Scripta Fac. Sci. nat. UJEP Brunensis
Arch. math. 1, VII: 23—28, 1971

CONTRIBUTIONS TO THE THEORY OF DECOMPOSITIONS ON A GROUP

OLDŘICH COUFAL

Received March 6, 1970

1. INTRODUCTION

If we consider, besides a group G, even a group A, which is a subgroup of the group of all automorphisms of G, we can form a so called A-decomposition on G. Article 2 deals with the properties of classes of an A-decomposition and with relations between A-decompositions in dependence on A. Article 3 concerns relations between A-decompositions and subgroups admissible with respect to A. The last three articles deal with the relation between the right and left cosets of a subgroup.

In this paper G denotes a group with automorphism group $A(G)$ and inner automorphism group $I(G)$. All the expressions that deal with decompositions are taken from [1]. Especially, if $\bar{F}, \bar{H}$ are decompositions on G, the infimum and the supremum of $\bar{F}$, $\bar{H}$ will be denoted by $(\bar{F}, \bar{H})$ or $[\bar{F}, \bar{H}]$, respectively. Decompositions $\bar{F}$, $\bar{H}$ are commuting if for every two elements $\bar{f} \in \bar{F}$, $\bar{h} \in \bar{H}$; $\bar{f}$, $\bar{h} \subset \bar{u}$, $\bar{u} \in [\bar{F}, \bar{H}]$, there holds $\bar{f} \cap \bar{h} \neq \emptyset$. A cover of a set M in a decomposition $\bar{F}$, $M \sqsubset \bar{F}$, is the set of all elements of $\bar{F}$ which are coincident with M. The elements $\bar{f}$, $\bar{g} \in \bar{F}$ can be connected in $\bar{H}$, when there exists a finite sequence of elements in $\bar{F}, \bar{f}_1, \bar{f}_2, \ldots, \bar{f}_n$ $(n \geqq 2)$ with the properties: $\bar{f}_1 = \bar{f}, \bar{f}_n = \bar{g}; \bar{f}_r, \bar{f}_{r+1}$ $(r = 1, 2, \ldots, n-1)$ are always coincident with the same element $\bar{h}_r \in \bar{H}$.

2. A-DECOMPOSITION AND ITS PROPERTIES

Let A be an arbitrary subgroup of $A(G)$.

The mapping associating with each element $g \in G$ the set gA of all elements $g\alpha$, $\alpha \in A$, is an equivalence relation on G. The decomposition belonging to this equivalence relation will be called A-decomposition of G and noted $\bar{A}$.

The product of two classes $\bar{g}_1, \bar{g}_2 \in \bar{A}$ consists of some classes of the decomposition $\bar{A}$. In fact, if $g_1 \in \bar{g}_1$, $g_2 \in \bar{g}_2$, $\alpha \in A$, then $(g_1 g_2)\, \alpha = g_1\alpha \,.\, g_2\alpha$, i.e. an element, which is an image of an element of $\bar{g}_1\bar{g}_2$ is also contained in this product.

If $\bar{g} \in \bar{A}$, then $\bar{g}^s \in \bar{A}$ ($\bar{g}^s$ is the set of s-powers of the elements of $\bar{g}$). Indeed, if $h = g\alpha$, then $h^s = g^s\alpha$ i.e. $\bar{g}^s$ is a part of some element of $\bar{A}$ and, according to the previous paragraph, we have $\bar{g}^s \in \bar{A}$.

Let $M \subset G$ be an arbitrary nonempty set. Let $N(M)$ be the set of all automorphisms of $A(G)$ which map M onto M. $N(M)$ is a subgroup of $A(G)$. If $g \in G$, then there evidently holds

$$\text{card } gA = \text{card } A/_r(N(\mathrm{g}) \cap A).$$

Let G be a finite group of order n. Let an A-decomposition of G be formed by the classes $\bar{g}_0, \bar{g}_1, \ldots, \bar{g}_k$. Among these classes there is also the class of elements in which the identity e of G is contained; let us suppose it is $\bar{g}_0$. This class $\bar{g}_0$ contains only one element e. The number h_i of elements in the class $\bar{g}_i$ $(i = 1, 2, \ldots, k)$ is equal to $card\ A/_r(N(g_i) \cap A)$, where g_i is an arbitrary element contained in $\bar{g}_i$. According to Lagrange's theorem about the index of a subgroup, h_i is a divisor of the order of A. There holds the so called classes equation

$$n = 1 + h_1 + h_2 + \ldots + h_k.$$

Thus order n of a finite group G is a sum of some divisors of the order of A.

