Factorizations in finite groups

Vik. S. Kulikov

Abstract. A necessary condition for uniqueness of factorizations of elements of a finite group $G$ with factors belonging to a union of some conjugacy classes of $G$ is given. This condition is sufficient if the number of factors belonging to each conjugacy class is big enough. The result is applied to the problem on the number of irreducible components of the Hurwitz space of degree $d$ marked coverings of $\mathbb{P}^1$ with given Galois group $G$ and fixed collection of local monodromies.

Bibliography: 9 titles.

Keywords: factorization semigroups, irreducible components of the Hurwitz space of coverings of the projective line.

Introduction

Let $f : X \to \mathbb{P}^1$ be a morphism of a nonsingular irreducible projective curve $X$ (defined over the field of complex numbers $\mathbb{C}$) onto the projective line $\mathbb{P}^1$. Denote by $\mathbb{C}(X)$ the field of rational functions on $X$. The morphism $f$ defines a finite extension $f^* : \mathbb{C}(z) \hookrightarrow \mathbb{C}(X)$ of the field of rational functions $\mathbb{C}(\mathbb{P}^1) \simeq \mathbb{C}(z)$. Denote by $G$ the Galois group of this extension.

Let us choose a point $z_0 \in \mathbb{P}^1$ such that $z_0$ is not a branch point of $f$ and number the points in $f^{-1}(z_0) = \{w_1, \ldots, w_d\}$, where $d = \deg f$. We will call the morphism $f$ with fixed numbering of the points of $f^{-1}(z_0)$ a marked covering.

Let $z_1, \ldots, z_n \in \mathbb{P}^1$ be the set of branch points of $f$. The numbering of the points in $f^{-1}(z_0)$ defines a homomorphism $f_* : \pi_1(\mathbb{P}^1 \setminus \{z_1, \ldots, z_n\}, z_0) \to \Sigma_d$ from the fundamental group $\pi_1 = \pi_1(\mathbb{P}^1 \setminus \{z_1, \ldots, z_n\}, z_0)$ to the symmetric group $\Sigma_d$. The image $\text{im} f_*$ acts transitively on $f^{-1}(z_0)$ and it is isomorphic to $G$ (so we can identify $\text{im} f_*$ and $G$). Let $\gamma_1, \ldots, \gamma_n$ be simple loops around, respectively, the points $z_1, \ldots, z_n$ starting at $z_0$ and such that they generate the group $\pi_1$. The image $g_j = f_*(\gamma_j) \in G$ is called a local monodromy of $f$ at the point $z_j$. Note that the set $\{g_1, \ldots, g_n\}$ of local monodromies generates the group $G$. The local monodromy $g_j$ depends on the choice of $\gamma_j$, therefore it is defined uniquely up to conjugation in $G$. Denote by $O = C_1 \sqcup \cdots \sqcup C_m \subset G$ the union of conjugacy classes.
of all local monodromies and by $\tau_i$ the number of local monodromies of $f$ belonging to the conjugacy class $C_i$. The pair $(G, O)$ is called an equipped group and the collection $\tau = (\tau_1 C_1, \ldots, \tau_m C_m)$ is called the monodromy type of $f$.

Let $\text{HUR}^m_{d,G,\tau}(\mathbb{P}^1)$ be the Hurwitz space (see the definition of Hurwitz spaces in [1]) of marked degree $d$ coverings of $\mathbb{P}^1$ with Galois group $G$ and monodromy type $\tau$. The famous Clebsch-Hurwitz Theorem ([2], [3]) states that if $G = \Sigma_d$ and $O$ is the set of transpositions, then $\text{HUR}^m_{d,\Sigma_d,\tau}(\mathbb{P}^1)$ consists of a single irreducible component if $\tau = (nO)$ with even $n \geq 2(d - 1)$ and it is empty otherwise. Generalizations of the Clebsch-Hurwitz Theorem were obtained in [4] and [5]. In particular, in [5] it was proved that for an equipped group $(\Sigma_d, O)$ with $O = C_1 \sqcup \cdots \sqcup C_m$, where $C_1$ is the conjugacy class of an odd permutation leaving fixed at least two elements, the Hurwitz space $\text{HUR}^m_{d,\Sigma_d,\tau}(\mathbb{P}^1)$ is irreducible if $\tau_1$ is big enough. On the other hand, the example in [6] shows that $\text{HUR}^m_{8,\Sigma_3,\tau}(\mathbb{P}^1)$ consists of two irreducible components at least, where $\tau = (1C_1, 1C_2, 1C_3)$ and $C_1$ is the conjugacy class of the permutation $(1,2)(3,4,5)$, $C_2$ is the conjugacy class of $(1,2,3)(4,5,6,7)$, and $C_3$ is the conjugacy class of $(1,2,3,4,5,6,7)$. Therefore we cannot expect that for a fixed equipped group $(G, O)$ the number of irreducible components of $\text{HUR}^m_{d,G,\tau}(\mathbb{P}^1)$ does not depend on the monodromy type $\tau$. But, we can expect that this number does not depend on $\tau$ if $\tau_i$ is big enough for some $i$ such that the elements of $C_i$ generate the group $G$.

In § 2.5, for each equipped finite group $(G, O)$ such that the elements of $O$ generate $G$, we define an ambiguity index $a_{(G, O)}$ depending on $G$ and $O$. As a straightforward corollary of Theorems 6 and 7 (see § 4.2) and results of [4], we have the following result.

**Theorem 1.** For each equipped finite group $(G, O)$, $O = C_1 \sqcup \cdots \sqcup C_m$ such that the elements of $O$ generate the group $G$ there is a constant $T$ such that the number of irreducible components of each nonempty Hurwitz space $\text{HUR}^m_{d,G,\tau}(\mathbb{P}^1)$ is equal to $a_{(G, O)}$ if $\tau_i \geq T$ for all $i = 1, \ldots, m$.

If the elements of $O_1 = C_1 \sqcup \cdots \sqcup C_k$ for some $k < m$ generate the group $G$, then there is a constant $T_1$ such that the number of irreducible components of $\text{HUR}^m_{d,G,\tau}(\mathbb{P}^1)$ is no more than $a_{(G, O_1)}$ if $\tau_i \geq T_1$ for $i = 1, \ldots, k$.

This article is a continuation of [4], in which the investigation of the factorization semigroups over finite groups was started. For the convenience of the reader, the main definitions and useful statements from [4] are recalled in § 1. In § 2, with each equipped group $(G, O)$, we associate a $C$-group whose factorization semigroup is the same as the factorization semigroup of $(G, O)$ and we investigate a connection between this $C$-group and $(G, O)$. In § 3, we prove the stability of the factorization semigroups over $C$-finite groups. Theorem 2, proved in this section, plays the key role in the proof of all main results of this article (see § 4). In § 5, we give a solution of the word problem for $C$-finite groups and give an algorithm of computation of the ambiguity index $a_{(G, O)}$ for an equipped finite group $(G, O)$.

The author is grateful to O. V. Kulikova who drew his attention to the important role of the van Kampen Lemma in geometric group theory. It is only due to the Lemma that it was possible to prove Theorem 2.
§ 1. Semigroups over groups

1.1. Factorization semigroups. A pair \((G, O)\), where \(G\) is a group and \(O\) is a subset of \(G\) invariant under the inner automorphisms, is called an equipped group. In the sequel, we will assume that \(1 \not\in O\) and \(O\) consists of a finite number of conjugacy classes \(C_i\) of \(G\), \(O = C_1 \sqcup \cdots \sqcup C_m\), and the numbering of these conjugacy classes is fixed.

A homomorphism \(f: G_1 \to G_2\) is called a homomorphism of equipped groups \((G_1, O_1)\) and \((G_2, O_2)\) if \(f(O_1) \subseteq O_2\).

The semigroup \(S(G, O)\) generated by the letters of the alphabet \(X = X_O = \{x_g \mid g \in O\}\) being subject to the relations

\[
x_{g_1} \cdot x_{g_2} = x_{g_2} \cdot x_{g_1}^{-1} g_1 g_2 = x_{g_1 g_2 g_1^{-1}} \cdot x_{g_1},
\]

is called the factorization semigroup with factors in \(O\) (or a factorization semigroup over the group \(G\)). A homomorphism

\[
\alpha = \alpha_G: S(G, O) \to G,
\]

given by \(\alpha(x_g) = g\) for each \(x_g \in X\) is called the product homomorphism. We will denote by \(g_1 \cdots g_n\) the image \(\alpha(x_{g_1} \cdots x_{g_n})\) of \(s = x_{g_1} \cdots x_{g_n} \in S(G, O)\).

The action \(\rho\) of the group \(G\) on the set \(X\) given by

\[
x_a \in X \mapsto \rho(g)(x_a) = x_{gag^{-1}} \in X,
\]

defines a homomorphism \(\rho: G \to \text{Aut}(S(G, O))\). The action \(\rho(g)\) on \(S(G, O)\) is called the simultaneous conjugation by \(g \in G\). Put \(\lambda(g) = \rho(g^{-1})\) and \(\lambda_S = \lambda \circ \alpha\), \(\rho_S = \rho \circ \alpha\).

Claim 1 ([4]). For all \(s_1, s_2 \in S(G, O)\) we have

\[
s_1 \cdot s_2 = s_2 \cdot \lambda_S(s_2)(s_1) = \rho_S(s_1)(s_2) \cdot s_1.
\]

With each element \(s = x_{g_1} \cdots x_{g_n} \in S(G, O)\) let us associate a positive integer \(\ln(s) = n\) called the length of \(s\). It is easy to see that

\[\ln: S(G, O) \to \mathbb{Z}_{\geq 0} = \{a \in \mathbb{Z} \mid a \geq 0\}\]

is a homomorphism of semigroups.

With each element \(s = x_{g_1} \cdots x_{g_n} \in S(G, O)\), we associate a subgroup \(G_s\) of \(G\) generated by the images \(\alpha(x_{g_1}) = g_1, \ldots, \alpha(x_{g_n}) = g_n\) of the factors \(x_{g_1}, \ldots, x_{g_n}\), and denote by \(G_O\) the subgroup of \(G\) generated by the elements of \(O\).

Claim 2 ([4]). The subgroup \(G_s\) of \(G\) is well defined, that is, it does not depend on a presentation of \(s\) as a product of generators \(x_{g_i} \in X_O\).

For subgroups \(H\) and \(Z\) of a group \(G\), we put

\[
S(G, O)_H = \{s \in S(G, O) \mid G_s = H\}, \quad S(G, O)_Z = \{s \in S(G, O) \mid \alpha(s) \in Z\}, \quad S(G, O)_Z^H = S(G, O)_Z \cap S(G, O)_H.
\]

It is easy to see that \(S(G, O)_H\) (respectively \(S(G, O)_Z^H\)) is isomorphic to the semigroup \(S(H, H \cap O)_H\) (respectively, isomorphic to \(S(H, H \cap O)_Z^H\)) and the isomorphism is induced by the embedding \((H, H \cap O) \hookrightarrow (G, O)\).
Proposition 1 ([4]). Let \((G,O)\) be an equipped group and let \(s \in S(G,O)\). We have

1. \(\ker \rho\) coincides with the centralizer \(C_O\) of the group \(G_O\) in \(G\);
2. if \(\alpha(s)\) belongs to the centre \(Z(G_s)\) of \(G_s\), then for each \(g \in G_s\) the action \(\rho(g)\) leaves fixed the element \(s \in S(G,O)\);
3. if \(\alpha(s \cdot x_g)\) belongs to the centre \(Z(G_{s \cdot x_g})\) of \(G_{s \cdot x_g}\), then \(s \cdot x_g = x_g \cdot s\);
4. if \(\alpha(s) = 1\), then \(s \cdot s' = s' \cdot s\) for any \(s' \in S(G,O)\).

Claim 3 ([4]). For any equipped group \((G,O)\) the semigroup \(S(G,O)_1\) is contained in the centre of the semigroup \(S(G,O)\) and, in particular, it is a commutative subsemigroup.

It is easy to see that if \(g \in O\) is an element of order \(n\), then \(x^n_g \in S(G,O)_1\).

Lemma 1 ([4]). Let \(s \in S(G,O)\) and let \(s_1 \in S(G,O)\) be such that \(G_{s_1} = G_O\), where \(Z(G_O)\) is the centre of \(G_O\). Then

\[ s \cdot s_1 = \rho(g)(s) \cdot s_1 \]

for all \(g \in G_O\).

In particular, if \(s \in S(G,O)\) is such that \(G_s = G\) and \(C \subset O\) is a conjugacy class of \(G\), then for any \(g_1, g_2 \in C\) we have

\[ x^n_{g_1} \cdot s = x^n_{g_2} \cdot s \]

if \(g^n_1\) belongs to the centre \(Z(G)\) of \(G\).

Proposition 2 ([4]). The elements of \(S(G,O)_1^G\) are fixed under the conjugation action of \(G\).

§ 2. C-groups and C-graphs

2.1. C-graphs of C-groups. Recall the definition of C-groups. By definition (see, for example, [7]), a C-group \(G\) is an equipped group \((G,O)\) such that the elements of \(O\) are the generators (so called, C-generators) of the group \(G\) being subject to the relations

\[ g_i^{-1}g_jg_i = g_k, \quad (g_i, g_j, g_k) \in M, \]

where \(M\) is a subset of \(O^3\). A homomorphism \(f : G_1 \to G_2\) of C-groups is called a C-homomorphism if it is a homomorphism of equipped groups. In particular, two C-groups \(G_1\) and \(G_2\) are C-isomorphic if they are isomorphic as equipped groups.

