Group extensions and graphs

A. Ballester-Bolinches* E. Cosme-Llópez†
R. Esteban-Romero‡

Abstract

A classical result of Gaschütz affirms that given a finite A-generated group G and a prime p, there exists a group $G^{\#}$ and an epimorphism $\varphi\colon G^{\#} \longrightarrow G$ whose kernel is an elementary abelian p-group which is universal among all groups satisfying this property. This Gaschütz universal extension has also been described in the mathematical literature with the help of the Cayley graph. We give an elementary and self-contained proof of the fact that this description corresponds to the Gaschütz universal extension. Our proof depends on another elementary proof of the Nielsen-Schreier theorem, which states that a subgroup of a free group is free.

Mathematics Subject Classification (2010): Primary: 20F65. Secondary: 05C25, 20D20, 20E22, 20F05, 20F10.

Keywords: group, group extension, graph

1 Introduction and statement of results

Recall that F is a *free group* over a set A when there exists a function $\iota\colon A \longrightarrow F$ such that given a group G and a map $f\colon A \longrightarrow G$, there exists a unique group homomorphism $\varphi\colon F \longrightarrow G$ such that $\iota\varphi = f$ (we will write maps and compositions on the right). The basic properties of the free group can be found, for instance, in [8, I, §19]. We will say that a group G is

*Departament d'Àlgebra, Universitat de València; Dr. Moliner, 50; E-46100 Burjassot, València, Spain, email: Adolfo.Ballester@uv.es

†Departament d'Àlgebra, Universitat de València; Dr. Moliner, 50; E-46100 Burjassot, València, Spain, email: Enric.Cosme@uv.es

‡Institut Universitari de Matemàtica Pura i Aplicada, Universitat Politècnica de València; Camí de Vera, s/n; E-46022 València, Spain, email: resteban@mat.upv.es. Current address: Departament d'Àlgebra, Universitat de València; Dr. Moliner, 50; E-46100 Burjassot, València, Spain, email: Ramon.Esteban@uv.es

generated by a set A or *A-generated* if there exists a map $f\colon A \longrightarrow G$ such that the image of f is a generating system for G, that is, if there exists an epimorphism φ_G from the free group F over A onto G. In this case, we can identify the elements of A with their images in G and we will assume that φ_G is a fixed once given G and A. If G and H are two A-generated groups, with associated epimorphisms φ_G and φ_H, we will say that a homomorphism $\varphi\colon G \longrightarrow H$ *preserves generators* if $\varphi_G\varphi = \varphi_H$. Of course, a homomorphism between A-generated groups preserving generators must be an epimorphism.

The following classical result was proved by Gaschütz ([4], see also [2, Proposition β.3]):

Theorem 1. *Given a finite A-generated group G and a prime p, then there exist an A-generated group $G^{\#}$ and an epimorphism $\varphi\colon G^{\#} \longrightarrow G$ preserving generators whose kernel is an elementary abelian p-group N with the following universal property:*

> *If H is an A-generated group and $\psi\colon H \longrightarrow G$ is an epimorphism preserving generators whose kernel is an elementary abelian p-group K, then there exists an epimorphism $\beta\colon G^{\#} \longrightarrow H$ such that $\beta\psi = \varphi$.*

If F is a free group over A and R is a normal subgroup of F such that $F/R \cong G$, then $G^{\#} = F/R'R^p$ satisfies the condition of Theorem 1. This group is used in the construction of a universal Frattini p-elementary extension of a finite group G, which is a group E with a normal, elementary abelian p-subgroup $A \neq 1$ such that $A \leq \Phi(E)$ and $E/A \cong G$ (see [2, B, Section 11 and Appendix β]). This extension plays a major role in the proof of the theorem of Gaschütz, Lubeseder, and Schmid, which states that every saturated formation can be locally defined by a formation function ([5, 6, 9, 13], see also [2, IV, Section 4] for details).