Let A, B be subgroups of $A(G)$. Let us denote $A \cap B = \Pi$, $\{A, B\} = \Sigma$. We have evidently

Theorem 1. If $A \subset B$, then $\bar{A} \leqq \bar{B}$.

Theorem 2. $\bar{A} = \bar{B}$ holds if, and only if, the equation

$$(\bar{N}_1 =) \quad A \sqsubset A(G)/_r N(g) = B \sqsubset A(G)/_r N(g) \quad (= \bar{N}_2)$$

holds for all $g \in G$.

Proof. If $\bar{A} = \bar{B}$, then to every element $g \in G$ and every automorphism $\alpha \in A$ $(\beta \in B)$ there exists $\beta' \in B$ $(\alpha' \in A)$ with the property $g\alpha = g\beta'$ $(g\beta = g\alpha')$. This implies in the first case $g\alpha\beta'^{-1} = g$, $g\beta'\alpha^{-1} = g$, whence $\alpha\beta'^{-1}$, $\beta'\alpha^{-1} \in N(g)$ and finally $N(g)\,\alpha = N(g)\,\beta'$. Analogously $N(g)\,\beta = N(g)\,\alpha'$ in the second case. This completes the proof of the equality $\bar{N}_1 = \bar{N}_2$. Conversely, since $\bar{N}_1 = \bar{N}_2$, there exists to every element $g \in G$ and every automorphism $\alpha \in A$ $(\beta \in B)$ an automorphism $\beta' \in B$ $(\alpha' \in A)$, $\beta' \in N(g)\alpha$ $(\alpha' \in N(g)\beta)$, hence $g\alpha = g\beta'$ $(g\beta = g\alpha')$; $\bar{A} = \bar{B}$.

Example. Let a group G be determined by generators a, b, c and defining relations $a^8 = b^8 = c^4 = e$, $b^{-1}ab = a^5$, $c^{-1}ac = a^5$, $c^{-1}bc = a^6b$. The automorphism $\alpha\colon a \to a^5$, $b \to b$, $c \to c$ is an outer automorphism of G and maps every class of conjugate elements of G onto itself ([2] p. 107). Evidently, the decompositions belonging to groups $I(G)$, $\{I(G), \alpha\}$ are equal.

The relations $\Pi \subset A$, $\Pi \subset B$, theorem 1 and the properties of the infimum of decompositons imply $\bar{\Pi} \leqq (\bar{A}, \bar{B})$. We shall demonstrate the case $\bar{\Pi} \neq (\bar{A}, \bar{B})$.

Example. Let us consider the same group as in the above example. We put $A = \{\alpha\}$, $B = I(G)$. The group A has two elements, the identity automorphism ε and the outer automorphism α, hence $\Pi = (A \cap B) = \{\varepsilon\}$. Every class of $\bar{\Pi}$ contains only one element of the group G. α maps every class of conjugate elements onto itself, therefore $\bar{B} \geqq \bar{A}$, $(\bar{A}, \bar{B}) = \bar{A}$. The class $aA \in \bar{A}$ contains two elements a, a^5, therefore $\bar{\Pi} \neq \bar{A} = (\bar{A}, \bar{B})$.

Theorem 3. $[\bar{A}, \bar{B}] = \bar{\Sigma}$.