With each C-group, let us associate a directed graph, called a C-graph. To give a definition of C-graphs, consider a directed graph \(\Gamma = (V,E)\), where \(V\) is the set of vertices of \(\Gamma\) and the set of its edges \(E\) is a collection \(\{e_{v_i,v_j} = (v_i, v_j)\}\) of ordered pairs of its vertices (some of the edges can be loops, that is, the equality \(v_i = v_j\) is allowed). For each vertex \(v \in V\), let us denote by \(T_v = \{e_{v,v_i}\}\) (resp., \(H_v = \{e_{v_i,v}\}\)) the set of edges whose tails (resp., heads) are the vertex \(v\). A directed graph \(\Gamma\) is called a C-graph if each edge \(e \in E\) is labelled by an element of \(V\) (that is, a map \(f : E \to V\) such that the label of \(e \in E\) is \(f(e) \in V\), is fixed; in the sequel, an edge \(e_{v_1,v_2}\) with label \(f(e_{v_1,v_2}) = v\) will be denoted by \(e_{v_1,v_2,v}\) and, in addition, \(\Gamma\) is such that the following five conditions are satisfied:
(i) for each vertex \( v \in V \) the restrictions \( f|_{T_v}, f|_{H_v} \) of the map \( f \) to \( T_v \) and \( H_v \) are one to one correspondences with \( V \);
(ii) for each vertex \( v \) the head \( v_1 \) of the edge \( e_{v,v_1,v} \) is the vertex \( v \), that is, \( e_{v,v_1,v} \) is the loop \( (v_1 = v) \).

Note that, by condition (i), the tail (resp., the head) \( v_1 \) and the label \( v_2 \) uniquely define the edge \( e \) whose tail (resp., head) is \( v_1 \) and whose label is \( v_2 \). Therefore a sequence \( v_1, \ldots, v_n \) and a tail \( v_0 \) uniquely define a path \( l(v_0; v_1, \ldots, v_n) \) starting at the vertex \( v_0 \) along edges (in the positive direction) with labels \( v_1, \ldots, v_n \).

(iii) If for some two vertices \( v_1 \) and \( v_2 \) the edge \( e_{v_1,v_3,v_2} \) is a loop, that is, \( v_1 = v_3 \), then the edge \( e_{v_2,v_4,v_1} \) is also a loop \( (v_2 = v_4) \);
(iv) for any edge \( e_{v_1,v_2,v_3} \) and for any vertex \( v \) the ends of the paths \( l(v; v_1, v_3) \) and \( l(v; v_3, v_2) \) coincide.

With each labelled directed graph \( \Gamma \), let us associate a two-dimensional complex \( K_\Gamma \) whose 1-skeleton is \( \Gamma \) and whose two-cells are the quadrangles \( Q(v,e_{v_1,v_2,v_3}) \) one to one corresponding to the pairs \( (v,e_{v_1,v_2,v_3}) \in V \times E \) such that the border \( \partial Q(v,e_{v_1,v_2,v_3}) \) of \( Q(v,e_{v_1,v_2,v_3}) \) is the loop \( l(v; v_1, v_3) \cdot l(v; v_3, v_2)^{-1} \).

The fifth condition is

(v) if for some two edges \( e_{v_1,v_2,v_3} \) and \( e_{v_1,v_2,v_3} \) the loop \( e_{v_1,v_2,v_3} \cdot e_{v_1,v_2,v_3}^{-1} \) represents the unity of the fundamental group \( \pi_1(K_\Gamma,v) \), then \( v_2 = v_3 \).

With each \( C \)-group \( (G,O) \), one can associate a \( C \)-graph. By definition, the \( C \)-graph \( \Gamma = \Gamma_{(G,O)} \) of a \( C \)-group \( (G,O) \) is a \( C \)-graph whose set of vertices \( V = \{v_g, | g \in O\} \) is in one to one correspondence with the set \( O \). Two vertices \( v_{g_1} \) and \( v_{g_2} \), \( g_1,g_2 \in O \), are connected by a labelled edge \( e_{v_{g_1},v_{g_2},v_g} \) if and only if in \( G \) we have a relation \( g^{-1}g_1g = g_2 \) with some \( g \in O \).

Conversely, with each \( \Gamma \)-graph \( \Gamma^* \) one can associate a \( C \)-group \( G_\Gamma = (G,Y) \) the set of \( C \)-generators \( Y = \{y_{v_i} | v_i \in V \} \) of which is in one to one correspondence with the set \( V \) of vertices of \( \Gamma \). In \( G_\Gamma \) there is a relation \( y_{v_3}^{-1}y_{v_1}y_{v_3} = y_{v_2} \) if and only if there is an edge \( e_{v_1,v_2,v_3} \).

**Claim 4.** For each \( C \)-graph \( \Gamma \), the \( C \)-group \( G_\Gamma \) is \( C \)-isomorphic to \( G_{\Gamma^*} \).

For each \( C \)-group \( G \), the \( C \)-graphs \( \Gamma_G \) and \( G_{\Gamma_G} \) are isomorphic.

The proof is obvious.

In the sequel, for a \( C \)-group \( G_\Gamma \) the generators \( x_{y_v}, v \in \Gamma \), of the semigroup \( S(G_\Gamma,Y) \) will be denoted by \( x_v \).

We say that a subgraph \( \Gamma_1 \) of a \( C \)-graph \( \Gamma \) is a \( C \)-subgraph if \( \Gamma_1 \) is a \( C \)-graph.

Let \( \Gamma_1 \) be a \( C \)-subgraph of a \( C \)-graph \( \Gamma \). Consider the \( C \)-groups \( (G,Y) = G_\Gamma \) and \( (G_1,Y_1) = G_{\Gamma_1} \) and their factorization semigroups \( S(G,Y) \) and \( S(G_1,Y_1) \). The embedding \( i: \Gamma_1 \hookrightarrow \Gamma \) defines the natural homomorphism \( i_*: G_{\Gamma_1} \rightarrow G_\Gamma \) of \( C \)-groups and the homomorphism \( i_*: S(G_1,Y_1) \rightarrow S(G,Y) \) of their factorization semigroups given, respectively, by \( i_*(y_{v_i}) = y_{v_i} \) and \( i_*(x_{v_i}) = x_{v_i} \) for \( v_i \in \Gamma_1 \hookrightarrow \Gamma \).

**Claim 5.** Let \( \Gamma_1 \) be a \( C \)-subgroup of a \( C \)-graph \( \Gamma \). Then the homomorphism \( i_*: S(G_{\Gamma_1},Y_1) \rightarrow S(G_\Gamma,Y) \) is an embedding.

The proof is obvious.

For each \( C \)-graph \( \Gamma \) a homomorphism from the \( C \)-group \( G_\Gamma \) to the automorphism group of \( \Gamma \) is defined as follows: the action of the \( C \)-generator \( y_v \) is given by the
rule: for a vertex \( v \) of \( \Gamma \) the image \( y_{v'}(v) \) is the head of the edge with tail \( v \) and label \( v' \), while for an edge \( e_{v_1,v_2,v_3} \) the image is \( y_{v'}(e_{v_1,v_2,v_3}) = e_{y_{v'}(v_1), y_{v'}(v_2), y_{v'}(v_3)} \). It follows from conditions (i)–(v) in the definition of \( C\)-graphs that this action is well defined.

In the sequel, we will consider only finitely generated \( C\)-groups (as groups without equipment) and \( C\)-graphs consisting of finitely many connected components. Denote by \( m \) the number of connected components of a \( C\)-graph \( \Gamma \). Then it is easy to see that \( G_\Gamma/[G_\Gamma, G_\Gamma] \cong \mathbb{Z}^m \) and any two \( C\)-generators \( y_{v_1} \) and \( y_{v_2} \) are conjugated in the \( C\)-group \( G_\Gamma \) if and only if \( v_1 \) and \( v_2 \) belong to the same connected component of \( \Gamma \), that is, the set \( Y \) of \( C\)-generators of the \( C\)-group \( G_\Gamma \) is the union of \( m \) conjugacy classes of \( G_\Gamma \). Denote by ab: \( G_\Gamma \to H_1(G_\Gamma, \mathbb{Z}) = G_\Gamma/[G_\Gamma, G_\Gamma] \) the natural epimorphism. In the sequel, we will assume that some numbering of the connected components of \( \Gamma \) is fixed. In this case the group \( H_1(G_\Gamma, \mathbb{Z}) \cong \mathbb{Z}^m \) has the natural basis consisting of the vectors \( a(y_v) = (0, \ldots, 0, 1, 0 \ldots, 0) \), where 1 stands on the \( i \)th place if \( v \) belongs to the \( i \)th connected component of \( \Gamma \). Denote the composition \( ab \circ \alpha_{G_\Gamma} \) by \( \tau \).

Let \( l = l(v_0; v_1, \ldots, v_n) \) be a path in a \( C\)-graph \( \Gamma \). The number \( n \) is called the length of \( l \). The smallest positive integer \( p_v \) (maybe, \( p_v = \infty \)) such that for any vertex \( v \) of \( \Gamma \) the path \( l(v; v, \ldots, v) \) of length \( p_v \) is a loop with origin and end at \( v \), is called the period of \( v \). It is easy to see that \( p_v = \min\{p \in \mathbb{N} \mid y_v^p \in Z(G_\Gamma)\} \), where \( Z(G_\Gamma) \) is the centre of \( G_\Gamma \).

**Claim 6.** If \( v_1 \) and \( v_2 \) belong to the same connected component of a \( C\)-graph \( \Gamma \), then \( p_{v_1} = p_{v_2} \).

**Proof.** The elements \( y_{v_1} \) and \( y_{v_2} \) are conjugated in \( G_\Gamma \). Therefore, if \( y_{v_1}^{p_{v_1}} \in Z(G_\Gamma) \) then \( y_{v_1}^{p_{v_1}} = y_{v_1}^{p_{v_2}} \) and hence \( y_{v_1}^{p_{v_1}} \in Z(G_\Gamma) \).

**Claim 7.** If a vertex \( v_1 \) of a \( C\)-graph \( \Gamma \) is such that its period \( p_{v_1} = 1 \), then the \( C\)-group \( G_\Gamma \) is naturally isomorphic to the direct product \( G_{\Gamma_1} \times \mathbb{F}_1 \), where \( \mathbb{F}_1 \) is a free group generated by \( y_v \) and the \( C\)-group \( G_{\Gamma_1} \) is generated by all the \( C\)-generators \( y_v \), where \( v \neq v_1 \), and it is associated with \( C\)-graph \( \Gamma_1 \) obtained from \( \Gamma \) by deleting the vertex \( v_1 \) and all the edges labelled by \( v_1 \).

The proof is obvious.

A \( C\)-group \( G_\Gamma \) is called a \( C\)-finite group if the \( C\)-graph \( \Gamma \) is a finite graph.

Let \( \Gamma = \Gamma_1 \sqcup \cdots \sqcup \Gamma_m \) be the decomposition into the disjoint union of the connected components of a finite \( C\)-graph \( \Gamma \) and let \( p_i \) be the period of the set of vertices \( V_i = \{v_{i,1}, \ldots, v_{i,n_i}\} \) of the connected component \( \Gamma_i \). The element

\[
c = \prod_{i=1}^{m} p_i \prod_{j=1}^{n_i} y_{v_{i,j}}^{p_i}
\]

is called the canonical element of the \( C\)-group \( G_\Gamma \).

**Proposition 3.** Let \( G_\Gamma \) be a \( C\)-finite group. Then the commutator \([G_\Gamma, G_\Gamma]\) is a finite group. Moreover, each element \( g \in [G_\Gamma, G_\Gamma] \) can be written in the form

\[
g = c^{-1} \prod_{i=1}^{m} y_{i,1}^{k_{1,i}} y_{i,2}^{a_{i,1}} \cdots y_{i,n_i}^{a_{i,n_i}},
\]  

(5)
where $c$ is the canonical element of $G_\Gamma$ and the integers $k_i$ and $a_{i,j}$ satisfy the following relations and inequalities

$$\sum_{j=1}^{n_i} a_{i,j} + k_ip_i = n_ip_i, \quad (6)$$

$$0 < a_{i,j} \leq p_i, \quad 0 \leq k_i < n_i. \quad (7)$$

**Proof.** Applying relations (4) and since $y_{i,j}^{p_i} = y_{i,1}^{p_i}$, each element $g \in [G, G]$ can be written in the form

$$g = \prod_{i=1}^{m} y_{i,1}^{k_i} y_{i,1}^{b_{i,1}} y_{i,2}^{b_{i,2}} \cdots y_{i,n_i}^{b_{i,n_i}}, \quad (8)$$

where the integers $k_i$ and $b_{i,j}$ satisfy the following relations and inequalities

$$\sum_{j=1}^{n_i} b_{i,j} + k_ip_i = 0, \quad (9)$$

$$|b_{i,j}| \leq p_i - 1, \quad |k_i| < n_i. \quad (10)$$

For fixed integers $p_i$ and $n_i$ the set of integer solutions of equations (9) under restrictions (10) is finite. Therefore $[G_\Gamma, G_\Gamma]$ is a finite group. To obtain presentation (5) from (8), it suffices to multiply presentation (8) of $g$ by $c^{-1}c$ and once more to use the relations $y_{i,j}^{p_i} = y_{i,1}^{p_i}$.

### 2.2. Canonical elements of factorization semigroups.

In the notations used above, the element

$$s_\Gamma = \prod_{i=1}^{k} \prod_{j=1}^{n_i} x_{v_{i,j}}^{p_i} \in S(G, Y)$$

is well defined and it is called the canonical element associated with the subgraph $\Gamma' = \Gamma_{i_1} \sqcup \cdots \sqcup \Gamma_{i_k}$ of the $C$-graph $\Gamma$. If $\Gamma' = \Gamma$, then the element $s_\Gamma$ is called the canonical element of the semigroup $S(G, Y)$. Obviously, $s_\Gamma$ belongs to the centre of $S(G, Y)$ since each factor $x_{v_{i,j}}^{p_i}$ of it belongs to the centre of $S(G, Y)$.

An element $s_1 \in S(G, Y)$ is said to be a divisor of an element $s \in S(G, Y)$ if there is $s_2 \in S(G, Y)$ such that $s = s_1 \cdot s_2$.

**Lemma 2.** An element $s \in S(G, Y)$ of length $\ln(s) \leq k$ is a divisor of $s_\Gamma^k$, if $s$ can be represented as a word in the generators $x_{v_{i,j}}$, where $v_{i,j} \in \Gamma'$.

The proof of Lemma 2 is obvious.

