Suppose by contradiction that $X$ is a group. Since $G = X \times Y$ and $Y$ is central, we have

$[G,G] = [X,X]$ and hence $X = \langle X\rangle$ contains all commutators in $G$ and hence also the derived subgroup $G' = \langle [G,G]\rangle$. But $G' = G$ by assumption and hence $X = G$. This contradicts $Y = Y_0 \nsubseteq X$. ∎

## 4. Finite quasi-simple groups

In this section we prove Theorem 1.11 which states conditions for the existence of non-trivial set-direct decompositions of finite quasi-simple groups. The proof demonstrates the use of some of the results of the previous sections. Recall that a group $G$ is quasi-simple if $G = G'$ and $G/Z(G)$ is a simple group. The center of a finite quasi-simple group $G$ must be isomorphic to a factor group of the Schur multiplier of $G/Z(G)$ ([1, Section 33]). Information on the relevant Schur multipliers is given in [2].

**Lemma 4.1.** *Let $G$ be a finite quasi-simple group such that $G = X \times Y$ with $|X| > 1$ and $|Y| > 1$. Then precisely one of $X$ and $Y$ is central and the other factor, which has non-central elements, generates $G$ but is not a group.*

*Proof.* Set $M := \langle X\rangle$, $N := \langle Y\rangle$ and $Z := M \cap N$. By Theorem 1.2, $G = M \circ_Z N$ and $Z \leq Z(G)$. We have $G/Z = (M/Z) \times (N/Z)$ and both $M/Z$ and $N/Z$ are perfect groups. Since $G/Z(G) \cong (G/Z)\,/\,(Z(G)/Z)$ is simple, we must have that one of $M/Z$ and $N/Z$ is trivial. Assume without loss of generality that $N = Z$. Then $Y$ is central and $M = G$. Now suppose by contradiction that $X$ is a group. Then, since $Y$ is central we get $[G,G] = [X,X]$ (see the first paragraph of Section 2). But this gives, using the fact that $G$ is perfect

$$G = G' = \langle [X,X]\rangle = X' \leq X,$$

in contradiction to $|Y| > 1$. ∎

Let $G$ be a finite quasi-simple group. Blau [3] has essentially classified the semi-regular elements of all finite quasi-simple groups. The following rephrasing of [3, Theorem 1] is a key result for the proof of Theorem 1.11. Recall that $z \in Z(G)$ is semi-regular if $zC \neq C$ for any $C \in \Omega_G$.

**Theorem 4.2** ([3, Theorem 1])**.** *Let $G$ be a finite quasi-simple group. If $z \in Z(G)$ is semi-regular then one of the following holds:*

(i) $G/Z(G) = A_6$, $A_7$, $\mathrm{Fi}_{22}$, $\mathrm{PSU}(6,4)$, or ${}^2\mathrm{E}_6(4)$ and $o(z) = 6$.
(ii) $G/Z(G) = \mathrm{PSU}(4,9)$, $\mathrm{M}_{22}$, or $G/Z(G) = \mathrm{PSL}(3,4)$ with $Z(G)$ cyclic, and $o(z) \in \{6,12\}$.
(iii) $G/Z(G) = \mathrm{PSL}(3,4)$, $Z(G)$ is non-cyclic and $o(z) \in \{2,4,6,12\}$.

For case (iii) of the last theorem we need more detailed information. We use the fact that the Schur multiplier of $\mathrm{PSL}(3,4)$ is isomorphic to $C_3 \times C_4 \times C_4$.

**Lemma 4.3.** *Let $G$ be a finite quasi-simple group with $G/Z(G) = \mathrm{PSL}(3,4)$, and $Z(G)$ is non-cyclic. Then:*

**(a):** *All elements of $Z(G)$ which are of order 6 or 12 are semi-regular.*
**(b):** *$Z(G)$ has a semi-regular 2-element if and only if $|Z(G)|$ is divisible by 8.*
**(c):** *If $|Z(G)|$ is divisible by 8 but not by 16 then $Z(G)$ has precisely one semi-regular involution and no semi-regular element of order 4.*
**(d):** *If $|Z(G)|$ is divisible by 16 then $Z(G)$ contains precisely six semi-regular elements of order 4 and no semi-regular involution.*