Proof. The relations $A \subset \Sigma$, $B \subset \Sigma$, theorem 1 and the properties of the supremum of decompositions imply $[\bar{A}, \bar{B}] \leqq \bar{\Sigma}$. Now we shall prove that $[\bar{A}, \bar{B}] \geqq \bar{\Sigma}$ is true. If $g \in G$, then there exist $\bar{u} \in [\bar{A}, \bar{B}]$, $\bar{s} \in \bar{\Sigma}$; $\bar{u} \cap \bar{s} \neq \emptyset$, $g \in (\bar{u} \cap \bar{s})$. The class $\bar{s}$ is equal to $g\Sigma$. Considering that Σ is generated by A and B, every element $\sigma \in \Sigma$ can be expressed in the form $\sigma = \beta_1\alpha_1\beta_2\alpha_2 \ldots \beta_n\alpha_n$, where n is an integer, $\alpha_i \in A$, $\beta_i \in B$; $i = 1, 2, \ldots, n$. If the product on the right-hand side of the last equality does not begin with an element from B or does not end with an element from A, we put $\beta_1 = \varepsilon$ or $\alpha_n = \varepsilon$, where ε is the identity automorphism. Let us denote $g\sigma = g_n$. There exist elements $k_i \in \bar{s}$, $g_i \in \bar{s}$; $k_{i-1}\beta_i = k_i$ $(k_0 = g)$, $k_i\alpha_i = g_i$ and classes $\bar{k}_i \in \bar{B}$, $\bar{g}_i \in \bar{A}$, $\bar{g} \in \bar{A}$; $\bar{k}_i \subset \bar{s}$, $\bar{g}_i \subset \bar{s}$, $\bar{g} \subset \bar{s}$; $g_{i-1} \in \bar{k}_i$ $(g_0 = g)$, $k_i \in \bar{g}_i$, $g \in \bar{g}$, $g_n \in \bar{g}_n$.

Hence $k_i \in \bar{k}_i$, $g_i \in \bar{g}_i$. Therefore the classes $\bar{g}_{i-1}$, $\bar{g}_i$ ($\bar{g}_0 = \bar{g}$) have common elements with the class $\bar{k}_i$; i.e. every two classes of the decomposition $\bar{A}$ which are contained in $\bar{s}$ can be connected with the class $\bar{g} \in \bar{A}$ in the decomposition $\bar{B}$. But the class $\bar{g}$ is in $\bar{u}$ ($\bar{A} \leqq [\bar{A}, \bar{B}]$) and, according to the definition of the supremum of decompositions, all classes of $\bar{A}$ which can be connected with $\bar{g}$ in $\bar{B}$ are included in $\bar{u}$ ([1] p. 14). Hence $\bar{s} \subset \bar{u}$ and also $\bar{\Sigma} \leqq [\bar{A}, \bar{B}]$. This relation together with $[\bar{A}, \bar{B}] \leqq \bar{\Sigma}$ complete the proof.

Theorem 4. Let A, B be subgroups of $A(G)$. The decompositions $\bar{A}$, $\bar{B}$ are commuting if, and only if,

$$(\bar{N}_1 =) \quad AB \sqsubset A(G)/_r N(g) = BA \sqsubset A(G)/_r N(g) \quad (= \bar{N}_2)$$

holds for every $g \in G$.

Proof. Let the decompositions $\bar{A}$, $\bar{B}$ be commuting. Choose arbitrary $g \in G$, $\alpha \in A$, $\beta \in B$. $N(g)\alpha\beta \in \bar{N}_1$. Let us denote $h = g\alpha\beta$; since $\bar{A}$, $\bar{B}$ are commuting, the classes $gB \in \bar{B}$, $hA \in \bar{A}$ coincide because g, h are in the same class of the decomposition $\bar{\Sigma}$, where $\Sigma = \{A, B\}$. There exist automorphisms $\alpha' \in A$, $\beta' \in B$ such that $h = g\beta'\alpha'$, hence for g the equality $g\alpha\beta = g\beta'\alpha'$ is true. Therefore $\beta'\alpha' \in N(g)\alpha\beta$, i.e. $N(g)\alpha\beta = N(g)\beta'\alpha'$. $N(g)\beta'\alpha' \in \bar{N}_2$, so that $\bar{N}_1 \leqq \bar{N}_2$. Analogously, one can prove $\bar{N}_2 \leqq \bar{N}_1$. Thus $\bar{N}_1 = \bar{N}_2$.