**Lemma 3.** Let $G_\Gamma = (G, Y)$ be a $C$-finite group. Let the $i$th coordinate $\tau_i(s)$ of $\tau(s)$ for an element $s = s' \cdot s'' \in S(G, Y)^G$ be no less than $n_ip_i + 1$. Assume that $\tau_i(s'') = 0$. Then for $1 \leq j \leq n_i$ the element $s$ can be written in the form

$$s = x_{v_{i,j}}^{p_i} \cdot s_i \cdot s'', \quad \text{where } s_i \cdot s'' \in S(G, Y)^G.$$

**Proof.** Since $\tau_i(s) \geq n_ip_i + 1$, for given $i$ there are at least $p_i + 1$ factors $x_{v_{i,j}}$ in a factorization of $s'$, $s' = x_{v_{i,j_1}} \cdots x_{v_{i,j_k}}$ having the same $j$. Applying relations (1), we can move them to the left and after that we obtain a new factorization $s' = x_{v_{i,j}}^{p_i} \cdot (x_{v_{i,j}} \cdot s_i')$. Obviously, $s_i \cdot s'' := (x_{v_{i,j}} \cdot s_i') \cdot s''$ belongs to $S(G, Y)^G$ since $s \in S(G, Y)^G$.

Applying Lemma 1, we complete the proof.
Corollary 1. Let \( G_\Gamma = (G,Y) \) be a \( C \)-finite group. Let, for an element \( s = s' \cdot s'' \in S(G,Y)^G \), the \( i \)th coordinate \( \tau_i(s) \) be no less than \( 2n_i p_i + 1 \). Assume that \( \tau_i(s') = 0 \). Then the element \( s \) can be written in the form \( s = s_{\Gamma_i} \cdot s_i \cdot s'' \), where \( s_i \cdot s'' \in S(G,Y)^G \).

2.3. Ample subgraphs of \( C \)-graphs. Let \( \Gamma' \) be a union of some connected components of a \( C \)-graph \( \Gamma \). We say that \( \Gamma' \) is ample if any two vertices belonging to any connected component of \( \Gamma \) can be connected by a path along edges of \( \Gamma \) labelled by vertices belonging to \( \Gamma' \). In the language of \( C \)-groups, this means that any two conjugated \( C \)-generators of \( G_\Gamma \) are conjugated by some element of the subgroup \( G_{\Gamma'} \) of \( G_\Gamma \) generated by the \( C \)-generators \( y_v, v \in \Gamma' \). Note that \( G_{\Gamma'} \) is the image of the \( C \)-group \( G_{\Gamma'} \) under the \( C \)-homomorphism \( i_* : G_{\Gamma'} \to G_\Gamma \) given by the embedding \( i : \tilde{\Gamma'} \hookrightarrow \Gamma \), where \( \tilde{\Gamma'} \) is the \( C \)-subgraph of \( \Gamma \) obtained from \( \Gamma' \) after deleting all edges labelled by the vertices \( v \not\in \Gamma' \).

The \( C \)-group \( G_\Gamma \) acts on \( \Gamma \). Therefore the homomorphism \( i_* \) defines an action of \( G_{\Gamma'} \) on \( \Gamma \) leaving fixed each connected component of \( \Gamma \). It is easy to see that if \( \Gamma' \) is ample then \( G_{\Gamma'} \) acts transitively on the set of vertices of each connected component of \( \Gamma \).

Lemma 4. Let a union \( \Gamma' \) of some connected components of a finite \( C \)-graph \( \Gamma \) be ample and let \( v_o, v_e \) be two vertices belonging to a connected component, say \( \Gamma_1 \), of \( \Gamma \). Then there is a path \( l(v_o; v_1, \ldots, v_n) \) connecting \( v_o \) and \( v_e \) such that \( v_1, \ldots, v_n \) are vertices of \( \Gamma' \).

Proof. Let \( V_1 \) be the set of vertices of \( \Gamma_1 \). For \( v \in V_1 \) denote by \( V_1(v) \) the set of all vertices \( v' \in V_1 \) such that for \( v' \) there is a path \( l(v; v_1, \ldots, v_n) \) connecting \( v \) and \( v' \) such that \( v_1, \ldots, v_n \) are vertices of \( \Gamma' \). We say that \( v \leq v' \) if \( v' \in V_1(v) \). It is easy to see that \( V_1(v) \subseteq V_1(v') \) if \( v' \subseteq v \). Therefore the set of subsets \( V_1(v) \subseteq V_1 \), \( v \in V_1 \), is partially ordered under inclusions and hence there is a maximal one, say \( V_1(\bar{v}) \), since \( \Gamma \) is a finite graph.

Next, it is easy to see that the \( C \)-group \( G_{\tilde{\Gamma}'} \) acts on the set of subsets \( V_1(v) \subseteq V_1 \), \( v \in V_1 \), by the rule: \( y_{v_1}(V_1(v)) = V_1(y_{v_1}(v)) \) for a \( C \)-generator \( y_{v_1} \in G_{\tilde{\Gamma}'} \). Therefore for a maximal subset \( V_1(\bar{v}) \) we have \( V_1(\bar{v}) = V_1(v) \) for all \( v \in V_1(\bar{v}) \) since \( G_{\tilde{\Gamma}'} \) acts transitively on \( V_1 \). Hence, \( V_1(\bar{v}) \) can be represented as the disjoint union \( V_1(\bar{v}_1) \sqcup \cdots \sqcup V_1(\bar{v}_m) \) of maximal subsets \( V_1(\bar{v}_i) \). Finally, since \( \Gamma' \) is ample and \( \Gamma_1 \) is connected, we obtain that \( m = 1 \).

Let a union \( \Gamma' \) of some connected components of a finite \( C \)-graph \( \Gamma \) be ample and let \( \Gamma_1 \) be a connected component of \( \Gamma \). By definition, the distance \( d_{\Gamma'}(v_o, v_e) \) between two vertices \( v_o, v_e \) of \( \Gamma_1 \) with respect to \( \Gamma' \) is the smallest \( n \) such that there is a path \( l(v_o; v_1, \ldots, v_n) \) connecting \( v_o \) and \( v_e \) such that \( v_1, \ldots, v_n \) are vertices of \( \Gamma' \). The number \( d_{\Gamma'}(\Gamma_1) = \max_{v_o, v_e \in V_1} d_{\Gamma'}(v_o, v_e) \) is called the diameter of \( \Gamma_1 \) with respect to \( \Gamma' \).

Proposition 4. Let \( G_\Gamma = (G,Y) \) be a \( C \)-finite group, \( \Gamma' = \Gamma_1 \sqcup \cdots \sqcup \Gamma_k \) an ample subgraph of \( \Gamma \) and \( \Gamma \setminus \Gamma' = \Gamma_k+1 \sqcup \cdots \sqcup \Gamma_m \), where \( \Gamma_i, i = 1, \ldots, m, \) are the connected components of \( \Gamma \). Denote

\[
d = d_{\Gamma'} = \max(d_{\Gamma'}(\Gamma_1), \ldots, d_{\Gamma'}(\Gamma_m)).
\]
Let an element \( s \in S(G,Y)^G \) be such that \( \tau_i(s) \geq 2n_ip_id + 1 \) for all \( i \leq k \), where \( \tau_i(s) \) is the \( i \)th coordinate of \( \tau(s) \). Then the element \( s \) can be written in the form
\[
s = (x_{v_{k+1}}^{a_{k+1}} \cdots x_{v_m}^{a_m}) \cdot s_{\Gamma'}^d \cdot s_1,
\]
where \( a_i = \tau_i(s) \) for \( i = k+1, \ldots, m \) and \( s_1 \in S(G,Y) \) is such that \( \tau_i(s_1) = 0 \) for \( i = k+1, \ldots, m \).

**Proof.** Let us write the element \( s \) in the form \( s' \cdot s'' \) where \( s' \) and \( s'' \) are such that \( \tau_i(s') = 0 \) for \( i \geq k+1 \) and \( \tau_i(s'') = 0 \) for \( i \leq k \). Then, by Corollary 1, the element \( s \) can be written in the form \( s = \tilde{s}' \cdot s_{\Gamma'}^d \cdot s'' \).

Let for some \( j \) a letter \( x_{v_{m+j}} \) enter \( s'' \). Connect the vertex \( v_{m,1} \) with \( v_{m,j} \) by a path \( l(v_{m,1}; v_1, \ldots, v_r) \) of length \( r \leq d \) (recall that \( \Gamma' \) is ample, therefore by Lemma 4, \( v_{m,1} \) and \( v_{m,j} \) can be connected by such a path), where \( v_1, \ldots, v_r \) are some vertices of \( \Gamma' \), and write \( s'' = x_{v_{m,j}} \cdot \tilde{s}'' \). By Lemma 2, \( s_{\Gamma'}^d = s' \cdot (x_{v_1} \cdots x_{v_r}) \) for some \( \tilde{s} \). We have \( \alpha(x_{v_1} \cdots x_{v_r}) = y_{v_1} \cdots y_{v_r} \) and by definition of \( C \)-graphs of \( C \)-groups, we have \( (y_{v_1} \cdots y_{v_r})y_{v_{m,j}}(y_{v_1} \cdots y_{v_r})^{-1} = y_{v_{m,1}} \). Therefore,
\[
s_{\Gamma}' \cdot x_{v_{m,j}} = \tilde{s} \cdot (x_{v_1} \cdots x_{v_r}) \cdot x_{v_{m,j}} = \tilde{s} \cdot x_{v_{m,1}} \cdot (x_{v_1} \cdots x_{v_r}),
\]
and hence (after moving \( x_{v_{m,1}} \) to the right)
\[
s = s'_1 \cdot s_{\Gamma'}^d \cdot s'' = s'_1 \cdot \tilde{s} \cdot x_{v_{m,1}} \cdot (x_{v_1} \cdots x_{v_r}) \cdot \tilde{s}'' = s'_1 \cdot s''_1 \cdot x_{v_{m,1}},
\]
where \( s'_1 \) is such that \( \tau_i(s'_1) = 0 \) for \( i \geq k+1 \) and \( \tau_i(s'_1) \geq 2n_i p_i d + 1 \) for all \( i \leq k \), and \( s''_1 \) is such that \( \tau_i(s''_1) = 0 \) for \( i \leq k \).

Applying Corollary 1, Claim 5 and Lemma 2, we can repeat \( a_m - 1 \) times the transformation described above and we obtain a factorization \( s = s'_{a_m} \cdot s''_{a_m} \cdot x_{v_{m,1}}^{a_m} \).

After that, for \( i = m-1, \ldots, k+1 \), we can repeat the transformation described above and we obtain a factorization \( s = s'_{a_m+a_m-1} \cdot s''_{a_m+a_m-1} \cdot x_{v_{m,1}}^{a_m-1} \cdot x_{v_{m,1}}^{a_m} \). Finally, we move the obtained product \( (x_{v_{k+1}}^{a_{k+1}} \cdots x_{v_m}^{a_m}) \) to the left and apply Corollary 1 to complete the proof.

### 2.4. **C-graphs of equipped groups.**

With each equipped group \((G,O)\), one can associate a \( C \)-graph. By definition, the **\( C \)-graph** \( \Gamma = \Gamma(G,O) \) of an equipped group \((G,O)\) is the \( C \)-graph whose set of vertices is in one to one correspondence with the set \( O \). Two vertices \( v_{g_1} \) and \( v_{g_2} \), \( g_1, g_2 \in O \), are connected by the labelled edge \( e_{v_{g_1},v_{g_2},v_g} \) if and only if \( g^{-1} g_{1} g = g_2 \) for some \( g \in O \).

**Example 1.** To describe the \( C \)-graph \( \Gamma(\Sigma_n,T_n) \) of the equipped symmetric group \((\Sigma_n,T_n)\), where \( T_n \) is the set of transpositions, consider an \((n-1)\)-simplex \( \Delta_{n-1} \).

Let \( V_1, \ldots, V_n \) be the vertices of \( \Delta_{n-1} \) and \( E_{i,j} \) its edges connecting the vertices \( V_i \) and \( V_j \). The vertices \( v_{i,j} \) of \( \Gamma(\Sigma_n,T_n) \) are the mid-points of the edges \( E_{i,j} \). If \( E_{i,j} \) and \( E_{k,l} \) are skewed edges, then the edge of \( \Gamma(\Sigma_n,T_n) \) with tail \( v_{i,j} \) and label \( v_{k,l} \) is a loop. The head of the edge with tail \( v_{i,j} \) and label \( v_{j,k} \) is \( v_{i,k} \).

With each equipped group \((G,O)\) we can associate a \( C \)-group \( G_{\Gamma(G,O)} \). Denote the \( C \)-generators \( y_{v_{g_1}} \in Y \), \( g_i \in O \), of the \( C \)-group \( G_{\Gamma(G,O)} \) by \( y_{g_i} \). We have the natural homomorphism of equipped groups \( \beta = \beta(G,O) : G_{\Gamma(G,O)} \rightarrow (G,O) \) given by \( \beta(y_{g_i}) = g_i \) for all \( g_i \in O \). Obviously, \( \beta|_Y : Y \rightarrow O \) is a one to one correspondence.
Claim 8. (i) \( \ker \beta \) is a subgroup of the centre of \( G_{\Gamma(G,O)} \).

(ii) If \((G,O)\) is an equipped group such that \( G \) is generated by the elements of \( O \), then \( \beta \) and \( \beta|_{[G_{\Gamma(G,O)},G_{\Gamma(G,O)}]} : [G_{\Gamma(G,O)},G_{\Gamma(G,O)}] \to [G,G] \) are epimorphisms.

The proof is obvious.

2.5. Equivalence of equipped groups. Let \((G_1,O_1)\) and \((G_2,O_2)\) be two equipped groups such that \( G_1 \) and \( G_2 \) are generated, resp., by the elements of \( O_1 \) and \( O_2 \). We say that \((G_1,O_1)\) and \((G_2,O_2)\) are equivalent if the \( C \)-graphs \( \Gamma(G_1,O_1) \) and \( \Gamma(G_2,O_2) \) are isomorphic as \( C \)-graphs.

Claim 9. Let \((G_1,O_1)\) and \((G_2,O_2)\) be two equivalent equipped groups. Then the \( C \)-graphs \( \Gamma(G_1,O_1) \) and \( \Gamma(G_2,O_2) \) are \( C \)-isomorphic.