According to a theorem of Ribes and Zalesskiĭ [12], given finitely generated subgroups $H_1, \ldots, H_n$ of a free group F, their product $H_1 \cdots H_n$ is closed in the profinite topology of F. This result confirmed a conjecture of Pin and Reutenauer [11] and completed a proof of the so-called *Rhodes type II conjecture* about finite monoids. The Ribes-Zalesskiĭ theorem has been proved and generalised in many ways. Connections of this theorem with other branches of Mathematics, like automata theory [16] and model theory [7], have also been investigated.

A constructive proof of the Ribes-Zalesskiĭ theorem was given by Auinger and Steinberg in [1]. The same proof can be easily adapted to give generalisations of this theorem for the pro-$\mathfrak{H}$ topology for varieties $\mathfrak{H}$ of groups satisfying that for each $G \in \mathfrak{H}$, there exists a prime p for which the wreath

product $C_p \wr G$ is also in $\mathfrak{H}$. One of the ingredients of this proof is the construction of a group $G^{\mathbf{Ab}_p}$, for an A-generated finite group G and a prime p, based on the Cayley graph of the group G. The details of this construction will be presented later in Section 3. Elston [3], with the help of techniques from semigroup theory and category theory, proved that $G^{\mathbf{Ab}_p}$ satisfies the same universal property of $G^{\#}$ stated in Theorem 1. Consequently:

Theorem 2. *The group $G^{\mathbf{Ab}_p}$ is isomorphic to the group $G^{\#}$ of Theorem 1.*

The aim of this paper is to find an elementary and self-contained proof of this theorem, which would clear up the connection between both constructions, by using only elementary techniques of graph theory, group theory, and linear algebra. This should make this result more accessible to the general mathematician. Our arguments depend on an elementary proof we give for the following classical result of Nielsen [10] and Schreier [14]:

Theorem 3 (Nielsen-Schreier)**.** *Let F be a free group and let H be a subgroup of F. Then H is free.*

If, in addition, F has rank n and H has finite index in F, then the rank of H is $1 + |F : H|(n - 1)$.

Many of the known proofs for Theorem 3 use techniques from algebraic topology. Our proof avoids the use of these techniques and is based only on elementary graph theory applied to a generalisation of the Cayley graph. As our aim is to make this paper self-contained, we will recall in Section 2 the definitions and results about graphs that we will use. The construction of $G^{\mathbf{Ab}_p}$ will be presented in Section 3. Finally, the proofs of the theorems will be given in Section 4.

2 Preliminaries about graphs

For the reader's convenience, we collect in this sections the basic concepts about graphs that we will need in our proofs. They can be found in any book about graph theory, for instance, [15].

A (directed) *graph* $\Gamma = (V, E, \iota, \tau)$ consists of a non-empty set V (of *vertices*) and a set E (of *arcs* or *edges*), together with two functions $\iota\colon E \longrightarrow V$ and $\tau\colon E \longrightarrow V$ giving the *initial* and *terminal* vertex, respectively, of a given edge. If $\iota(e) = v_1$ and $\tau(e) = v_2$, we will say that e *joins* v_1 and v_2 and we can express it in the form $v_1 \to v_2$. Sometimes we will add a *label* to each arc of the graph, which is an element of a given set A. If a is the label of the arc e, we will write $v_1 \xrightarrow{e} v_2$. For convenience, given an arc e joining v_1 and

v_2, then we say that the *inverse arc* e^{-1} joins v_2 and v_1 and if the label of e is a, the label of e^{-1} is a^{-1}. The set $\{e^{-1} \mid e \in E\}$ will be denoted by E^{-1}.