Now suppose that $\bar{N}_1 = \bar{N}_2$. We shall prove that $\bar{A}$, $\bar{B}$ are commuting decompositions. Let $gA \in \bar{A}$, $hB \in \bar{B}$ be two classes which are contained in one and the same class of $\bar{\Sigma}$. There exist elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$; $\beta_1, \beta_2, \ldots, \beta_n \in B$ with the property $h = g(\alpha_1\beta_1\alpha_2\beta_2 \ldots \alpha_n\beta_n)$. The supposition implies $\alpha\beta = \nu\beta'\alpha'$ ($\bar{\beta}\bar{\alpha} = \bar{\nu}\alpha''\beta''$) for every two elements $\alpha \in A$, $\beta \in B$ ($\bar{\alpha} \in A$, $\bar{\beta} \in B$), where $\bar{\nu} \in N(g)$, $\beta' \in B$, $\alpha' \in A$ ($\nu \in N(g)$, $\alpha'' \in A$, $\beta'' \in B$) are convenient elements. Therefore the product $\alpha_1\beta_1 \ldots \alpha_n\beta_n$ can be expressed in the form $\nu\alpha\beta$, where $\nu \in (N)g$; $\alpha \in A$; $\beta \in B$. Hence $h = g(\alpha_1\beta_1 \ldots \alpha_n\beta_n) = g(\nu\alpha\beta) = g\nu(\alpha\beta) = g\alpha\beta$ which implies $g\alpha \in (gA \cap hB)$, which is what we were to prove.

3. ADMISSIBLE SUBGROUPS AND A-DECOMPOSITIONS

Let A be a subgroup of $A(G)$. A nonempty subset $H \subset G$ is called admissible with respect to A, in short, admissible, if $H\alpha = H$ holds for every $\alpha \in A$. A decomposition $\bar{H}$ in G is called admissible with respect to A, if to every element $\bar{h} \in \bar{H}$ and to every automorphism $\alpha \in A$ there exists an element $\bar{g} \in \bar{H}$ with the property $\bar{g} = \bar{h}\alpha$. If $H \subset G$ is an admissible subgroup, then the decompositions $G/_l H$, $G/_r H$ are admissible. Obviously $(gA)\ \alpha = gA$ holds for every class $gA \in \bar{A}$ and for every automorphism $\alpha \in A$, i.e. every admissible subset is a union of some classes of the decomposition A. A subgroup of G, generated by an admissible subset of G, is an admissible subgroup. Indeed, every element of $\{M\alpha\}$ is an element of $\{M\}\ \alpha$ and conversely, hence $\{M\}\ \alpha = \{M\alpha\} = \{M\}$, because $M\alpha = M$.

A group G is called A-simple, if G and $\{e\}$ are its only admissible subgroups with respect to A. From the above considerations there follows: A group G is A-simple if, and only if, $G = \{gA\}$ for every $g \in G$, $g \neq e$.

Let G be of order n. The order of every admissible subgroup H with respect to A is equal to a sum of the number 1 and some of the summands h_1 upto h_k from the classes equation, since H contains the identity of G and since H contains all $g\alpha$, $\alpha \in A$ for every $g \in H$.

Theorem 1. Let K be an arbitrary subgroup of G. Then

$$H = \bigcap_{\alpha \in A} K\alpha, \qquad F = \{\bigcup_{\alpha \in A} K\alpha\}$$

are the admissible subgroups of G, H is the greatest admissible subgroup of G contained in K, and F is the least admissible subgroup of G containing K.

Proof. Let H' be a union of the classes of the decompositon $\bar{A}$ which are contained in K. $H' \neq \emptyset$, since the class containing the only element $e \in G$ is always in $\bar{A}$. H' is admissible and $H' \subset K\alpha$ for every $\alpha \in A$; thus $H' \subset H$. Since H cannot contain other elements than the elements of H', we have $H = H'$. Therefore H is an admissible subgroup of G and evidently H is the greatest admissible subgroup of G contained in K.