This follows from Claim 4.

It follows from Claims 8 and 4 that for each class of equivalent equipped groups corresponding to a \( C \)-graph \( \Gamma \), there is a maximal one, namely, the \( C \)-group \( G_{\Gamma} \) belonging to this class there is an epimorphism of equipped groups, namely \( \beta(G,O) : G_{\Gamma(G,O)} \to (G,O) \), which is defined uniquely by an isomorphism \( \Gamma \simeq \Gamma(G,O) \) and by the following condition: for each \( C \)-generator \( y \) of \( G_{\Gamma} \) the image \( \beta(G,O)(y) = g \in O \) if \( y \) and \( g \) correspond to the same vertex \( v \) of \( \Gamma \simeq \Gamma(G,O) \). By Claim 8, \( \ker \beta(G,O) \) is a subgroup of the centre \( Z(G_{\Gamma}) \) of \( G_{\Gamma} \). The converse statement is also true, namely, an equipped group \((G,O)\) obtained as the quotient group \( G_{\Gamma}/H \) of a \( C \)-group \( G_{\Gamma} \), is equivalent to \( G_{\Gamma}/H \) if \( H \) is a subgroup of \( Z(G_{\Gamma}) \) and it contains neither \( C \)-generators of \( G_{\Gamma} \) nor quotients \( y_i y_j^{-1} \) of \( C \)-generators \( y_i \) and \( y_j \), \( y_i \neq y_j \).

The order \( a_{(G,O)} = |H\cap[G_{\Gamma},G_{\Gamma}]| \) of the group \( H\cap[G_{\Gamma},G_{\Gamma}] \) is called the ambiguity index of the equipped group \((G = G_{\Gamma}/H,O)\) equivalent to \( G_{\Gamma} \).

Proposition 5. Let an equipped group \((G,O)\) be equivalent to a \( C \)-group \( G_{\Gamma} \). If \( G \) is a perfect group, then \( G_{\Gamma} \) is isomorphic to the direct product \([G_{\Gamma},G_{\Gamma}] \times (G_{\Gamma}/[G_{\Gamma},G_{\Gamma}])\).

Proof. For each connected component \( \Gamma_i \) of \( \Gamma \), let us choose a vertex \( v_i \in \Gamma_i \).

The restriction of \( \beta(G,O) \) to \([G_{\Gamma},G_{\Gamma}]\) is an epimorphism onto \( G \) since \( \beta(G,O) \) is an epimorphism and \( G \) is a perfect group. Therefore for each \( C \)-generator \( y_{v_i} \) of \( G_{\Gamma} \), there is an element \( g_i \in [G_{\Gamma},G_{\Gamma}] \) such that \( \beta(G,O)(g_i) = \beta(G,O)(y_{v_i}) \). We have \( y_{v_i} g_i^{-1} \in \ker \beta(G,O) \subseteq Z(G_{\Gamma}) \) and \( ab(y_{v_i} g_i^{-1}) = (0, \ldots, 0, 1, 0, \ldots, 0) \), where \( 1 \) stands on the \( i \)th place. Therefore the elements \( y_{v_i} g_i^{-1} \) generate in \( Z(G_{\Gamma}) \) a free Abelian group \( H \) such that \( a_{(G,O)} = 1 \) is an isomorphism and the proposition follows from the short exact sequence

\[
1 \to [G_{\Gamma},G_{\Gamma}] \to G_{\Gamma} \to G_{\Gamma}/[G_{\Gamma},G_{\Gamma}] \to 1. \tag{11}
\]

Proposition 6. Let an equipped group \((G,O)\) be equivalent to a \( C \)-group \( G_{\Gamma} \). If \( O \) consists of a single conjugacy class, then the group \( G_{\Gamma} \) is isomorphic to the semidirect product \([G_{\Gamma},G_{\Gamma}] \times \mathbb{Z}\).

This follows from exact sequence (11) since \( G_{\Gamma}/[G_{\Gamma},G_{\Gamma}] \simeq \mathbb{Z} \) if \( O \) consists of a single conjugacy class.
Let a subgroup $F$ be generated by the elements $y_i^{k_ip_i} \in Z(G_\Gamma)$, $i = 1, \ldots, m$, where $k_ip_i \geq 2$, $v_i$ is a vertex of the $i$th connected component of the $C$-graph $\Gamma$ and $p_i$ is its period. Then $(G, O) = G_\Gamma/H$ is an equipped group equivalent to $G_\Gamma$ and $\beta_{(G,O)}: [G_\Gamma(G,O), G_\Gamma(G,O)] \rightarrow [G, G]$ is an isomorphism. In particular, $a_{(G,O)} = 1$.

The proof is obvious.

2.6. The type homomorphism. Let $(G, O)$ be an equipped group, $\Gamma = \Gamma_{(G,O)}$ its $C$-graph, and $G_\Gamma$ the $C$-group equivalent to $(G, O)$. The homomorphism $\beta = \beta_{(G,O)}: G_\Gamma \rightarrow (G, O)$ defines a homomorphism of semigroups

$$\beta_*: S(G_\Gamma, Y) \rightarrow S(G, O),$$

given by $\beta_*(x_y) = x_g$ for $g \in O$.

Claim 10. The homomorphism $\beta_*$ is an isomorphism.

The proof is obvious.

In the sequel, in accordance with Claim 10, we will identify the semigroups $S(G, O)$ and $S(G_{\Gamma_{(G,O)}}, Y)$.

The homomorphism of semigroups

$$\tau: S(G, O) = S(G_{\Gamma_{(G,O)}}, Y) \rightarrow \mathbb{Z}_m^n \subset \mathbb{Z}^m = G_{\Gamma_{(G,O)}}/[G_{\Gamma_{(G,O)}}, G_{\Gamma_{(G,O)}}]$$

is called the type homomorphism and the image $\tau(s)$ of $s \in S(G, O)$ is called the type of $s$. If $O$ consists of a single conjugacy class, then the homomorphism $\tau$ can (and will) be identified with the homomorphism $\ln: S(G, O) \rightarrow \mathbb{Z}_{\geq 0}$. In the general case, if $\tau(s) = (\tau_1(s), \ldots, \tau_m(s))$, then $\ln(s) = \sum_{i=1}^m \tau_i(s)$.

An element $g \in G_\Gamma$ is called positive if there is $s \in S(G_{\Gamma}, Y)$ such that $\alpha_{G_\Gamma}(s) = g$.

Lemma 6. Any element $g$ of the $C$-group $G_\Gamma$ can be represented in the form

$$g = g_1g_2^{-1}, \quad (12)$$

where $g_1$ and $g_2$ are positive elements. In particular, $g \in [G_\Gamma, G_\Gamma]$ if and only if $\text{ab}(g_1) = \text{ab}(g_2)$ in representation (12) of $g$ as a quotient of two positive elements $g_1$ and $g_2$.

If $G_\Gamma$ is a $C$-finite group, then for each $g \in G_\Gamma$ there is a presentation (12) of $g$ as a quotient of two positive elements $g_1$ and $g_2$ such that $g_2 = \alpha_{G_\Gamma}(s^n_1)$ for some $n$ and $g_1 = \alpha_{G_\Gamma}(s_1)$ for some $s_1 \in S(G_\Gamma, Y)^{\Gamma_\Gamma}$, where $s^n_1$ is the canonical element of $S(G_\Gamma, Y)$.

Proof. The first part of Lemma 6 is obvious. The second part follows from Lemma 2.

Let $H$ be a subgroup of the centre of a $C$-finite group $G_\Gamma$. Denote by $z_H$ the minimal exponent $n$ such that each element $g \in H \cap [G_\Gamma, G_\Gamma]$ has presentation (12) in which $g_2 = \alpha_{G_\Gamma}(s^n_1)$.
Proposition 7. Let \( G_\Gamma = (G,Y) \) be a \( C \)-finite group, \( \Gamma' = \Gamma_1 \sqcup \cdots \sqcup \Gamma_k \subset \Gamma \) be an ample subgraph of \( \Gamma \), and \( \tilde{\Gamma}' \) the \( C \)-graph defined by \( \Gamma' \). Then
\[
i_*|_{[G_{\tilde{\Gamma}'},G_{\tilde{\Gamma}'}]} : [G_{\tilde{\Gamma}'},G_{\tilde{\Gamma}'}] \to [G_\Gamma,G_\Gamma]
\]
is an epimorphism.

This follows from Proposition 4 and Lemma 6.

Corollary 2. Let \( G_\Gamma \) and \( G_{\tilde{\Gamma}'} \) be \( C \)-finite groups equivalent respectively to equipped groups \((G,O)\) and \((G,O')\), where \( O' \subset O \) are equipments of \( G \) such that the elements of \( O' \) generate the group \( G \). Then \( a_{(G,O)} \leq a_{(G,O')} \); in particular, if \( a_{(G,O')} = 1 \), then \( a_{(G,O)} = 1 \).

§ 3. Stability of factorization semigroups

3.1. Equivalence of elements. Elements \( s_1 \) and \( s_2 \) of a semigroup \( S \) are said to be \( r \)-equivalent (resp., \( l \)-equivalent) if there is an element \( s_3 \in S \) such that \( s_1 \cdot s_3 = s_2 \cdot s_3 \) (resp., \( s_3 \cdot s_1 = s_3 \cdot s_2 \)), and they are equivalent if there are two elements \( s_3, s_4 \in S \) such that \( s_3 \cdot s_1 \cdot s_4 = s_3 \cdot s_2 \cdot s_4 \). The notation \( s_1 \sim s_2 \) (resp., \( s_1 \sim_r s_2 \) and \( s_1 \sim_l s_2 \)) means that elements \( s_1 \) and \( s_2 \) are equivalent (resp., \( r \)-equivalent and \( l \)-equivalent). It is easy to see that if \( s_1 \sim s_2 \), where \( s_1, s_2 \in S(G,O) \), then \( \tau(s_1) = \tau(s_2) \).

Lemma 7. Let \( s_1, s_2 \in S(G,O) \) be two elements of a factorization semigroup over a group \( G \). Then the following statements are equivalent:

(i) \( s_1 \sim_r s_2 \);
(ii) \( s_1 \sim_l s_2 \);
(iii) \( s_1 \sim s_2 \).

Proof. We prove only the implication \( (i) \longrightarrow (ii) \) since the proofs of all other implications are similar.

We have \( s_1 \cdot s_3 = \rho(\alpha_G(s_1))(s_3) \cdot s_1 \) and \( s_2 \cdot s_3 = \rho(\alpha_G(s_2))(s_3) \cdot s_2 \). Since \( \alpha_G \) is a homomorphism, it is easy to see that \( \alpha_G(s_1) = \alpha_G(s_2) \) if \( s_1 \) and \( s_2 \) are \( r \)-equivalent (resp., \( l \)-equivalent or equivalent). Therefore, if \( s_1 \sim_r s_2 \), that is, \( s_1 \cdot s_3 = s_2 \cdot s_3 \) for some \( s_3 \in S(G,O) \), then \( \rho(\alpha_G(s_1))(s_3) \cdot s_1 = \rho(\alpha_G(s_2))(s_3) \cdot s_2 \), that is, \( s_1 \sim_l s_2 \).

Lemma 8. Let \( S(G,O) \) be a factorization semigroup over a group \( G \). Then the relation \( s_1 \sim s_2 \) is an equivalence relation.

Proof. Let \( s_1 \sim s_2 \) and \( s_2 \sim s_3 \). Then, by Lemma 7, there are elements \( s_4 \) and \( s_5 \) such that \( s_4 \cdot s_1 = s_4 \cdot s_2 \) and \( s_2 \cdot s_5 = s_3 \cdot s_5 \). Therefore \( s_4 \cdot s_1 \cdot s_5 = s_4 \cdot s_2 \cdot s_5 = s_4 \cdot s_3 \cdot s_5 \), that is, \( s_1 \sim s_3 \).

Lemma 9. Let \( s_1, s_2, s_3, s_4 \in S(G,O) \) be four elements of a factorization semigroup over a group \( G \). Then \( s_1 \cdot s_2 \sim s_3 \cdot s_4 \) if \( s_1 \sim s_3 \) and \( s_2 \sim s_4 \). If \( s_1 \sim s_3 \sim s_2 \cdot s_4 \) and \( s_1 \sim s_2 \), then \( s_3 \sim s_4 \).

The proof is similar to the proof of Lemma 8.

Theorem 2. Let \( G \) be a \( C \)-group and \( Y \) the set of its \( C \)-generators. Two elements \( s_1 \) and \( s_2 \in S(G,Y) \) are equivalent if and only if \( \alpha_G(s_1) = \alpha_G(s_2) \), where \( \alpha_G \) is the product homomorphism.
Proof. It is obvious that if \( s_1 \sim s_2 \), then \( \alpha_G(s_1) = \alpha_G(s_2) \).

Denote by \( x_i = x_{y_i} \) the generator of \( S(G,Y) \) corresponding to the \( C \)-generator \( y_i \in Y \). Let \( s_1 = x_{i_1} \cdots x_{i_n} \) and \( s_2 = x_{j_1} \cdots x_{j_k} \) be such that \( \alpha_G(s_1) = y_i \cdots y_{i_n} = y_j \cdots y_{j_k} = \alpha_G(s_2) \). Then it is easy to see that \( \tau(s_1) = \tau(s_2) \) and, in particular, \( n = k \). In addition, the word \( w = y_{i_1} \cdots y_{i_n}y_{j_1}^{-1} \cdots y_{j_k}^{-1} \) represents the unity of \( G \).