*Proof.* $Z(G)$ must be isomorphic to one of the following six non-cyclic subgroups of $C_3 \times C_4 \times C_4$:

$$C \times C_4 \times C_4,\ C \times C_4 \times C_2,\ C \times C_2 \times C_2,$$

where $C$ is either the trivial group or a group of order 3. Moreover, each of these six groups determines a unique, up to isomorphism, quasi-simple $G$ with $G/Z(G) = \mathrm{PSL}(3,4)$. By [3, Lemma 1], $z \in Z(G)$ is semi-regular if and only if $\sum\limits_{\chi\in \mathrm{Irr}(G)} \chi(z)/\chi(1) = 0$, where $\mathrm{Irr}(G)$ is the set of complex irreducible characters of $G$. The character tables of all of the six relevant groups are implemented in GAP's character table library ([5],[4]), and this was used in order to identify the central elements and check, for each one of them, the cited condition. ∎

The following two lemmas are needed for analyzing the case of a quasi-simple $G$ with $G/Z(G) = \mathrm{PSL}(3,4)$.

**Lemma 4.4.** *Let $H_6 = \langle a\rangle \times \langle b\rangle$ with $o(a) = 3$ and $o(b) = 2$. Let $X := \{1, x\}$ where $x \neq 1$ is some element of $H_6$ and $Y := \{1, a, ab\}$. Then $XY$ is not direct.*

*Proof.* A direct computation gives $YY^{-1} = H_6$. Hence $XX^{-1} \cap YY^{-1} = XX^{-1}$. Since $x \in XX^{-1}$, we get $XX^{-1} \neq \{1_G\}$, and therefore the claim follows from Lemma 2.7. ∎

**Lemma 4.5.** *Let $H_{12} = \langle a\rangle \times \langle b\rangle$ with $o(a) = 3$ and $o(b) = 4$. Let $X \subseteq H_{12}$ where $1 \in X$ and $|X| = 4$, and let $Y := \{1, b, ab^{\varepsilon}\}$ with $\varepsilon \in \{1, -1\}$ . Then $XY$ is not direct.*

*Proof.* Assume, by contradiction, that $XY$ is direct. Then, by Lemma 2.7, $XX^{-1} \cap YY^{-1} = \{1\}$. We have

$$YY^{-1} = \left\{1, b, b^{-1}\right\} \cup S_Y \text{ where } S_Y := \left\{ab^{\varepsilon}, a^{-1}b^{-\varepsilon}, a^{-1}b^{1-\varepsilon}, ab^{\varepsilon-1}\right\}.$$

Since $\left|YY^{-1}\right| = 7$ and $|H_{12}| = 12$, the size of $XX^{-1}$ is either 4, 5, or 6. Also note that (using $b^{2-\varepsilon} = b^{\varepsilon}$ for all $\varepsilon \in \{1, -1\}$):

$$H_{12}\backslash \left\{YY^{-1}\right\} = \left\{b^2\right\} \cup S_X \text{ where } S_X := b^2 S_Y = \left\{ab^{-\varepsilon}, a^{-1}b^{\varepsilon}, a^{-1}b^{-(1+\varepsilon)}, ab^{1+\varepsilon}\right\}.$$

Since $\{1\} = X \cap YY^{-1}$, the set $X$ has no element of order 4 and hence $X$ is not a subgroup.

Assume that $|XX^{-1}| = 4$. Since $X \cup X^{-1} \subseteq XX^{-1}$, we must have $XX^{-1} = X \cup X^{-1}$ and so $X = X^{-1}$ implying that $X^2 = X$. Thus $X$ is a subgroup contradicting our previous assertion.

Assume that $\left|XX^{-1}\right| = 5$. Both $X \cup X^{-1}$ and $XX^{-1}$ are inverse closed and contain 1. Also, for any $h \in H_{12}$, $h = h^{-1}$ if and only if $h \in \left\{1, b^2\right\}$. Since $\left|XX^{-1}\right|$ is odd this implies $b^2 \notin XX^{-1}$. But then $b^2 \notin X \cup X^{-1}$ and hence $\left|X \cup X^{-1}\right|$ is odd, implying $XX^{-1} = X \cup X^{-1} = \{1\} \cup S_X$.