Let F' be a union of all classes of $\bar{A}$ which are coincident with K. F' is the admissible subset consisting of the elements $k\alpha$; $k \in K$, $\alpha \in A$. Evidently $F' = \bigcup_{\alpha \in A} K\alpha$. An admissible subgroup containing K necessarily contains F'. The least of such subgroups is $\{F'\} = F$.

Theorem 2. If F is an arbitrary admissible subgroup of G, then the decompositions $\bar{A}$, $G/_lF$ and $\bar{A}$, $G/_rF$ are commuting.

Proof. The statement will be proved only for $G/_lF$. The proof for $G/_rF$ is analogical. Put $\bar{U} = [\bar{A}, G/_lF]$. Let $\bar{u} \in \bar{U}$, $g_1F \in G/_lH$, $g_nF \in G/_lF$, $\bar{k} \in \bar{A}$; $g_1F \subset \bar{u}$, $g_nF \subset \bar{u}$, $\bar{k} \subset \bar{u}$, $g_1F \cap \bar{k} \neq \emptyset$ be arbitrary classes. It is sufficient to prove $g_nF \cap \bar{k} \neq \emptyset$. g_1F can be connected with g_nF in $\bar{A}$ ([1] p. 14) i.e. there exists such a sequence $g_1F, g_2F, \ldots, g_nF$, that every two classes g_iF, $g_{i+1}F$ $(i = 1, 2, \ldots, n-1)$ are coincident with the same class $\bar{k}_i \in \bar{A}$. The statement is obvious if $n = 1$. We shall proceed by induction on n. Let $n \geqq 2$, $g_jF \cap \bar{k} \neq \emptyset$ for $j = 1, 2, \ldots, n-1$. We shall prove $g_nF \cap \bar{k} \neq \emptyset$. The classes $g_{n-1}F$, g_nF are coincident with $\bar{k}_{n-1} \in \bar{A}$. Since $g_{n-1}F \cap \bar{k} \neq \emptyset$, there exists an element $k \in (g_{n-1}F \cap \bar{k})$, therefore $g_{n-1}F = kF$. Further, there exists $f \in F$ and $\alpha \in A$ such that $kf \in (\bar{k}_{n-1} \cap g_{n-1}F)$, $(kf)\,\alpha \in (\bar{k}_{n-1} \cap g_nF)$. Hence $g_nF = (kf)\,\alpha \,.\, F = (k\alpha \,.\, f\alpha)\, F = k\alpha(f\alpha \,.\, F)$, but $f\alpha \,.\, F = F$ (F is admissible), therefore $g_nF = k\alpha \,.\, F$. Since $k\alpha \in \bar{k}$, we have $k\alpha \in (\bar{k} \cap g_nF)$, i.e. $\bar{k} \cap g_nF \neq \emptyset$, and the theorem is proved.

4. COMMON ELEMENTS OF TWO DECOMPOSITIONS INDUCED BY SUBGROUPS

Let F, H be subgroups of G. Let $gF = gH$ or $Fg = Hg$ hold for some element $g \in G$; every such equality implies $F = H$. So, if F, H are different subgroups of G, then the decompositions $G/_lF$, $G/_lH$ or G_r/F, G_r/H have no common elements.

Suppose that $Fg = gH$ is a common element of the decompositions $G/_rF$, $G/_lH$. The equality $Fg = gH$ implies $H = g^{-1}Fg$. Conversely, if F, H are conjugate subgroups, then there exists an element $g \in G$ with the property $H = g^{-1}Fg$ and the decompositions $G/_rF$, $G/_lH = G/_lg^{-1}Fg$ have the common element $Fg = g(g^{-1}Fg) = gH$. Therefore the decompositions $G/_rF$, $G/_lH$ have a common element if, and only if, the subgroups F, H are conjugate. If $H = g^{-1}Fg$, then $H = (ng)^{-1}F(ng) = g^{-1}Fg$, where n is an arbitrary element of the normalizer N of F in G. Also $Fng = ngH$ for every $n \in N$. $Fn_1g = Fn_2g$ for $n_1, n_2 \in N$ if, and only if, $Fn_1 = Fn_2$.