To prove \( s_1 \sim s_2 \) we will use some admissible transformations of van Kampen diagrams defined over the \( C \)-presentation of \( G \). To define them, recall that by the van Kampen Lemma (see, for example, \([8]\) or \([9]\)), for the word \( w \) there is a van Kampen diagram, that is, a planar finite cell complex \( D \subset \mathbb{R}^2 \) with the following additional data and satisfying the following additional properties:

1) the complex \( D \) is connected and simply connected;

2) each edge (one-cell) of \( D \) is directed and labelled by a letter \( y \in Y \);

3) some vertex (zero-cell) which belongs to the topological boundary \( \partial D \) of \( D \) is specified as a base-vertex \( A \) called the origin of the diagram;

4) each region (two-cell) \( Q \) of \( D \) is a quadrangle corresponding to a \( C \)-relation \( y_iy_j = y_ky_i \) of the \( C \)-presentation of \( G \) (see Fig. 1; the vertex \( v_1 \) will be called the bottom of \( Q \) and the vertex \( v_2 \) will be called the top of \( Q \));

5) the boundary cycle \( \partial D \), that is, an edge-path corresponding to going around once in the clockwise direction along the boundary of the unbounded complementary region of \( D \), starting and ending at the origin \( A \), has the label \( w = y_1 \cdots y_ny_{j_1}^{-1} \cdots y_{j_k}^{-1} \).

Since in our case the word \( w \) splits into two subwords: the first one consists of letters with positive exponents and the other one consists of letters with negative exponents, the van Kampen diagram \( D \) is of the following form: it is a chain of discs connected by simple directed paths (see Fig. 2).

\[
\begin{array}{c}
\text{Figure 1} \\
\begin{tikzpicture}
\node (a) at (0,0) {$v_1$};
\node (b) at (1,1) {$v_2$};
\node (c) at (1,0) {$y_2$};
\node (d) at (0,1) {$y_1$};
\draw (a) -- node[anchor=east]{$y_i$} (b);
\draw (b) -- node[anchor=north]{$y_j$} (c);
\draw (c) -- node[anchor=north]{$y_k$} (d);
\draw (d) -- node[anchor=west]{$y_i$} (a);
\end{tikzpicture}
\end{array}
\]

\[
\begin{array}{c}
\text{Figure 2} \\
\begin{tikzpicture}
\node (a) at (0,0) {$A$};
\node (b) at (3,0) {$B$};
\node (c) at (1.5,1.5) {$\cdots$};
\draw[->] (a) to[out=180,in=90] (b);
\draw[->] (b) to[out=0,in=270] (a);
\draw[->] (a) to[out=90,in=180] (c);
\draw[->] (c) to[out=0,in=90] (a);
\draw[->] (c) to[out=180,in=0] (b);
\end{tikzpicture}
\end{array}
\]

Denote the end vertex of this chain by \( B \) and call it the end of \( D \). Diagrams satisfying conditions 1–5 will be called admissible.
It follows from Lemmas 8 and 9 that it suffices to consider only the case when $D$ consists of a single disc (see Fig. 3).

![Figure 3](image.png)

A vertex $v$ in a van Kampen diagram $D$ is called *locally maximal* (resp., *minimal*) if there is no edge of $D$ for which $v$ is the tail (resp., head). A path $l$ along edges $e_1, \ldots, e_k$ of $D$ is called *increasing* if the tail of each edge $e_{i+1}$ is the head of the edge $e_i$ for $i = 1, \ldots, k - 1$. The label of increasing path $l$ is a positive word $y_{l_1} \ldots y_{l_k}$.

The origin $A$ and the end $B$ divide the boundary $\partial D$ into two parts. The increasing path $\partial_l D$ (resp., $\partial_r D$) along the boundary $\partial D$ connecting $A$ and $B$ and having the label $y_{i_1} \ldots y_{i_n}$ (resp., $y_{j_1} \ldots y_{j_n}$) will be called the *left* (resp., *right*) *side* of $\partial D$.

If the origin $A$ is not a locally minimal vertex of $D$, then there are a locally minimal vertex $C$ and a simple increasing path $l$ connecting the vertices $C$ and $A$. (Note that the vertex $C$ cannot be a vertex belonging to the boundary $\partial D$ since a positive word in $C$-generators cannot represent the unity of a $C$-group.) Then we can cut the disc $D$ along the path $l$ and, as a result, we obtain a new disc diagram $D'$ (see Fig. 4) in which $C$ is the origin and the label of $\partial D'$ is

$$y_{l_1} \ldots y_{l_k} y_{i_1} \ldots y_{i_n} y_{j_1}^{-1} \ldots y_{j_k}^{-1} y_{l_1}^{-1} \ldots y_{l_k}^{-1},$$

where $y_{l_1} \ldots y_{l_k}$ is the label of $l$.

![Figure 4](image.png)

We call the transformation $D \rightsquigarrow D'$ described above an *admissible transformation* I. Note that after transformation I the diagram $D'$ is admissible and the origin $C$ of $D'$ is a locally minimal vertex.
Similarly, if the end $B$ is not a locally maximal vertex of $D$, then there are a locally maximal vertex $C$ and a simple increasing path $l$ connecting $B$ and $C$. Then we can cut the disc $D$ along the path $l$ and, as a result, we obtain a new admissible disc diagram $D'$ in which $C$ is the end and the label of $\partial D'$ is

$$y_{i_1} \cdots y_{i_k} y_{i_{k+1}} \cdots y_{i_n} y_{j_1} \cdots y_{j_n},$$

where $y_{i_1} \cdots y_{i_k}$ is the label of $l$. We call this transformation $D \leadsto D'$ an admissible transformation II. Note that after transformation II the end $C$ of $D'$ is a locally maximal vertex.

Let $v \in \partial l D$ be a vertex of an admissible disc diagram $D$ such that $v$ is neither the origin $A$ nor the end $B$ of $D$ and there is an edge $e$ of $D$, $e \not\subset \partial D$, for which $v$ is the tail. Denote by $y_0$ the label of this edge and let $C$ be its head, $C \not\in \partial D$. Assume for definiteness that $v \in \partial l D$ (the case when $v \in \partial s D$ is similar). Let $y_{i_k}$ (resp., $y_{i_{k+1}}$) be the label of the edge belonging to $\partial D$ for which $v$ is the head (resp., the tail). Let us cut the diagram $D$ along $e$ and after that paste sequentially $n - k$ additional quadrangles as depicted in Fig. 5, where the quadrangle, glued at the $l$th step to the cut disc diagram along the edges labelled by $y_0$ and $y_{i_{k+l}}$ corresponds to the relation $y_{i_{k+l}} y_{i_0} = y_{i_0} y_{i_{k+l}}$, $l = k + 1, \ldots, n - k$, in the $C$-group $G$.

After gluing these quadrangles we obtain a new admissible disc diagram $D'$ whose end is the vertex $B'$ and the label of $\partial D'$ is

$$y_{i_1} \cdots y_{i_k} y_0 y_{i_{k+1}} \cdots y_{i_n}^{-1} y_{j_1}^{-1} \cdots y_{j_n}^{-1}.$$ 

We call the transformation $D \leadsto D'$ described above an admissible transformation III defined by the edge $e$. 

Figure 5
Claim 11. If the elements \( x_{i_1} \cdots x_{i_k} \cdot x_0 \cdot x_{i_{k+1}}' \cdots x_{i_n}' \) and \( x_{j_1} \cdots x_{j_n} \cdot x_0 \), obtained from \( x_{i_1} \cdots x_{i_k} \cdot x_{i_{k+1}} \cdots x_{i_n} \) and \( x_{j_1} \cdots x_{j_n} \) after admissible transformation III defined by the edge \( e \) are equivalent then the elements \( x_{i_1} \cdots x_{i_k} \cdot x_{i_{k+1}} \cdots x_{i_n} \) and \( x_{j_1} \cdots x_{j_n} \) are also equivalent.

The proof is obvious.

Let \( D \) be an admissible disc diagram such that its origin \( A \) is a locally minimal vertex and its end \( B \) is a locally maximal vertex. Let \( C \) be a locally maximal vertex of \( D, C \neq B \). Then \( C \not\in \partial D \) since there is only one locally maximal vertex belonging to \( \partial D \), namely, the end \( B \). We say that \( C \) is visible if there is a vertex \( v \in \partial D, v \neq A \), such that \( v \) can be connected with \( C \) by an increasing path \( l \) along edges of \( D \setminus \partial D \) and such that \( l \cap \partial D = v \). Let the path \( l \) consist of edges \( e_1, \ldots, e_k \) with labels \( y_1, \ldots, y_k \). Perform the sequence of admissible transformations III defined by the edges \( e_1, \ldots, e_k \). As a result, we obtain a new admissible diagram \( D' \) in which the origin \( A \) is a locally minimal vertex, the end \( B' \) is a locally maximal vertex, and the number of locally maximal vertices is strictly less than the number of locally maximal vertices of \( D \). Such a sequence of admissible transformations will be called a transformation decreasing the number of locally maximal vertices.

Let us return to the proof that \( s_1 \sim s_2 \) if \( \alpha_G(s_1) = \alpha_G(s_2) \), where \( s_1 = x_{i_1} \cdots x_{i_n} \) and \( s_2 = x_{j_1} \cdots x_{j_n} \) are two elements of the factorization semigroup \( S(G, Y) \) over a \( C \)-group \( (G, Y) \). Since \( \alpha_G(s_1) = \alpha_G(s_2) \), the word \( w = y_{i_1} \cdots y_{i_n} y_{j_1}^{-1} \cdots y_{j_n}^{-1} \) represents the unity of the group \( G \). Therefore, by the van Kampen Lemma, there is a plane disc diagram \( D \) over the \( C \)-presentation of the group \( G \) whose boundary label is the word \( w \). By Lemmas 8 and 9, as was mentioned above, we can assume that \( D \) is a single disc. Conversely, an admissible disc diagram with boundary label \( w = y_{i_1} \cdots y_{i_n} y_{j_1}^{-1} \cdots y_{j_n}^{-1} \) defines two elements \( s_1(D) = x_{i_1} \cdots x_{i_n} \) and \( s_2(D) = x_{j_1} \cdots x_{j_n} \) of \( S(G, Y) \) such that \( \alpha_G(s_1(D)) = \alpha_G(s_2(D)) \). Note that if \( D \sim D' \) is an admissible transformation I or II, or III, then, by Lemmas 8, 10, and Claim 11, \( s_1(D) \sim s_2(D) \) if and only if \( s_1(D') \sim s_2(D') \). Therefore, without loss of generality, we can assume that \( D \) is an admissible disc diagram such that

(i) the origin \( A \) of \( D \) is a locally minimal vertex;
(ii) the end \( B \) of \( D \) is a locally maximal vertex;
(iii) there is only one visible locally maximal vertex of \( D \), namely, the end \( B \).

Let us show that if an admissible disc diagram \( D \) satisfies conditions (i)–(iii), then \( s_1(D) \sim s_2(D) \). Indeed, if \( D \) consists of a single quadrangle \( Q \), then the origin \( A \) is the bottom of \( Q \) and the end \( B \) is the top of \( Q \). Obviously, in this case we have \( s_1(D) = s_2(D) \) (see Fig. 1).

Now, let \( D \) satisfy conditions (i)–(iii), have \( K \) invisible locally maximal vertices and consist of \( k \) quadrangles. Consider the edge \( e_1 \subset \partial D \) whose tail is \( A \). Let \( v_1 \) be the head of \( e_1 \) and \( Q \) a quadrangle such that \( e_1 \subset \partial Q \). Then the bottom of \( Q \) is the origin \( A \) since \( A \) is a locally minimal vertex. Let \( v_2 \) be the top of \( Q \) and \( e_2 \subset \partial Q \) the edge connecting \( v_1 \) and \( v_2 \).

There are two possibilities: either \( e_2 \subset \partial D \) and hence \( v_2 \in \partial D \), or \( e_2 \notin \partial D \). In the first case if \( y_{j_1} y_{j_2} y_{l_2}^{-1} y_{l_1}^{-1} \) is the label of \( \partial Q \), then

\[
s_1(D) = x_{i_1} \cdot x_{i_2} \cdot (x_{i_3} \cdots x_{i_n}) = x_{i_1} \cdot x_{i_2} \cdot (x_{i_3} \cdots x_{i_n})
\]
and if we cut \(Q\) from \(D\), then we obtain a new admissible diagram \(D'' = D \setminus Q\) having only \(k - 1\) quadrangles and such that \(s_1(D'') = x_{l_1} \cdot x_{l_2} \cdot (x_{i_3} \cdots x_{i_n})\) and \(s_2(D'') = x_{j_1} \cdots x_{j_n}\). Denote also \(Q\) by \(D'\). Note that it is not obligatory that \(D''\) satisfies conditions (i)–(iii). Indeed, if the edge \(e\) of \(Q\) with label \(x_{l_1}\) belongs to \(\partial_r D\), then we must delete it to obtain an admissible disc diagram. Therefore in this case the boundary label of \(\partial D''\) is \(y_{l_2}(y_{i_3} \cdots y_{i_n})y_{j_1}^{-1} \cdots y_{j_2}^{-1}\) (since \(y_{l_1} = y_{j_1}\)) and if the origin of \(D''\) is not a locally minimal vertex of \(D''\), then we must perform a transformation \(I\) which increases neither the number of locally maximal vertices nor the number of quadrangles. Next, it is possible that an invisible locally maximal vertex of \(D\) becomes visible in \(D''\). (It is possible only if \(K > 0\).) But, in this case we can perform an admissible transformation decreasing the number of locally maximal vertices and obtain a new admissible disc diagram having strictly less than \(K\) invisible locally maximal vertices.

If \(v_2 \not\in \partial D\), then there is an edge \(e_3\) in \(D\) whose tail is \(v_2\) since, by assumption, \(v_2\) is not a locally maximal vertex. Let \(v_3\) be the head of \(e_3\). If \(v_3 \not\in \partial D\), then there is an edge \(e_4\) whose tail is \(v_3\), and so on. As a result, we can find an increasing path \(l = (e_2, \ldots e_m)\) connecting the vertex \(v_1\) and a vertex \(v_m\) belonging to \(\partial D\). There are two possibilities: either \(v_m \in \partial_l D\) (see Fig. 6, Case \(l\)) or \(v_m \in \partial_r D\) (see Fig. 6, Case \(r\)). In both cases the path \(l\) divides \(D\) into two disc diagrams \(D'\) and \(D''\) each of which consists of no more than \(k - 1\) quadrangles. If the label of \(l\) is \(y_{l_2} \cdots y_{l_m}\),
then
\[ s_1(D') = x_{i_2} \cdots x_{i_m}, \quad s_2(D') = x_{l_2} \cdots x_{l_m}, \]
\[ s_1(D'') = x_{i_1} \cdot x_{i_2} \cdots x_{i_{m+1}} \cdots x_{i_n}, \quad s_2(D'') = x_{j_1} \cdots x_{j_n} \]
if \( v_2 \in \partial_l D \) and
\[ s_1(D') = x_{i_2} \cdots x_{i_n}, \quad s_2(D') = x_{l_2} \cdots x_{l_m} \cdot x_{j_{m+1}} \cdots x_{j_n}, \]
\[ s_1(D'') = x_{i_1} \cdot x_{i_2} \cdots x_{i_m}, \quad s_2(D'') = x_{j_1} \cdots x_{j_m} \]
if \( v_2 \in \partial_r D \). If the end vertex \( v_m \) of \( D' \) (resp., \( D'' \)) in Case \( l \) (resp., in Case \( r \)) is not locally maximal, then we perform an admissible transformation \( II \) of \( D' \) (resp., \( D'' \)) which increases neither the number of quadrangles nor the number of locally maximal vertices. Similarly, we perform an admissible transformation \( I \) of \( D' \) if its origin \( v_1 \) is not a locally minimal vertex.