An (undirected) *path* of *length* n in a graph Γ is a sequence

$$p = (v_0, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, v_n)$$

such that for $0 \leq i \leq n$, $v_i \in V$ and for $1 \leq i \leq n$, $e_i \in E \cup E^{-1}$ joins v_{i-1} and v_i. The initial vertex of p will be v_0 and the final vertex of p will be v_n. If the arcs of the graph are labelled, then the label of p is the product of the labels of the e_i. Two vertices v and w of a graph will be *weakly connected* if there is a path with initial vertex v and final vertex w. A graph is *weakly connected* if every two vertices are weakly connected. A path is called *simple* if no edge nor its inverse appears more than once in the path. A simple path of positive length in which the initial and the terminal vertices coincide and in which no other pair of vertices coincide is called a *cycle*. A weakly connected graph with no cycles is called an *undirected tree* or simply a *tree*. It is clear that a graph is a tree if and only if given two vertices u and v there is exactly one simple path with initial vertex u and final vertex v.

A graph $\Gamma_1 = (V_1, E_1, \iota_1, \tau_1)$ is a *subgraph* of $\Gamma = (V, E, \iota, \tau)$ if $V_1 \subseteq V$, $E_1 \subseteq E$ and for each $e_1 \in E_1$, $\iota_1(e_1) = \iota(e_1) \in V_1$ and $\tau_1(e_1) = \tau(e_1) \in V_1$. We say that a subgraph of a graph is a *spanning tree* if it is a tree containing all vertices of the graph.

For weakly connected graphs with a finite number of vertices and arcs, there are algorithms to obtain a spanning tree starting from one vertex. In the general case, we need to use Zorn's lemma. The following proof is due to Serre [15, Section 2.3, Proposition 11].

Theorem 4. *Every weakly connected graph* Γ *has a spanning tree.*

Proof. Consider the set $\mathcal{T}$ of all subgraphs Γ_1 of Γ which are trees. This set can be partially ordered with the relation of being a subgraph. Let $\mathcal{C} = \{\Gamma_\omega = (V_\omega, E_\omega, \iota_\omega, \tau_\omega) \mid \omega \in \Omega\}$ be a non-empty chain in $\mathcal{S}$. Its union $(\bigcup_{\omega\in\Omega} V_\omega, \bigcup_{\omega\in\Omega} E_\omega, \tilde{\iota}, \tilde{\tau})$, where $\tilde{\iota}(e) = \iota_\omega(e)$ and $\tilde{\tau}(e) = \iota_\omega(e)$ if $e \in E_\omega$, is an upper bound of $\mathcal{C}$. By Zorn's lemma, $\mathcal{T}$ possesses a maximal element T. Assume that T is not a spanning tree. Since Γ is weakly connected, there exists an arc with initial vertex in T and final vertex outside T, or with initial vertex outside T and final vertex in T. If we add this edge and this vertex to T, we obtain a larger tree T'. This contradicts the maximality of T. Hence T is a spanning tree. □

Note that a tree with a finite number n of vertices must have exactly $n-1$ edges.

3 The Cayley graph and a construction of the Gaschütz extension

Given an A-generated group G, the *Cayley graph* of G (with respect to A) has as vertices the elements of G and edges of the form $g \xrightarrow{a} ga$, where $g \in G$ and $a \in A$, labelled with a. The Cayley graph of an A-generated group G is always weakly connected.

Now assume that G is an A-generated finite group, A is finite, and p is a prime. We present the construction of [1] for the group $G^{\mathbf{Ab}_p}$, which can be regarded as a particular case of the construction for monoids presented in [3]. Let E be the set of arcs of the Cayley graph of G, and let $V(E)$ be the additive group of the free $\mathbb{Z}/p\mathbb{Z}$-module generated by E. The group G acts on the left on E via $g(h \xrightarrow{a} ha) = gh \xrightarrow{a} gha$ for every g, $h \in G$, $a \in A$. This action extends uniquely to an action by automorphisms on $V(E)$ and so we can construct the semidirect product $U = [V(E)]G$. Consider the subgroup