We conclude

$$\text{card } (G/_r F \cap G/_l H) = \text{card } N/_r F$$

and the common elements of the decompositions $G/_r F$, $G/_l H$ form the set Ng.

5. THE INFIMUM OF DECOMPOSITIONS $G/_l F$ AND $G/_r H$

Put $P = (G/_l F, G/_r H)$. Let $g \in G$ be an arbitrary element. Let us consider the cosets $gF \in G/_l F$, $Hg \in G/_r H$. If we denote $D = g^{-1}Hg \cap F$, then $gF \cap Hg = gD$. The equality $g_1^{-1}Hg_1 = g^{-1}Hg_2$ holds if, and only if, the elements $g_1, g_2 \in G$ are contained in the same right coset of the normalizer N of H. Therefore the intersections of elements of $G/_l F$ and $G/_r H$ in the same right coset of N are equal to some left cosets of D. Hence

$$\bar{P} = \bigcup_{g \in G} [Ng \sqsubset G/_l(F \cap g^{-1} Hg)].$$

6. THE SUPREMUM OF DECOMPOSITIONS $G/_l F$ AND $G/_r H$

$[G/_l F, G_r/H]$ is the set of all double cosets HgF $(g \in G)$. The decompositions $G/_l F$, $G/_r H$ are commuting ([1] p. 147). Let $g \in G$ be an arbitrary element. $\bar{F} = HgF \sqsubset \sqsubset G/_l F$, $\bar{H} = HgF \sqsubset G/_r H$ are decompositions on HgF. Let us denote $D = g^{-1}Hg \cap \cap F$. According to [2] p. 25, there is

$$\text{card } \bar{H} = \text{card } F/_r D$$

$$\text{card } \bar{F} = \text{card } g^{-1}Hg/_l D.$$

Choose $F = H$, then $D = g^{-1}Fg \cap F$. If $\bar{F}_l = FgF \sqsubset G/_l F$, $\bar{F}_r = FgF \sqsubset G/_r F$, then

$$\text{card } \bar{F}_r = \text{card } F/_r D$$

$$\text{card } \bar{F}_l = \text{card } g^{-1}Fg/_l D.$$

If F is a finite subgroup of G, then $g^{-1}Fg$, D are also finite subgroups. By Lagrange's theorem the decompositions $F/_r D$, $g^{-1}Fg/_l D$ and also $\bar{F}_r$, $\bar{F}_l$ have the same number of elements. If F is not finite, the relation *card* $\bar{F}_r =$ *card* $\bar{F}_l$ is not necessarily true.

Example. Let G be the group of permutations of the set of integers. $M \subset G$ consists of permutations

$$(1, 2), (2, 3), \ldots, (n, n + 1), \ldots \qquad n > 0.$$

Put $F = \{M\}$, $g = (\ldots, -k, \ldots, -2, -1, 0, 1, 2, \ldots, k, \ldots)$, then

$$g^{-1}(n, n + 1)\, g = (n + 1, n + 2)$$

i.e. $g^{-1}Mg$ is a proper subset of M. Evidently, $g^{-1}Fg = \{g^{-1}Mg\}$ is a proper subgroup of F ([3] p. 70), hence $D = g^{-1}Fg \cap F = g^{-1}Fg$. There holds

$$\text{card } \bar{F}_r = \text{card } F/_r g^{-1}Fg > 1$$

$$\text{card } \bar{F}_l = \text{card } g^{-1}Fg/_l g^{-1} Fg = 1.$$

REFERENCES

[1] **Borůvka** O., *Grundlagen der Grupoid - und Gruppentheorie*. Berlin 1960
[2] **Hall** M., *The theory of groups* (Russian translation). Moscow 1962
[3] **Kurosh** A. G., *The theory of groups* (in Russian). Moscow 1967

Ústav speciální elektroenergetiky
FE VUT, Brno, Božetěchova 2,
Czechoslovakia