Observe that for any $\delta \in \{1, -1\}$, we have $a^{-1}b^{\varepsilon} \in X^{\delta}$ if and only if $ab^{1+\varepsilon} \in X^{\delta}$, since otherwise $b^{-1} = \left(a^{-1}b^{\varepsilon}\right)\left(ab^{1+\varepsilon}\right) \in XX^{-1}$ is a contradiction. Similarly, $ab^{-\varepsilon} \in X^{\delta}$ if and only if $a^{-1}b^{-(1+\varepsilon)} \in X^{\delta}$. But the combination of the last two assertions contradicts $|X| = 4$.

Assume that $|XX^{-1}| = 6$. Then $XX^{-1} = \{1, b^2\} \cup S_X$. First suppose that $b^2 \notin X$. Then $|X \cup X^{-1}| = 5$ as in the discussion of the $\left|XX^{-1}\right| = 5$ case, and this implies $X \cup X^{-1} = \{1\} \cup S_X$. But now a routine check shows that $b^2 \notin$

$\left(X \cup X^{-1}\right)^2 \supseteq XX^{-1}$ - a contradiction. Thus $b^2 \in X$ and hence $b^2X^{-1} \subseteq XX^{-1}$. Since $b^2S_X = S_Y \subseteq YY^{-1}$, we have

$$b^2(X^{-1} \cap S_X) = b^2X^{-1} \cap b^2S_X \subseteq XX^{-1} \cap YY^{-1} = \{1\}.$$

Since $b^2$ is an involution, it follows that $X^{-1} \cap S_X \subseteq \{b^2\}$, implying $X^{-1} \cap S_X = \emptyset$ and $|X| = 2$ - the final contradiction. ∎

*Proof of Theorem 1.11.* Suppose that $G = X \times Y$ such that $X$ and $Y$ are normalized and $|X| > 1$ and $|Y| > 1$. Set $M = \langle X \rangle$, $N = \langle Y \rangle$, $Z := M \cap N$. By Theorem 1.2, $G = M \circ_Z N$, and by Lemma 4.1 we can assume $N = Z = \langle Y \rangle$ and $M = G$. Since $Y$ is normalized we have $1 \in Y$, and since $1 \in M_m$ for every $m \in M$ we get, by Theorem 3.4(a), that for all $1 \neq y \in Y$ and all $m \in M$, $y \notin M_m$. Thus, all non-trivial elements of $Y$ must be semi-regular, and it suffices to consider groups $G$ which fall into one of the cases (i)-(iii) of Theorem 4.2. We now split the discussion into three cases.

**Case I:** $G/Z\left(G\right)$ is not isomorphic to PSL(3,4) or $G/Z\left(G\right) = \mathrm{PSL}(3,4)$ and 8 does not divide $|Z\left(G\right)|$. We have to show that the assumptions of Case I lead to a contradiction. By Theorem 1.5, using its notation, there exists an associated $\mathcal{MN}$-direct factorization system $\left(\{X_m\}_{m \in M}, \{Y_n\}_{n \in N}\right)$ of $Z$. It suffices to show that the assumption $Z = X_m \times Y$, for all $m \in M$, leads to a contradiction. By Theorem 4.2 and by Lemma 4.3, all non-trivial $y \in Y$ satisfies $o\left(y\right) \in \{6, 12\}$. Since $Y \subseteq Z$ this implies that $|Z|$ is divisible by 6. Therefore, $Z$ has an element of order 2 and an element of order 3, and each such element must fix at least one conjugacy class of $G$, whereby we must have $m_1, m_2 \in M$ (not necessarily distinct!) such that $2 \mid |M_{m_1}|$ and $3 \mid |M_{m_2}|$. Now, by Equations 3.2 and 3.3, 6 divides $|X_m|$ for all $m \in M$. Hence, since $|Y| > 1$ we can conclude that $|Z| = |X_m|\,|Y| \geq 12$ (for any $m \in M$). Suppose that $|Z| = 12$. In this case $|Y| = 2$ and since $Z = N = \langle Y \rangle$ and $1 \in Y$, the single non-trivial element of $Y$ must be a generator of $Z$ and hence has order 12. Therefore $Z$ has an element of order 4, which fixes a conjugacy class, and Equation 3.3 implies that 12 divides $|X_m|$ in contradiction to $|Y| = 2$. Thus, we must have $|Z| > 12$. Examining the relevant Schur multipliers of $G/Z\left(G\right)$, we are left with the possibility $G/Z\left(G\right) = \mathrm{PSU}(4,9)$. The Schur multiplier of this group is isomorphic to $C_3 \times C_3 \times C_4$. The condition $|Z| > 12$ and the fact that $|Z|$ divides the order of the Schur multiplier leave two possibilities for $Z$.