$$G^{\mathbf{Ab}_p} = \langle (1 \xrightarrow{a} a, a) \mid a \in A \rangle$$

of U. The assignment $(1 \xrightarrow{a} a, a) \mapsto a$ defines an epimorphism from $G^{\mathbf{Ab}_p}$ onto G whose kernel C is an elementary abelian p-group. Let $A^{-1} = \{a^{-1} \mid a \in A\}$, $\widetilde{A} = A \cup A^{-1}$, and $\widetilde{A}^*$ be the set of all words with letters in $\widetilde{A}$, which can be regarded as the free monoid on $\widetilde{A}$. Given a word $w \in \widetilde{A}^*$ and an A-generated group G, we denote by $[w]_G$ the image of w under the natural homomorphism from $\widetilde{A}^*$ onto G. Given a word $w \in \widetilde{A}^*$ and an arc e, we denote by $w(e)$ the number of signed traversals of e by the path of the Cayley graph of G labelled by w and starting at 1 and $w_p(e) = w(e) \bmod p$. Then

$$[w]_{G^{\mathbf{Ab}_p}} = \left(\sum_{e \in E} w_p(e) e, [w]_G \right).$$

4 Proofs of the theorems

For completeness, we will give a proof of Theorem 1.

Proof of Theorem 1. Let G be an A-generated group with associated epimorphism $\varphi_G \colon F \longrightarrow G$, where F is the free group with basis A. Then $R = \operatorname{Ker} \varphi_G$ is a normal subgroup of F and $G \cong F/R$. Let p be a prime. Then we construct $R^{\#} = R'R^p$ and consider $G^{\#} = F/R^{\#}$. Then $G^{\#}$ is an A-generated group, where $\varphi_{G^{\#}} \colon F \longrightarrow G^{\#}$ is the natural epimorphism. It follows that $R/R^{\#}$ is a normal elementary abelian p-subgroup of $F/R^{\#}$ such that $(F/R^{\#})/(R/R^{\#}) \cong F/R \cong G$. Moreover, $\varphi_{G^{\#}}\varphi = \varphi_G$. Let H

be an A-generated group with associated epimorphism $\varphi_H\colon F \longrightarrow H$ and let $\psi\colon H \longrightarrow G$ be an epimorphism preserving generators with kernel a normal elementary abelian p-subgroup N. Let $w \in R$. Then $w\varphi_H\psi = 1$. In particular, $w\varphi_H \in N$. Therefore, given w_1, $w_2 \in R$, $[w_1, w_2]\varphi_H = 1$ and $(w_1^p)\varphi_H = 1$. Since H satisfies the relations of $G^{\#}$, by von Dyck's theorem ([8, I, Hilfssatz 19.4]) there exists an epimorphism $\beta\colon G^{\#} \longrightarrow H$ preserving generators such that $\beta\psi = \varphi$. □

Our proof of Theorem 3 is based on a generalisation of the Cayley graph to the set of right coclasses of a subgroup.

Proof of Theorem 3. Assume that F is a free group with basis A. Let us consider the graph Γ whose set of vertices is $\{Hw \mid w \in F\}$ and with arcs of the form $Hw \xrightarrow{a} Hwa$, where $w \in F$ and $a \in A$, labelled by a. The graph Γ, being weakly connected, possesses a spanning tree T by Theorem 4. Given $w \in F$, there is a unique path from H to Hw in T. Let us denote by p_w the label of this path. If $Hw = H$, then we say that $p_w = 1$. Given $w \in F$ and $a \in A$, let $r_{Hw,a} = [p_w a p_{wa}^{-1}]_F$ and $r_{Hw,a^{-1}} = [p_w a^{-1} p_{wa^{-1}}^{-1}]_F = (r_{Hwa^{-1},a})^{-1}$. If $Hw \xrightarrow{a} Hwa$ is an arc of T, then $r_{Hw,a} = r_{Hwa,a^{-1}} = 1$. Otherwise, $r_{Hw,a} = (r_{Hwa,a^{-1}})^{-1} \neq 1$, since the path with label $p_w a$ starting at H contains once the arc $Hw \xrightarrow{a} Hwa$, that does not belong to T, while the path with label p_{wa} starting at H only contains arcs from T.