To complete the proof of Theorem 2, we use two inductions: the first on the number \( K \) of the invisible locally maximal vertices of admissible disc diagrams satisfying conditions (i)–(iii), and the second on the number \( k \) of quadrangles entering into such diagrams. As it was shown above, in each step of the inductions we can find a path \( l \) dividing the admissible disc diagram \( D \) satisfying conditions (i)–(iii) into two subdiagrams \( D' \) and \( D'' \) such that either (after an admissible transformation) \( D' \) and \( D'' \) have no more than \( K \) invisible locally maximal vertices and have strictly less than \( k \) quadrangles, or \( D' \) and \( D'' \) have strictly less than \( K \) invisible locally maximal vertices (if \( K > 0 \)). By the inductive assumptions, we have \( s_1(D') \sim s_2(D') \) and \( s_1(D'') \sim s_2(D'') \). Therefore, by Lemmas 8 and 9, we have \( s_1(D) \sim s_2(D) \).

3.2. Stability of the factorization semigroups over \( C \)-finite groups. Recall that the factorization semigroup \( S(G, O) \) over an equipped group \( (G, O) \) is called stable if there is an element \( s \in S(G, O) \) such that \( s_1 \cdot s = s_2 \cdot s \) for any two elements \( s_1, s_2 \in S(G, O) \) such that \( \alpha_G(s_1) = \alpha_G(s_2) \) and \( \tau(s_1) = \tau(s_2) \). The element \( s \in S(G, O) \) participating in the definition of a stable semigroup is called the stabilizing element of this semigroup over an equipped group.

Let \( s_1, s_2 \) be two equivalent elements of the factorization semigroup \( S(G, Y) \) of a \( C \)-group \( (G, Y) \). Denote by \( e(s_1, s_2) \) the smallest number \( k \) such that there is an element \( s \in S(G, Y) \) of length \( k \) and such that \( s_1 \cdot s = s_2 \cdot s \).

As above, let \( \Gamma = \Gamma_1 \sqcup \cdots \sqcup \Gamma_m \) be the decomposition of the finite \( C \)-graph of a \( C \)-group \( (G, Y) = G_\Gamma \) into the disjoint union of its connected components, \( V_i = \{v_{i,1}, \ldots, v_{i,n_i}\} \) be the set of vertices of \( \Gamma_i \), and \( p_i \) be the period of the vertices \( v_{i,j} \).

Any element \( s \in S(G, Y) \) can be written in the form \( s = \prod_{v_{i,j} \in \Gamma} x_{v_{i,j}}^{k_{i,j}} \). Consider the set
\[ R = \left\{ s = \prod_{v_{i,j} \in \Gamma} x_{v_{i,j}}^{k_{i,j}} \in S(G, Y) \mid \sum_{j=1}^{n_i} k_{i,j} \leq p_i n_i, \ i = 1, \ldots, m \right\}, \]
and let
\[ E = \{ (s_1, s_2) \in R^2 \mid s_1 \sim s_2 \}. \]
Put\[e_{\Gamma} = \max_{(s_1, s_2) \in E} e(s_1, s_2).\]

**Lemma 10.** We have $s_1 \cdot s_{\Gamma}^e = s_2 \cdot s_{\Gamma}^e$ for all $(s_1, s_2) \in E$, where $s_{\Gamma}^e$ is the canonical element of $S(G, Y)$.

**Proof.** For any $(s_1, s_2) \in E$ there is an element $s_{1,2}$ with $e(s_{1,2}) \leq e_{\Gamma}$ such that $s_1 \cdot s_{1,2} = s_2 \cdot s_{1,2}$. By Lemma 2 there is an element $s'_{1,2}$ such that $s_{1,2} \cdot s'_{1,2} = s_{\Gamma}^e$. Therefore

$$s_1 \cdot s_{\Gamma}^e = s_1 \cdot s_{1,2} = s_2 \cdot s_{1,2} \cdot s'_{1,2} = s_2 \cdot s_{\Gamma}^e.$$  

**Theorem 3.** Let $(G, Y) = G_{\Gamma}$ be a $C$-finite group. Then the semigroup $S(G, Y)$ is stable and $s_{\Gamma}^e$ is a stabilizing element.

**Proof.** Let $s_1, s_2$ be two elements of the factorization semigroup $S(G, Y)$ such that $\alpha_G(s_1) = \alpha_G(s_2)$ and $\tau(s_1) = \tau(s_2)$. Write them in the form

$$s_1 = \prod_{v_{i,j} \in \Gamma} x_{v_{i,j}}^{k_{i,j,1}}, \quad s_2 = \prod_{v_{i,j} \in \Gamma} x_{v_{i,j}}^{k_{i,j,2}}.$$  

Since $\tau(s_1) = \tau(s_2)$, we have

$$\sum_{j=1}^{n_i} k_{i,j,1} = \sum_{j=1}^{n_i} k_{i,j,2}, \quad i = 1, \ldots, m.$$  

If $\sum_{j=1}^{n_i} k_{i,j,1} \geq p_i n_i$ for some $i$, then there is $j_1$ (resp., $j_2$) such that $k_{i,j_1,1} \geq p_i$ (resp., $k_{i,j_2,2} \geq p_i$). If again

$$k_{i,j_1,1} - p_i + \sum_{j=1, j \neq j_1}^{n_i} k_{i,j,1} \geq p_i n_i$$

(resp., $k_{i,j_2,2} - p_i + \sum_{j=1, j \neq j_2}^{n_i} k_{i,j,2} \geq p_i n_i$),

then either there is $j'_1$ (resp., $j'_2$) such that $k_{i,j'_1,1} \geq p_i$ (resp., $k_{i,j'_2,2} \geq p_i$) or $k_{i,j_1,1} - p_i \geq p_i$ (resp., $k_{i,j_2,2} - p_i \geq p_i$). Continuing this process, as a result, we obtain that the elements $s_1$ and $s_2$ can be written in the following form:

$$s_1 = \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{p_i c_{i,j,1} + r_{i,j,1}} = \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{p_i c_{i,j,1}} \right) \cdot \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,1}} \right),$$

$$s_2 = \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{p_i c_{i,j,2} + r_{i,j,2}} = \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{p_i c_{i,j,2}} \right) \cdot \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,2}} \right),$$

where

$$\sum_{i=1}^{m} r_{i,j,1} = \sum_{i=1}^{m} r_{i,j,2} < n_i p_i, \quad i = 1, \ldots, m.$$
and
\[ \sum_{j=1}^{n_i} c_{i,j,1} = \sum_{j=1}^{n_i} c_{i,j,2}, \quad i = 1, \ldots, m. \]

Since \( \alpha_G(x_{v_{i,j}}^{p_i}) = \alpha_G(x_{v_{i,j}}^{p_i}) = y_{v_{i,j}}^{p_i} \) for \( 1 \leq j_1 \leq j_2 \leq n_i \) and for all \( i \) and since \( \alpha_G(s_1) = \alpha_G(s_2) \), we have

\[ \alpha_G \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,1}} \right) = \alpha_G \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,2}} \right). \]

Then by Theorem 2 we have

\[ \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,1}} \sim \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,2}} \]

and by Lemma 10,

\[ \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,1}} \right) \cdot s_{\Gamma}^{e_{\Gamma}} = \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,2}} \right) \cdot s_{\Gamma}^{e_{\Gamma}}. \]

Note that \( s_1 \cdot s_{\Gamma}^{e_{\Gamma}} \) (resp., \( s_2 \cdot s_{\Gamma}^{e_{\Gamma}} \)) belongs to \( S(G,Y)^G \). Therefore, by Lemma 1

\[ s_1 \cdot s_{\Gamma}^{e_{\Gamma}} = \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{p_i(c_{i,j,1})} \right) \cdot \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,1}} \right) \cdot s_{\Gamma}^{e_{\Gamma}} = \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{c_{i,j,1}} \right) \cdot \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,1}} \right) \cdot s_{\Gamma}^{e_{\Gamma}}, \]

\[ s_2 \cdot s_{\Gamma}^{e_{\Gamma}} = \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{p_i(c_{i,j,2})} \right) \cdot \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,2}} \right) \cdot s_{\Gamma}^{e_{\Gamma}} = \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{c_{i,j,2}} \right) \cdot \left( \prod_{i=1}^{m} \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,2}} \right) \cdot s_{\Gamma}^{e_{\Gamma}}, \]

where \( c_i = \sum_{j=1}^{n_i} c_{i,j,1} = \sum_{j=1}^{n_i} c_{i,j,2} \), and hence \( s_1 \cdot s_{\Gamma}^{e_{\Gamma}} = s_2 \cdot s_{\Gamma}^{e_{\Gamma}} \).

**Theorem 4.** Let \( (G,O) \) be an equipped finite group. The semigroup \( S(G,O) \) (resp., \( S(G,O)^G \), \( S(G,O)_1 \), and \( S(G,O)^G_Y \) over the group \( G \) is stable if and only if the ambiguity index \( a_{(G,O)} = 1 \).

**Proof.** The equipped group \( (G,O) \) is equivalent to the \( C \)-finite group \( (G_\Gamma,Y) \), where \( \Gamma = \Gamma_{(G,O)} \), and there is an epimorphism \( \beta_{(G,O)} : G_\Gamma \to G \) such that \( H = \ker \beta \subset Z(G_\Gamma) \). By Claim 9, the semigroups \( S(G,O) \) and \( S(G_\Gamma,Y) \) are naturally isomorphic. Let \( \alpha_{G_\Gamma} \) and \( \alpha_G \) be respectively the product homomorphisms of \( S(G,O) \) to \( G_\Gamma \) and \( G \). Note that, by Theorem 3, for any positive integer \( c \) the element \( s_{\Gamma}^{e_{\Gamma}} \) is a stabilizing element of \( S(G_\Gamma,Y) \) over the group \( G_\Gamma \) and there is a positive integer \( c_0 \) such that \( \alpha_G(s_{\Gamma}^{c_0 e_{\Gamma}}) = 1 \in G \) since \( G \) is a finite group.
If \( a_{(G,O)} = |H \cap [G_\Gamma, G_\Gamma]| = 1 \), then for \( s_1, s_2 \in S(G, O) \) such that \( \tau(s_1) = \tau(s_2) \), we have \( \alpha_G(s_1) = \alpha_G(s_2) \) if and only if \( \alpha_{G_\Gamma}(s_1) = \alpha_{G_\Gamma}(s_2) \). Therefore if \( a_{(G,O)} = 1 \), then the semigroups \( S(G, O) \), \( S(G, O)^G \), \( S(G, O)_1 \), and \( S(G, O)_1^G \) over the group \( G \) are stable and \( s_{1, gpr}^G \) is one of their stabilizing elements.

If \( a_{(G,O)} > 1 \), then there is an element \( g \in H \cap [G_\Gamma, G_\Gamma] \) such that \( g \neq 1 \). By Lemma 6, there are two elements \( s_1, s_2 \in S(G_\Gamma, Y) \) such that \( g = \alpha_{G_\Gamma}(s_1)\alpha_{G_\Gamma}(s_2)^{-1} \). Therefore, \( s_1 \not\sim s_2 \), but \( \alpha_G(s_1) = \alpha_G(s_2) \) and \( \tau(s_1) = \tau(s_2) \), that is, the semigroups \( S(G, O) \), \( S(G, O)^G \), \( S(G, O)_1 \), and \( S(G, O)_1^G \) over the group \( G \) are not stable (multiplying \( s_1 \) and \( s_2 \) by some element \( s \), we can assume that \( s_1, s_2 \in S(G, O)_1^G \).

\[ \frac{q}{4}. \text{ Uniqueness of factorizations in the case of a big enough number of factors} \]

4.1. The case of \( C \)-finite groups. Let \( G_\Gamma = (G, Y) \) be a \( C \)-finite group and \( m \) the number of connected components of the \( C \)-graph \( \Gamma \).

**Theorem 5.** For each \( C \)-finite group \( G_\Gamma = (G, Y) \), there is a constant \( T \in \mathbb{N} \) such that if elements \( s_1, s_2 \in S(G, Y)^G \) satisfy the following conditions:

(i) \( \tau_i(s_1) \geq T \) for \( i = 1, \ldots, m \);

(ii) \( \alpha_G(s_1) = \alpha_G(s_2) \),

then \( s_1 = s_2 \).

**Proof.** Put \( \alpha = \alpha_G \) and note first of all that if \( \alpha(s_1) = \alpha(s_2) \), then \( \tau_i(s_1) = \tau_i(s_2) \) for \( i = 1, \ldots, m \) since \( \tau_i(s_j) = ab_i(\alpha(s_j)) \).

Let us denote by \( d_\Gamma \) the diameter of \( \Gamma \) and, using the notations of §3.2, denote \( T_1 = (d_\Gamma + 1) \max_{1 \leq i \leq m} n_i p_i + 1 \).