**(1):** $Z \cong C_3 \times C_3 \times C_2$. Choose generators for the direct factors so that $Z = \langle g_1 \rangle \times \langle g_2 \rangle \times \langle g_3 \rangle$ with $o\left(g_1\right) = o\left(g_2\right) = 3$ and $o\left(g_3\right) = 2$. We have $Z = \langle Y \rangle$, and all non-trivial elements of $Y$ have order 6. As argued above, $6 \mid |X_m|$ for all $m \in M$, and hence $6\,|Y|$ divides $|X_m|\,|Y| = |Z| = 18$, forcing $|Y| = 3$. Thus $Y = \{1, y_1, y_2\}$ with $o\left(y_1\right) = o\left(y_2\right) = 6$. Note that $y_i = \theta_i g_3$ where $\theta_1$ and $\theta_2$ are elements of order 3. Since $Z = \langle Y \rangle$ we get that $\theta_1$ and $\theta_2$ belong to two distinct order 3 subgroups. Note that $Z$ has 4 distinct subgroups of order 3, and fixing any two of them, the other two are the two diagonal subgroups of the direct product of the first two. Therefore we can assume, without loss of generality, that $y_1 := g_1g_3$ and $y_2 := g_2g_3$. Observe that $g_1$, being of order 3, must fix a conjugacy class of $G$. It follows that there exists some $m \in M$ such that $g_1$ fixes the conjugacy class of $m$. Thus $X_mg_1$

$= X_m$ and so $\langle g_1 \rangle \leq K(X_m)$. However, we will now prove that there is no $m \in M$ such that $Z = X_m \times Y$ and $\langle g_1 \rangle \leq K(X_m)$. Assume by contradiction that there exists $m \in M$ such that $Z = X_m \times Y$ and $\langle g_1 \rangle \leq K(X_m)$. Note that the cyclic group $\langle g_2 g_3 \rangle$ of order 6 is a transversal of $\langle g_1 \rangle$, and hence $X_m = \langle g_1 \rangle \alpha_1 \cup \langle g_1 \rangle \alpha_2$, where $\alpha_1$ and $\alpha_2$ are two distinct elements of $\langle g_2 g_3 \rangle$. By Lemma 2.9(c) $Z = \left(\alpha_1^{-1} X_m\right) \times Y$, and hence we can assume, without loss of generality, that $X_m = \langle g_1 \rangle \cup \langle g_1 \rangle \alpha$ for some $\alpha \notin \langle g_1 \rangle$. Furthermore, $Z = X_m \times Y$ implies $Z / \langle g_1 \rangle = \{1, \alpha\} \times \{1, g_2, g_2 g_3\}$, where, by a slight abuse of notation, we label $\langle g_1 \rangle$ cosets of $Z$ by their $Z$-representatives names. This contradicts the assertion of Lemma 4.4. Hence the possibility $Z \cong C_3 \times C_3 \times C_2$ is ruled out By Theorem 1.5 (see also Definition 1.4).