Note that given $w \in F$, then $w \in H$ if and only if w, regarded as an element of $\widetilde{A}^*$, is the label of a path in Γ from H to H. Let

$$B = \{r_{Hw,a} \mid w \in F,\, a \in A,\, Hw \xrightarrow{a} Hwa \text{ is not an arc in } T\}.$$

We will prove that H is a free group with basis B. Let $U = \langle B \rangle$. Since the generators of U, regarded as words in $\widetilde{A}^*$, are labels of paths from H to H, we have that $U \leq H$. Now let $w \in \widetilde{A}^*$ be such that $[w]_F \in H$, then w is the label of a path from H to H. Suppose that $w = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_t^{\varepsilon_t}$, where $a_i \in A$, $\varepsilon_i \in \{-1, 1\}$, $1 \leq i \leq t$. Then

$$\prod_{i=1}^{t} r_{Ha_1^{\varepsilon_1}\cdots a_{i-1}^{\varepsilon_{i-1}}, a_i^{\varepsilon_i}} = \prod_{i=1}^{t} [p_{a_1^{\varepsilon_1}\cdots a_{i-1}^{\varepsilon_{i-1}}} a_i^{\varepsilon_i} p^{-1}_{a_1^{\varepsilon_1}\cdots a_i^{\varepsilon_i}}]_F = [w]_F [p_w^{-1}]_F = [w]_F.$$

Hence $w \in U$, because the factors of the product are either 1 or generators or inverses of generators of U, and so $H \leq U$. Therefore $H = U$. Now suppose that $\prod_{i=1}^{t} r_{Hw_i, a_i^{\varepsilon_i}} = 1$, where $r_{Hw_i,a_i} \in B$ if $\varepsilon_i = 1$ or $r_{Hw_i a_i^{-1}, a_i} = (r_{Hw_i, a_i^{-1}})^{-1} \in B$ if $\varepsilon_i = -1$ for $1 \leq i \leq t$ and $t \geq 1$ is least possible. Then $\prod_{i=1}^{t} r_{Hw_i, a_i^{\varepsilon_i}}$ can be regarded as the label of a path in Γ starting at H and