Let us show that any integer \( T \geq T_1 \) satisfies the conditions of Theorem 5. Indeed let \( \tau_i(s_1) \geq T_1 \) for \( i = 1, \ldots, m \). Then, by Corollary 1, the elements \( s_1 \) and \( s_2 \) can be written in the form \( s_1 = s_1^{d_\Gamma} \cdot s_1' \) and \( s_2 = s_2^{d_\Gamma} \cdot s_2' \). We have

\[ \alpha(s_1') = \alpha(s_1)\alpha(s_1^{d_\Gamma})^{-1} = \alpha(s_2)\alpha(s_2^{d_\Gamma})^{-1} = \alpha(s_2') \]

Therefore \( s_1' \sim s_2' \) by Theorem 2 and hence \( s_1 \sim s_2 \) by Theorem 3.

4.2. The case of equipped finite groups. Let \( (G, O) \) be an equipped group equivalent to a \( C \)-finite group \( G_\Gamma \), \( \beta_{(G,O)} : G_\Gamma \rightarrow (G, O) \) the natural epimorphism of equipped groups, \( H = \ker \beta_{(G,O)} \), \( a_{(G,O)} = |H \cap [G_\Gamma, G_\Gamma]| \) the ambiguity index of \((G, O)\), and \( m \) the number of connected components of \( \Gamma \).

**Theorem 6.** For each equipped finite group \( (G, O) \) there is a constant \( T = T_{(G,O)} \) such that if for an element \( s_1 \in S(G, O)^G \) the \( i \)-th type \( \tau_i(s_1) \geq T \) for all \( i = 1, \ldots, m \), then there are \( a_{(G,O)} \) elements \( s_1, \ldots, s_{a_{(G,O)}} \in S(G, O)^G \) such that

- (i) \( s_i \neq s_j \) for \( 1 \leq i < j \leq a_{(G,O)} \);
- (ii) \( \tau_i(s_1) = \tau_i(s_1) \) for \( 1 \leq i \leq a_{(G,O)} \);
- (iii) \( \alpha_G(s_1) = \alpha_G(s_1) \) for \( 1 \leq i \leq a_{(G,O)} \);
- (iv) if \( s \in S(G, O)^G \) is such that \( \tau(s) = \tau(s_1) \) and \( \alpha_G(s) = \alpha_G(s_1) \), then \( s = s_i \) for some \( i, 1 \leq i \leq a_{(G,O)} \).
Proof. By Lemma 6, for \( n \geq z_H \) each element \( g_i \in H \cap [G_\Gamma, G_\Gamma] \) (where \( g_1 = 1 \)) can be presented in the form \( g_i = \alpha_{G_\Gamma}(s_{i,n})\alpha_{G_\Gamma}(s_{i,n}^t)^{-1} \), where \( s_{i,n} \in S(G_\Gamma, Y) = S(G, O) \) (in particular, \( s_{1,n} = s_{1,n}^t \)). We have \( s_{i,n} \neq s_{j,n} \) for \( 1 \leq i < j \leq a_{(G, O)} \), \( \tau(s_{i,n}) = \tau(s_{1,n}) \) and \( \alpha_G(s_{i,n}) = \alpha_G(s_{1,n}) \) for \( 1 \leq i \leq a_{(G, O)} \).

Put \( T_2 = (\max(d_1, z_H) + 1) \max_{1 \leq i \leq m} n_i p_i + 1 \). By Corollary 1, if \( T \geq T_2 \), then the element \( s_1 \) can be written in the form: \( s_1 = s_{1, z_H}^* \cdot s_1^t \). Denote \( s_i := s_{1, z_H}^* \cdot s_i^t \). It is easy to see that the elements \( s_1, \ldots, s_{a_{(G, O)}} \in S(G, O)^G \) satisfy conditions (i)–(iii) and if \( s \in S(G, O)^G \) is such that \( \tau(s) = \tau(s_1) \) and \( \alpha_G(s) = \alpha_G(s_1) \), then \( \alpha_G(s)\alpha_G(s_1)^{-1} \in H \cap [G_\Gamma, G_\Gamma] \) and hence, by Theorem 5, \( s = s_i \) for some \( 1 \leq i \leq a_{(G, O)} \).

Let \( (G, O) \) be an equipped group, \( O = C_1 \sqcup \cdots \sqcup C_m \), where \( C_i \) are conjugacy classes of \( G \). Let for some \( k < m \) the elements of the set \( O' = C_1 \sqcup \cdots \sqcup C_k \) generate the group \( G \). The embedding \( i : O' \hookrightarrow O \) defines subgraphs \( \Gamma' \subset \Gamma' = \Gamma_1 \sqcup \cdots \sqcup \Gamma_k \) of the \( C \)-graph \( \Gamma_{(G, O)} = \Gamma \), where \( \Gamma' \) is the \( C \)-graph of the equipped group \( (G, O') \). The subgraph \( \Gamma' \) is ample since the elements of \( O' \) generate the group \( G \).

Let \( G_\Gamma \) and \( G_{\Gamma'} \) be \( C \)-groups equivalent respectively to \( (G, O) \) and \( (G, O') \), and \( S(G_\Gamma, Y) \) and \( S(G_{\Gamma'}, Y') \) their factorization semigroups. The embedding \( i : O' \hookrightarrow O \) defines a homomorphism \( i_* : G_{\Gamma'} \to G_\Gamma \) of \( C \)-groups and an embedding

\[
i_* : S(G, O') \simeq S(G_{\Gamma'}, Y') \hookrightarrow S(G_\Gamma, Y) \simeq S(G, O)
\]

of semigroups such that \( i_*(\alpha_{G_{\Gamma'}}(s)) = \alpha_{G_\Gamma}(i_*(s)) \) for all \( s \in S(G_{\Gamma'}, Y') \).

**Theorem 7.** Let \( G \) be a finite group and \( O' \subset O \) two equipments of it such that the elements of \( O' \) generate the group \( G \). Then, in the notations used above, there is a constant \( T = T_{(O, O')} \) such that if for an element \( s_1 \in S(G, O)^G \) the \( i \)th type \( \tau_i(s_1) \geq T \) for all \( i = 1, \ldots, k \), then there are no more than \( a_{(G, O')} \) elements \( s_1, \ldots, s_n \in S(G, O)^G \) such that

(i) \( s_i \neq s_j \) for \( 1 \leq i < j \leq n \);

(ii) \( \tau(s_i) = \tau(s_1) \) for \( 1 \leq i \leq n \);

(iii) \( \alpha_G(s_i) = \alpha_G(s_1) \) for \( 1 \leq i \leq n \),

where \( a_{(G, O')} \) is the ambiguity index of \( (G, O') \).

**Proof.** Let \( T_1 = 2d_{\Gamma'} \max_{1 \leq i \leq k} n_i p_i \), where \( d_{\Gamma'} \) is the diameter of \( \Gamma' \) with respect to the ample subgraph \( \Gamma' \), let \( p_i \) and \( n_i \), respectively, be the period and the number of vertices of the connected component \( \Gamma_i \) of the graph \( \Gamma \), and let \( T_2 \) be a constant the existence of which for the equipped group \( (G, O') \) is claimed in Theorem 6. Put \( T = \max(T_1, T_2) \). By Proposition 4, if for \( s \in S(G, Y)^G \) its \( i \)th type \( \tau_i(s) \geq T \) for all \( i \leq k \), then \( s \) can be written in the form: \( s = (x_{i}^{a_{k+1}} \cdot \ldots \cdot x_{m}^{a_{m}}) \cdot s_{1,i} \), where \( a_i = \tau_i(s) \) for \( i = k + 1, \ldots, m \) and \( s_1 \in S(G, O') \). Now, Theorem 7 follows from Theorem 6 applied to the element \( s_{1,i} \cdot s_1 \in S(G, O)^G \).

**4.3. Generating functions.** For each \( \bar{k} = (k_1, \ldots, k_m) \in \mathbb{Z}_{\geq 0}^m \) denote by \( h_{\bar{k}} \) the number of elements \( s \in S(G, O)^G \) with \( \tau(s) = \bar{k} \) and associate with \( (G, O) \) a power series

\[
\chi(G, O)(t_1, \ldots, t_m) := \sum_{\bar{k} \in \mathbb{Z}_{\geq 0}^m} h_{\bar{k}} t_1^{k_1} \cdots t_m^{k_m}.
\]
Proposition 8. Let \( G \) be a finite group and \( C \) its conjugacy class such that the elements of \( C \) generate the group \( G \). Then \( \chi_{(G,C)}(t) \) is a rational function.

Proof. Let \( p \) be the period and \( n \) the number of vertices of \( \Gamma_{(G,C)} \), and \( a = a_{(G,C)} \) the index of ambiguity of \((G,C)\). Consider the set of integers

\[
R = \{ r \mid 0 \leq r \leq pn - 1 \text{ and } \exists i \equiv r \pmod{np} \text{ such that } h_i > 0 \},
\]

and let \( i_r \) be the smallest \( i \) for which \( i \equiv r \pmod{np} \) and \( h_i > 0 \). Next, for each \( r \in R \) choose a representative \( s_r \in S(G,C)^G_1 \) of length \( \ln(s_r) = i_r \) and choose a constant \( M \) such that \( T = 2pnM \) is big enough, then it follows from Proposition 3 and Theorem 7 that \( h_r > 0 \), for which \( \chi(t) = \chi_{(G,C)}(t) \).

Write \( \chi_{(G,C)}(t) \) in the form \( \chi_{(G,C)}(t) = \chi_{<T}(t) + \chi_{\geq T}(t) \), where \( \chi_{<T}(t) = \sum_{i=1}^{T-1} h_it^i \). Note that \( \chi_{<T}(t) \) is a polynomial. The function \( \chi_{\geq T}(t) \) can be written in the form

\[
\chi_{\geq T}(t) = \sum_{r \in R} \sum_{j=0}^{\infty} h_{r+T+jpn} t^{r+T+jpn}.
\]

By Theorem 6, we have \( h_{r+T+jpn} = a \) for each \( r \in R \) and each \( j \geq 0 \), therefore

\[
\chi_{\geq T}(t) = at^T \sum_{r \in R} t^r \sum_{j=0}^{\infty} t^{jpn} = \frac{at^T}{1-t^{pn}} \sum_{r \in R} t^r.
\]

Example 2. If \( G = \Sigma_n \) is the symmetric group and \( O \) the set of transpositions, then by the Clebsch-Hurwitz Theorem \( \chi_{(G,O)} = t^{\frac{2(n-1)}{2}}/(1-t^2) \).

A generalization of Proposition 8 is the following result.

Theorem 8. Let \( G \) be a finite group and \( O = C_1 \sqcup \cdots \sqcup C_m \) a disjoint union of its conjugacy classes such that the elements of each class \( C_i \) generate the group \( G \). Then \( \chi_{(G,O)}(t_1, \ldots, t_m) \) is a rational function.

Proof. This is similar to the proof of Proposition 8. We only need to note that if \( k_i \) is big enough, then it follows from Lemma 3 and Theorem 7 that

\[
0 \leq h_{\{k_1, \ldots, k_{i-1}, k_i+p_i, n_i, k_{i+1}, \ldots, k_m\}} \leq h_{\{k_1, \ldots, k_{i-1}, k_i, n_i, k_{i+1}, \ldots, k_m\}}.
\]

Question. Is \( \chi_{(G,O)}(\overline{t}) \) a rational function for any equipped finite group \((G,O)\)?

§ 5. Computation of the ambiguity index

5.1. The word problem for \( C \)-finite groups. In this subsection we prove

Theorem 9. The \( C \)-finite groups have a solvable word problem.

Proof. Let \( \Gamma = \Gamma_1 \sqcup \cdots \sqcup \Gamma_m \) be the \( C \)-graph of a \( C \)-finite group \((G,Y)\). By Claim 7, without loss of generality, we can assume that for each connected component \( \Gamma_i \) of \( \Gamma \) the period \( p_i \) of its vertices is greater than 1.

By Proposition 3, applying the relations of a \( C \)-group given by a \( C \)-graph \( \Gamma \), any word in letters of \( Y \) can be transformed into a word of the following form:

\[
w = c^{-1} y_{1,1}^{t_1} y_{2,1}^{t_2} \cdots y_{m,1}^{t_m} \prod_{i=1}^{m} y_{i,1}^{k_i p_i} y_{i,1}^{a_{i,1}} y_{i,2}^{a_{i,2}} \cdots y_{i,n_i}^{a_{i,n_i}},
\]  

(13)
where \( c \) is the canonical element of \( G_\Gamma \), \( n_i \) is the number of vertices of \( \Gamma_i \), and the integers \( k_i \) and \( a_{i,j} \) satisfy the following relations and inequalities:

\[
\sum_{j=1}^{n_i} a_{i,j} + k_ip_i = n_ip_i, \quad (14)
\]

\[
0 < a_{i,j} \leq p_i - 1, \quad 0 \leq k_i < n_i. \quad (15)
\]

If two words \( w_1 \) and \( w_2 \) represent the same element \( g \in G_\Gamma \), then \( ab(w_1) = ab(w_2) = (t_1, \ldots, t_m) \). Therefore, to prove the theorem it suffices to show that there is a finite algorithm solving the following problem: recognize when two words

\[
w_l = \prod_{i=1}^{m} y_{i,1}^{k_{i,1}p_i} y_{i,1}^{a_{i,1,1}} y_{i,2}^{a_{i,1,2}} \cdots y_{i,n_i}^{a_{i,n_i,1}}, \quad l = 1, 2, \quad (16)
\]

in which the integers \( k_{i,l} \) and \( a_{i,j,l} \) with fixed \( l = 1, 2 \) satisfy relations (14) and inequalities (15), represent the same element in \( G_\Gamma \).

Note also that the words of the form

\[
wlc^{-1}, \quad l = 1, 2, \quad (17)
\]

where the \( w_l \) are the words from (16), represent elements of \([G_\Gamma, G_\Gamma]\).