**(2):** $Z \cong C_3 \times C_3 \times C_4$. Choose generators for the direct factors so that $Z = \langle g_1 \rangle \times \langle g_2 \rangle \times \langle g_4 \rangle$ with $o(g_1) = o(g_2) = 3$ and $o(g_4) = 4$. In this case, every element in $Z$ of order 3 or 4 must fix a conjugacy class of $G$. Hence, by Equation 3.3, 12 divides $|X_m|$ for all $m \in M$. By similar arguments to those of case (1), $Y = \{1, y_1, y_2\}$ with $\{o(y_1), o(y_2)\} \subseteq \{6, 12\}$. If $o(y_1) = o(y_2) = 6$ then $\langle Y \rangle < Z$ - a contradiction. Suppose that $Y = \{1, y_1, y_2\}$ with $o(y_1) = 6$, $o(y_2) = 12$ and $\langle Y \rangle = Z$. Then (compare with the treatment of the previous case $Z \cong C_3 \times C_3 \times C_2$) we may assume that $y_1 := g_1 g_4^2$ and $y_2 := g_2 g_4$ or $y_1 := g_2 g_4^2$ and $y_2 := g_1 g_4$. Assume $y_1 := g_1 g_4^2$ and $y_2 := g_2 g_4$. Then $Y y_2^{-1} = \left\{1, y_1' := y_1 y_2^{-1} = g_1 g_2^{-1} g_4, y_2' := y_2^{-1}\right\}$ and $o(y_1') = o(y_2') = 12$. By Lemma 2.9(c) $Z = X_m \times \left(Y y_2^{-1}\right)$. Applying similar considerations for the case $y_1 := g_2 g_4^2$ and $y_2 := g_1 g_4$, we conclude that it remains to consider $Y = \{1, y_1, y_2\}$ with $o(y_1) = o(y_2) = 12$. We prove, by contradiction, that there is no $m \in M$ such that $Z = X_m \times Y$ and $\langle g_1 \rangle \leq K(X_m)$. Arguing as before, we can assume, without loss of generality, that $y_1 := g_1 g_4^{\varepsilon_1}$ and $y_2 := g_2 g_4^{\varepsilon_2}$ with $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$. Using the fact that $Z = X_m \times Y$ if and only if $Z = X_m^{-1} \times Y^{-1}$ implies that it would suffice to check $(\varepsilon_1, \varepsilon_2) = (1, 1)$ and $(\varepsilon_1, \varepsilon_2) = (1, -1)$. The cyclic group $\langle g_2 g_4 \rangle$ of order 12 is a transversal of $\langle g_1 \rangle$, and hence we can assume, without loss of generality, using arguments as before, that $X_m = \langle g_1 \rangle \cup \langle g_1 \rangle \alpha_1 \cup \langle g_1 \rangle \alpha_2 \cup \langle g_1 \rangle \alpha_3$, where $\alpha_1, \alpha_2, \alpha_3$ represent any three distinct non-trivial cosets of $\langle g_1 \rangle$ in $Z$ which are contained in $\langle g_2 g_4 \rangle \langle g_1 \rangle \setminus \langle g_1 \rangle Y$. Furthermore, $Z = X_m \times Y$ implies $Z / \langle g_1 \rangle = \{1, \alpha_1, \alpha_2, \alpha_3\} \times \left\{1, g_4, g_2 g_4^{\pm 1}\right\}$. This contradicts the assertion of Lemma 4.5. Hence the possibility $Z \cong C_3 \times C_3 \times C_4$ is ruled out.

**Case II:** $G/Z(G) = \mathrm{PSL}(3,4)$, and $Z(G)$ is non-cyclic such that 8 divides $|Z(G)|$ but 16 does not divide $|Z(G)|$. By Lemma 4.3 (c), $Z(G)$ has a unique semi-regular involution $z$. Choose $Z = \langle z \rangle \cong C_2$. Clearly $G = M \circ_Z N$ with $M = G$ and $N = Z$. Notice that each orbit of conjugacy classes of $G$ with respect to the multiplication action of $Z$ has length 2. Setting $I := O(\Omega_M)$ and $J := O(\Omega_N)$, we have $|J| = 1$, and all of the point stabilizers, $M_i$ with $i \in I$ and the single $N_j$ with $j \in J$ are trivial. Thus $\mathcal{A} := \{A_i\}_{i \in I}$ and $\mathcal{B} := \{B_j\}_{j \in J}$ is an $\mathcal{MN}$-direct factorization system of

$Z$, where $\mathcal{M} = \{M_i\}_{i\in I}$, $\mathcal{N} = \{N_j\}_{j\in J}$, $A_i = \{1\}$ for all $i \in I$ and $B_j = Z$. By Theorem 1.6 we get a normalized set-direct factorization $G = X \times Z$, where $X$ contains precisely one conjugacy class from each $Z$-orbit, and $X$ is not a group by Lemma 4.1.

**Case III:** $G/Z(G) = \mathrm{PSL}(3,4)$, and $Z(G)$ is non-cyclic such that 16 divides $|Z(G)|$. By Lemma 4.3 (d), $Z(G)$ has semi-regular elements of order 4. In this case $G$ satisfies all the conditions of Corollary 1.10 and hence $G$ has a non-trivial normalized set-direct factorization such that none of the factors is a group.

∎

## 5. Products of two conjugacy classes

In this section we consider the directness of products of two conjugacy classes.