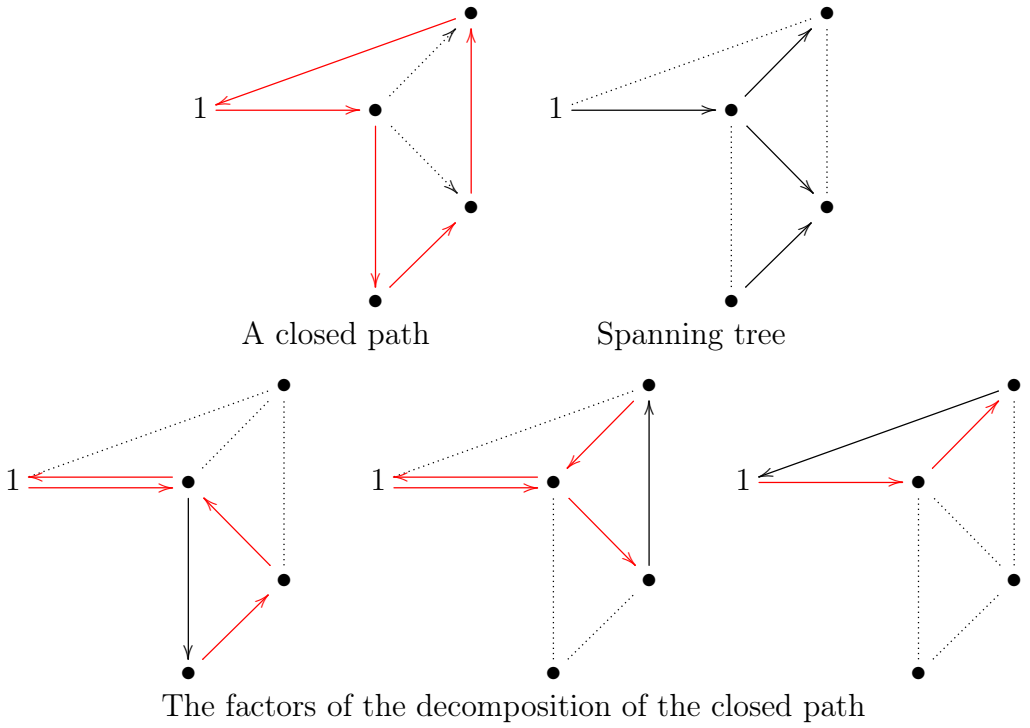

Figure 1: A decomposition of an element of R as a product of generators

all arcs in this path belong to T, except the arcs of the form $Hw_i \xrightarrow{a_i} Hw_ia_i$ (if $\varepsilon_i = 1$) or $Hw_ia_i^{-1} \xrightarrow{a_i} Hw_i$ (if $\varepsilon_i = -1$), for $1 \leq i \leq t$. Since the product is 1, the operation of reducing the path by removing products of consecutive factors of the form aa^{-1} or $a^{-1}a$ should convert it into a path of length zero. In particular, there should be two consecutive arcs not contained in T which reduce, of the form $Hw_i \xrightarrow{a_i} Hw_ia_i$ and its inverse or vice-versa. These arcs correspond to r_{Hw_i,a_i} and $r_{Hw_ia_i,a_i^{-1}} = (r_{Hw_i,a_i})^{-1}$. But in this case, the product of these two factors is trivial and hence we can obtain another expression of 1 as a product of factors of the form r_{Hw,a^ε} with less factors, against the minimality of t. It follows that H is free with basis B.

Now suppose that A and $|F : H|$ are finite. The graph Γ has then $|F : H|$ vertices and $n|F : H|$ arcs. A spanning tree of Γ has $n-1$ vertices. Therefore Γ has $n|F : H| - (|F : H| - 1) = 1 + |F : H|(n-1)$ arcs outside the spanning tree of Γ. Since H is free on a set with the same cardinality as the set of arcs outside the spanning tree of Γ, H is free of rank $1 + |F : H|(n-1)$, as desired. □

Figure 1 shows a decomposition of an element of H as a product of the generators according to the proof of Theorem 3.

Proof of Theorem 2. The construction of Theorem 3 for $H = R$ gives a graph Γ which is isomorphic to the Cayley graph of G when we identify an element $g \in G$ with a right coclass Rw with $w \in F$. With this identification, will write $r_{g,a}$ instead of $r_{Rw,a}$. Therefore R is generated by $B = \{r_{g,a} \mid g \in G,\, a \in A,\, g \xrightarrow{a} ga \text{ not in } T\}$, where T is a spanning tree of the Cayley graph of G. The elements of B generate the normal elementary abelian p-subgroup C. Since the path starting at 1 labelled by $r_{g,a}$ in the Cayley graph of G has a unique arc not in the spanning tree T, the arc $g \xrightarrow{a} ga$, we can conclude that the set $\{\bar{r}_{g,a} \mid r_{g,a} \in B\}$, where $\bar{r}_{g,a}$ denotes the image of $r_{g,a}$ under the epimorphism from F to $G^{\mathbf{Ab}_p}$, is a linearly independent subset of the $\mathbb{Z}/p\mathbb{Z}$-vector space C. On the other hand, the set $\{r_{g,a}R^{\#} \mid r_{g,a} \in B\}$ is a generating set for $R/R^{\#}$ and so its dimension as a $\mathbb{Z}/p\mathbb{Z}$-vector space is at most $|B|$. Since $G^{\mathbf{Ab}_p}$ is a homomorphic image of $G^{\#}$, it turns out, by order considerations, that they are isomorphic. □