In the sequel, to simplify notations, we will consider only the case when \( m = 1 \), since the general case is similar. We will use the following notations: \( \Gamma = \Gamma_1 \), \( n := n_1 \), \( p := p_1 \), \( \{v_1, \ldots, v_n\} \) is the set of vertices of \( \Gamma \) and \( y_i \) is the \( C \)-generator of \( G_\Gamma \) corresponding to a vertex \( v_i \). Denote by \( R_\Gamma \) the set of relations in \( G_\Gamma \) defined by the \( C \)-graph \( \Gamma \) (see §2.1). Recall that for each ordered pair \((l_1, l_2)\) such that \( 1 \leq l_1, l_2 \leq n \), there is a unique \( l_3 \) (depending on \((l_1, l_2)\)), \( 1 \leq l_3 \leq n \), such that

\[
y_{l_1}y_{l_2}y_{l_3}^{-1}y_{l_3}^{-1} \in R_\Gamma. \quad (18)
\]

Consider an equipped group \((\overline{G} = G_\Gamma/H, O)\), where \( H \) is the subgroup of the centre \( Z(G_\Gamma) \) generated by the element \( y_i^p = y_i^p, \quad i = 1, \ldots, n \). Denote by \( f = f_{(G,O)}: G_\Gamma \to \overline{G} \) the natural epimorphism and by \( f' = f|_{[G_\Gamma, G_\Gamma]} \) its restriction to \([G_\Gamma, G_\Gamma]\). The group \( \overline{G} \) has the following presentation:

\[
\overline{G} = \langle y_1, \ldots, y_n \mid R(\overline{y}) = 1 \text{ for } R \in R_\Gamma \text{ and } y_1^p = \cdots = y_n^p = 1 \rangle.
\]

By Lemma 5, we have the commutative diagram

\[
1 \longrightarrow [G_\Gamma, G_\Gamma] \longrightarrow G \xrightarrow{ab} \mathbb{Z} \longrightarrow 0
\]

\[
\downarrow f' \quad \sim \quad \downarrow f
\]

\[
1 \longrightarrow [\overline{G}, \overline{G}] \longrightarrow \overline{G} \xrightarrow{ab} \mathbb{Z}/p\mathbb{Z} \longrightarrow 0
\]

in which \( f' \) is an isomorphism, and \( f \) and \( f'' \) are epimorphisms. It follows from the above considerations and diagram (*) that each element \( g \in \overline{G} \) can be represented by a word of the form

\[
w = a_1^n y_2^a \cdots y_n^a, \quad (19)
\]
Factorizations in finite groups

where each integer \( a_j \) satisfies the inequality

\[
0 \leq a_j \leq p - 1,
\]

and hence

\[
\sum_{j=1}^{n} a_j \leq n(p - 1).
\]

Denote by \( W_i \) the set of positive words \( w \) in letters of \( Y \) whose lengths \( \ln(w) = i \) (in particular, \( W_0 \) consists of the empty word), \( W_{\leq k} = \bigcup_{i=0}^{k} W_i \), and let

\[
\tilde{W}_{\leq k} = \{ w \in W_{\leq k} \mid \text{each letter } y_j \in Y \text{ enters } w \text{ fewer than } p \text{ times} \}.
\]

Let us show that there is a finite algorithm recognizing when two words \( w_1, w_2 \in \tilde{W}_{\leq n(p-1)} \) represent the same element of \( \tilde{G} \). Prior to describing such an algorithm, we give several definitions. A word \( w \) is reduced if there does not exist \( y_j \in Y \) entering \( w \) sequentially \( p \) times. If some letter \( y_j \in Y \) enters \( w \) sequentially \( p \) times, that is, \( w = w'y_jp'w'' \), then the word \( w_1 = w'w'' \) is called a reduction of \( w \). For each positive word \( w \), denote by \( \tilde{w} \) the reduced word obtained from \( w \) by reductions and for each subset \( V \subset W_{\leq 2n(p-1)} \), we define the subset

\[
\nabla = \{ \tilde{w} \in \tilde{W}_{\leq n(p-1)} \mid \exists w \in V \text{ such that } \tilde{w} = w \}.
\]

Let \( \sigma_1, \ldots, \sigma_{k-1} \) be a set of Artin generators of the braid group \( B_k \). Define an action of the group \( B_k \) on the set \( W_i \) as follows: if \( i \neq k \), then this action is trivial; and if \( i = k \), then for a word

\[
w = y_{i_1} \cdots y_{i_{j-1}} y_{i_j} y_{i_{j+1}} y_{i_{j+2}} \cdots y_{i_k}
\]

its image \( \sigma_j(w) = y_{i_1} \cdots y_{i_{j-1}} y'_{i_j} y_{i_{j+1}} y_{i_{j+2}} \cdots y_{i_k} \), where \( i' \) depends on the pair \((i_j, i_{j+1})\) and it is defined by relation (18) if we put \( l_1 = i_j, l_2 = i_{j+1} + 1, \) and \( l' = l_3 \). Denote

\[
B = B_0 \times B_1 \times \cdots \times B_{2n(p-1)},
\]

where \( B_0 \) and \( B_1 \) are trivial groups. The action of the groups \( B_k \), defined above, makes it possible to define a natural action of \( B \) on \( W_{\leq 2n(p-1)} = \bigcup_{i=0}^{2n(p-1)} W_i \). For each subset \( V \) of \( W_{\leq 2n(p-1)} \) denote by \( BV \) the union of the orbits of the elements of \( V \) under the action of \( B \).

Let \( N_1 \) be the number of words in \( \tilde{W}_{\leq n(p-1)} \). Let us number them, \( w_1, \ldots, w_{N_1} \), and consider each of them as a subset of \( \tilde{W}_{\leq n(p-1)} \) (denote them by \( \tilde{V}_{j,1} = \{ w_j \} \)). The algorithm can be described as follows. Suppose at the end of the \((k-1)\)th step we have obtained a presentation of \( \tilde{W}_{\leq n(p-1)} \) as a disjoint union of its subsets,

\[
\tilde{W}_{\leq n(p-1)} = \tilde{V}_{1,k} \sqcup \cdots \sqcup \tilde{V}_{N_k,k}.
\]

At the \( k \)th step for each pair \((i, j) \in \{1, \ldots, N_k\}^2 \), we form subsets

\[
\tilde{V}_{i,k} \tilde{V}_{j,k} = \{ w = w'w'' \mid w' \in \tilde{V}_{i,k}, w'' \in \tilde{V}_{j,k} \} \subset W_{\leq 2n(p-1)}
\]
and form the set of their orbits \( \{ B(\tilde{V}_{i,k} \tilde{V}_{j,k}) \} \). Define an equivalence relation induced by the following equivalence: two orbits \( B(\tilde{V}_{i,k} \tilde{V}_{j,k}) \) and \( B(\tilde{V}_{i,k} \tilde{V}_{j,k}) \) (resp., \( B(\tilde{V}_{i,k} \tilde{V}_{j,k}) \) and \( B(\tilde{V}_{i,k} \tilde{V}_{j,k}) \)) are equivalent if there is \( j_0 \) (resp., \( i_0 \)) such that
\[
B(\tilde{V}_{i_1,k} \tilde{V}_{j_0,k}) \cap B(\tilde{V}_{i_2,k} \tilde{V}_{j_0,k}) \neq \emptyset
\]
(resp., \( B(\tilde{V}_{i_0,k} \tilde{V}_{j_2,k}) \cap B(\tilde{V}_{i_0,k} \tilde{V}_{j_2,k}) \neq \emptyset \)), and for each equivalence class we unite the subsets \( B(\tilde{V}_{i,k} \tilde{V}_{j,k}) \) belonging to this class. Denote the obtained subsets by \( V_{1,k}, \ldots, V_{N_{k+1},k} \) and put \( \tilde{V}_{i,k+1} := \tilde{V}_{i,k} \).

It is easy to see that \( N_{k+1} \leq N_k \) and \( \tilde{V}_{1,k+1} \sqcup \cdots \sqcup \tilde{V}_{N_{k+1},k+1} = \tilde{W}_{\leq n(p-1)} \). The algorithm is stopped if \( N_{k+1} = N_k \). In this case two words \( w_l = y_1^{a_{1,l}} y_2^{a_{2,l}} \ldots y_n^{a_{n,l}} \), \( l = 1, 2 \), satisfying inequality (20) (in the case \( m = 1 \)) represent the same element in \( \tilde{G} \) if and only if \( w_1 \) and \( w_2 \) belong to the same subset \( \tilde{V}_i := \tilde{V}_{i,k+1} \) for some \( i \). To show this, let us introduce a group structure on the set \( \tilde{G} = \{ \tilde{V}_i \} \). By definition, the product of \( \tilde{V}_i \) and \( \tilde{V}_j \) is
\[
\tilde{V}_i \tilde{V}_j = B(\tilde{V}_i \tilde{V}_j).
\]
This product is well defined by construction of subsets \( \tilde{V}_i \) and since \( N_{k+1} = N_k \). The unity in \( \tilde{G} \) is a subset \( \tilde{V}_{i_0} \) containing the empty word, the inverse element of \( \tilde{V}_i \) containing a word \( w = y_1^{a_1} y_2^{a_2} \ldots y_n^{a_n} \) is the subset \( \tilde{V}_j \) containing the reduction of the word \( w = y_1^{p-a_1} y_2^{p-a_2} \ldots y_n^{p-a_n} \). Let us renumber the subsets \( \tilde{V}_j \) so that for \( i = 1, \ldots, n \) the subset \( \tilde{V}_i \) contains the word \( y_i \). Then it is easy to see that \( \tilde{O} \) is invariant under the inner automorphisms of \( \tilde{G} \) and the \( C \)-graph of the equipped group \( (\tilde{G}, \tilde{O}) \) coincides with \( \Gamma \). Moreover, since to construct the elements of \( \tilde{G} \), we used only the relations from \( \mathcal{R}_\Gamma \) and the relations \( y_1^p = \cdots = y_n^p = 1 \), obviously, the equipped group \( (\tilde{G}, \tilde{O}) \) is isomorphic to \( (\tilde{G}, \tilde{O}) \). Therefore, the epimorphism \( f_{(\tilde{G}, \tilde{O})} : [G_{\Gamma}, G_{\Gamma}] \to [\tilde{G}, \tilde{G}] \) coincides with the isomorphism \( f' : [G_{\Gamma}, G_{\Gamma}] \to [\tilde{G}, \tilde{G}] \) if we identify the equipped groups \( (\tilde{G}, \tilde{O}) \) and \( (\tilde{G}, \tilde{O}) \).

Finally, by Proposition 3 and since the words of form (17) represent elements of \( [G_{\Gamma}, G_{\Gamma}] \), two words of the form (16) satisfying relations (14) and inequalities (15) represent the same element of \( G_{\Gamma} \) if and only if the reductions of these words represent the same element of \( \tilde{G} \).

5.2. Computation of the ambiguity index. We say that an equipped finite group \( (G, O) \) is defined efficiently if there is a finite algorithm to enumerate the elements of \( G \) (for example, if \( G \) is given by its Cayley graph, or generators of \( G \) as permutations of some symmetric group are given) and a representative of each class \( C_i \subset O \) is also given.

**Proposition 9.** If an equipped finite group \( (G, O) \) is defined efficiently, then there is a finite algorithm to compute the ambiguity index \( a_{(G, O)} \).

**Proof.** Since \( (G, O) \) is given efficiently, then, obviously, there is a finite algorithm to define completely the \( C \)-graph \( \Gamma = \Gamma_{(G, O)} \).
Using the description of $\Gamma$, as in the proof of Theorem 9, we enumerate the subsets $V_i$ containing words of the form

$$w = \prod_{i=1}^{m} y_{i,1}^{k_i} y_{i,2}^{a_{i,1,1}} y_{i,2}^{a_{i,1,2}} \cdots y_{i,n_i}^{a_{i,n_i}},$$  

(22)

where the integers $k_i$ and $a_{i,j}$ satisfy the following relations and inequalities

$$\sum_{j=1}^{n_i} a_{i,j} + k_i p_i = n_i p_i,$$  

(23)

$$0 < a_{i,j} \leq p_i - 1, \quad 0 \leq k_i < n_i.$$  

(24)

After that for each $i$ we choose a word $w_i$ of the form (22) the reduction of which belongs to $V_i$ and check if $c^{-1}w_i$ represents the unity in $G$, where $c$ is the canonical element of $G_{\Gamma}$. By Proposition 3, the number of the sets $V_i$, for which the corresponding words $c^{-1}w_i$ represent the unity of $G$, is equal to $a_{(G,O)}$.

Bibliography

[1] W. Fulton, “Hurwitz schemes and irreducibility of moduli of algebraic curves”, *Ann. of Math.* (2) **90**:3 (1969), 542–575.

[2] A. Clebsch, “Zur Theorie der Riemann'schen Fläche”, *Math. Ann.* **6**:2 (1873), 216–230.

[3] A. Hurwitz, “Ueber Riemann’sche Flächen mit gegebenen Verzweigungspunkten”, *Math. Ann.* **39**:1 (1981), 1–60.

[4] Vik. S. Kulikov, “Factorization semigroups and irreducible components of the Hurwitz space”, *Izv. Ross. Akad. Nauk Ser. Mat.* **75**:4 (2011), 49–90; English transl. in *Izv. Math.* **75**:4 (2011), 711–748.

[5] Vik. S. Kulikov, “Factorization semigroups and irreducible components of the Hurwitz space. II”, *Izv. Ross. Akad. Nauk Ser. Mat.* **76**:2 (2012), 151–160; English transl. in *Izv. Math.* **76**:2 (2012), 356–364.

[6] B. Wajnryb, “Orbits of Hurwitz action for coverings of a sphere with two special fibers”, *Indag. Math. (N.S.)* **7**:4 (1996), 549–558.

[7] Vik. S. Kulikov, “Hurwitz curves”, *Uspekhi Mat. Nauk* **62**:6 (2007), 3–86; English transl. in *Russian Math. Surveys* **62**:6 (2007), 1043–1119.

[8] R. C. Lyndon and P. E. Schupp, *Combinatorial group theory*, Springer-Verlag, Berlin–Heidelberg–New York 1977.

[9] A. Yu. Ol’shanskii, *Geometry of defining relations in groups*, Mir, Moscow 1989; English transl., Math. Appl. (Soviet Ser.), vol. 70, Kluwer Acad. Publ., Dordrecht 1991.

Vik. S. Kulikov  
Steklov Mathematical Institute,  
Russian Academy of Sciences  
E-mail: kulikov@mi.ras.ru  

Received 4/AUG/11 and 30/OCT/12  
Translated by Vik. KULIKOV