**Theorem 5.1.** *Let $G$ be a group having a unique minimal normal subgroup $N$. Suppose in addition that $N$ is non-abelian. Let $C$ and $D$ be any two non-trivial conjugacy classes of $G$. Then the product $CD$ is non-direct. In particular, if $G$ is a finite almost simple group then the product of any two non-trivial conjugacy classes of $G$ is non-direct.*

*Proof.* Suppose by contradiction that the product $CD$ is direct. By Theorem 3.1, $C$ and $D$ centralize each other. Now $\langle C\rangle$ and $\langle D\rangle$ are non-trivial normal subgroups of $G$, and hence $N \leq \langle C\rangle \cap \langle D\rangle$. But since $C$ and $D$ centralize each other we have that $\langle C\rangle \cap \langle D\rangle$ is abelian while $N$ is not - a contradiction. ∎

**Remark 5.2.** *The conclusion of Theorem 5.1 is false if $G$ has more than one non-abelian minimal normal subgroup. In fact, let $G$ be a group and let $N_1$ and $N_2$ be two minimal normal subgroups of $G$ which are not central. Then there are two non-trivial conjugacy classes $C_1$ and $C_2$ of $G$, such that $C_1 \subset N_1$ and $C_2 \subset N_2$ and it is easy to see that $C_1C_2$ is direct. Furthermore, the conclusion of Theorem 5.1 need not be true if $G$ has an abelian minimal normal subgroup which is non-central. Consider, for example, a dihedral group of order* 10. *Then $G$ has a unique minimal normal subgroup $\langle g\rangle$ of order* 5. *Set $C_1 := \{g, g^4\}$ and $C_2 := \{g^2, g^3\}$. These are conjugacy classes of $G$ and their product is direct.*

## Acknowledgement

We are indebted to the anonymous referee for noticing a mistake in a previous version of Theorem 1.11 and for the many comments which significantly improved the correctness and clarity of our original exposition. We are also grateful to S. Szabó for a helpful communication.

## References

[1] M. Aschbacher, Finite Group Theory, second edition, Cambridge studies in advanced mathematics 10, Cambridge University Press, (2000).

[2] ATLAS of finite group representations - version 3. (http://brauer.maths.qmul.ac.uk/Atlas/v3/).

[3] H.I. Blau, A fixed point theorem for central elements in quasi-simple groups, Proc. Am. Math. Soc., vol. 122, no. 1 (1994), 79-84.

[4] T. Breuer, CTblLib, - GAP's Character Table Library package, version 1.2.1, (2012), http://www.math.rwth-aachen.de/ ˜Thomas.Breuer/ctbllib

[5] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.7; 2017. (http://www.gap-system.org).

[6] D. Gorenstein, Finite Groups, AMS Chelsea Publishing, second edition, (1980).

[7] G. Hajós, Covering multidimensional spaces by cube lattices, Mat. Fiz. Lapok. 45 (1938), 171-190 (in Hungarian).

[8] G. Hajós, Über einfache und merfache Bedeckung des $n$-dimensionalen Raumes mit einem Würfelgitter, Math. Zeit. 47 (1942), 427-467.

[9] K. Corradi, P.Z. Hermann, and S. Szabó, On factorizations of nonabelian groups, Acta Sci. Math. (Szeged), 67, (2001), 529–533.

[10] W. Lempken, T.V. Trung, On minimal logarithmic signatures of finite groups. Experiment. Math. 14 (2005), no. 3, 257–269.

[11] M.W. Liebeck , C.E. Praeger, J. Saxl, "The maximal factorizations of the finite simple groups and their automorphism groups", Memoirs of the American Mathematical Society, (1990), vol 86, 1-151.

[12] S. S. Magliveras, A cryptosystem from logarithmic signatures of finite groups, in Proceedings of the 29'th Midwest Symposium on Circuits and Systems, Elsevier Publ. Co. (1986), 972–975.

[13] H. Minkowski, Geometrie der Zahlen, Teubner, Leipzig, 1896.

[14] S. Szabó, A.D. Sands, Factoring Groups into Subsets, Lecture notes in pure and applied mathematics, Chapman & Hall / CRC, (2009).

(Dan Levy) The School of Computer Sciences, The Academic College of Tel-Aviv-Yaffo, 2 Rabenu Yeruham St., Tel-Aviv 61083, Israel
*E-mail address*: danlevy@mta.ac.il

(Attila Maróti) Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Reáltanoda utca 13-15, H-1053, Budapest, Hungary
*E-mail address*: maroti.attila@renyi.mta.hu