5 Final remarks

Some proofs of Theorem 3 refer to Schreier transversals, which are transversals U of H in F composed of elements such that if $x_1x_2\cdots x_r \in U$, where $x_i \in A \cup A^{-1}$, $1 \leq i \leq r$, then $x_1x_2\cdots x_{r-1} \in U$. It is possible to obtain a Schreier transversal by taking an element of each coclass with the smallest possible length. The edges of the form $Hx_1x_2\cdots x_{r-1} \xrightarrow{x_r} Hx_1x_2\cdots x_r$, if $x_r \in A$, or $Hx_1x_2\cdots x_r \xrightarrow{x_r^{-1}} Hx_1x_2\cdots x_{r-1}$, if $x_r \in A^{-1}$, where $x_1x_2\cdots x_r \in U$, form a generating tree for the graph Γ in the proof of Theorem 3. Moreover, the elements of B form a basis for the fundamental group of the graph Γ at H.

Acknowledgements

This work has been supported by the grant MTM-2014-54707-C3-1-P of the *Ministerio de Economía y Competitividad* (Spain). The first author is also supported by the project No. 11271085 from the National Natural Science Foundation of China. The second author is supported by the predoctoral grant AP2010-2764 (*Programa FPU, Ministerio de Educación*, Spain).

References

[1] K. Auinger and B. Steinberg. A constructive version of the Ribes-Zalesskiĭ product theorem. *Math. Z.*, 250(2):287–297, 2005.

[2] K. Doerk and T. Hawkes. *Finite Soluble Groups*, volume 4 of *De Gruyter Expositions in Mathematics*. Walter de Gruyter, Berlin, New York, 1992.

[3] G. Z. Elston. Semigroup expansions using the derived category, kernel, and Malcev products. *J. Pure Appl. Algebra*, 136:231–265, 1999.

[4] W. Gaschütz. Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werten. *Math. Z.*, 60:274–286, 1954.

[5] W. Gaschütz. Zur Theorie der endlichen auflösbaren Gruppen. *Math. Z.*, 80:300–305, 1963.

[6] W. Gaschütz and U. Lubeseder. Kennzeichnung gesättigter Formationen. *Math. Z.*, 82:198–199, 1963.

[7] B. Herwig and D. Lascar. Extending partial automorphisms and the profinite topology on free groups. *Trans. Amer. Math. Soc.*, 352:1985–2021, 2000.

[8] B. Huppert. *Endliche Gruppen I*, volume 134 of *Grund. Math. Wiss.* Springer Verlag, Berlin, Heidelberg, New York, 1967.

[9] U. Lubeseder. *Formationsbildungen in endlichen auflösbaren Gruppen.* Dissertation, Universität Kiel, Kiel, 1963.

[10] J. Nielsen. Om Regning med ikkekommutative faktorer og dens anvendelse i gruppenteorien. *Matematisk Tidsskrift B*, pages 77–94, 1921.

[11] J.-É. Pin and C. Reutenauer. A conjecture on the Hall topology for the free group. *Bull. London Math. Soc.*, 23:356–362, 1991.

[12] L. Ribes and P. Zalesskiĭ. On the profinite topology of a free group. *Bull. London Math. Soc.*, 25:37–43, 1993.

[13] P. Schmid. Every saturated formation is a local formation. *J. Algebra*, 51:144–148, 1978.

[14] O. Schreier. Die Untergruppen der freien Gruppen. *Abh. Math. Semin. Univ. Hambg.*, 5(1):161–183, 1927.

[15] J.-P. Serre. *Trees.* Springer, Berlin, Heidelberg, 1980.

[16] B. Steinberg. Finite state automata: a geometric approach. *Trans. Amer. Math. Soc.*, 353:3409–3464, 2001.