



Logical generation of groups

Alireza Abdollahi & Mohammad Shahryari

To cite this article: Alireza Abdollahi & Mohammad Shahryari (2024) Logical generation of groups, Communications in Algebra, 52:8, 3457-3460, DOI: [10.1080/00927872.2024.2320811](https://doi.org/10.1080/00927872.2024.2320811)

To link to this article: <https://doi.org/10.1080/00927872.2024.2320811>



Published online: 28 Feb 2024.



Submit your article to this journal [↗](#)



Article views: 29



View related articles [↗](#)



View Crossmark data [↗](#)



Logical generation of groups

Alireza Abdollahi^a and Mohammad Shahryari^b

^aDepartment of Pure Mathematics, Faculty of Mathematics and Statistics, University of Isfahan, Isfahan, Iran; ^bDepartment of Mathematics, College of Science, Sultan Qaboos University, Muscat, Oman

ABSTRACT

A group G is called logically generated by a subset S , if every element of G can be defined by a first order formula with parameters from S . We consider the case where G is a direct product of finite nilpotent groups with mutually coprime orders and we show that logical and algebraic generations are equivalent in G . We also prove that in the case when G is a free non-abelian group, if S logically generates G then either it generates G algebraically or $\langle S \rangle$ is not a free factor of G .

ARTICLE HISTORY

Received 05 July 2023
Revised 18 December 2023
Communicated by Mandi Schaeffer Fry

KEYWORDS

Definability; elementary extensions; logically cyclic groups; logical generation

2020 MATHEMATICS

SUBJECT CLASSIFICATION

Primary: 20A15; Secondary: 03C07; 03C98

1. Introduction

Consider the first order language of groups $\mathcal{L} = (\cdot, ^{-1}, 1)$. Let G be a group and $S \subseteq G$. We extend the language $\mathcal{L}$ to the new one $\mathcal{L}_S$ by attaching elements of S to $\mathcal{L}$ as constants. An element $g \in G$ is S -definable if there exists a first order formula $\varphi(x)$ in the language $\mathcal{L}_S$ (having x as the only free variable) such that g is the unique element satisfying φ in G , in other words

$$\{g\} = \{x \in G : G \models \varphi(x)\}.$$

It is known that this happens if and only if for every elementary extension G^* of G and every automorphism α of G^* , the assumption $\alpha|_S = \text{id}$ implies $\alpha(g) = g$. The group G is said to be logically generated by S if every element is S -definable. In this case we use the notation $G = \text{def}_G(S)$. It is evident that if we let H to be the subgroup generated by S then $G = \text{def}_G(H)$ is equivalent to $G = \text{def}_G(S)$. Study of the case when S is a singleton subset $\{s\}$ is already started in [5]. A group G is called logically cyclic if there exists an element s such that $G = \text{def}_G(s)$. All such groups are abelian. In [5] the following cases of logically cyclic groups are studied:

1. Every finite logically cyclic group is cyclic.
2. Every finitely generated logically cyclic group is cyclic or isomorphic to $\mathbb{Z} \times \mathbb{Z}_2$.
3. Every non-trivial divisible logically cyclic group is isomorphic to the additive group of rationales $(\mathbb{Q}, +)$.
4. Every torsion-free logically cyclic is a subgroup of $(\mathbb{Q}, +)$.

This classification is not completed yet and one can see there are new classes of logically cyclic groups.

Example. Let p be a prime and consider the group $G = \mathbb{Z}[\frac{1}{p}] \times \mathbb{Z}_p$, where $\mathbb{Z}_p$ is the cyclic group of order p and $\mathbb{Z}[\frac{1}{p}]$ is the additive group of the rational of the form a/p^n with a and integer and $n \geq 0$. This group is logically generated by $s = (1, 1)$. To see this, suppose G^* is an elementary extension of G . Considering the following first order sentence

$$\forall x \exists (y, z) : x = y + z \wedge p|y \wedge pz = 0$$

we see that $G^* = pG^* \times \mathbb{Z}_p$ ($\exists$ means existence and uniqueness). Further, pG^* is an elementary extension $\mathbb{Z}[\frac{1}{p}]$. Consequently, every automorphism $\alpha : G^* \rightarrow G^*$ has the form $\alpha = (\alpha_1, \alpha_2)$, where α_1 is an automorphism of pG^* and α_2 is an automorphism of $\mathbb{Z}_p$. This means that if $\alpha(1, 1) = (1, 1)$ then α_2 is identity and α_1 fixes every element of $\mathbb{Z}[\frac{1}{p}]$. As a result, G is logically cyclic.

As trivially every algebraic generator set is also a logical generator, the converse is not true in general (even in the case of logically cyclic groups as one can see it in the above statements). In this note, we show that under some assumptions these two concepts are equivalent. We prove that every finite nilpotent group (as well as any restricted direct product of an infinite family of finite nilpotent groups of mutually coprime orders) has this property. More precisely, we prove

Theorem 1.1. *Let $G = \text{Dr}_{i \in \Lambda} G_i$ be the (restricted) direct product of non-trivial finite p_i -groups with distinct odd primes p_i . Suppose a subset $S \subseteq G$ logically generates G . Then $G = \langle S \rangle$.*

As a special case of [Theorem 1.1](#), one can consider any finite nilpotent group of odd order. The proof of [Theorem 1.1](#) shows that one can consider even the case where $p_j = 2$ for some j . But in this case $\mathbb{Z}_2$ must not be a direct factor of G_j . Notice that the theorem is not valid otherwise: let $\Lambda = \{1\}$ and $G_1 = \mathbb{Z}_2$. Then the empty set is a logical generator of G while it does not generate G algebraically. We may have a partial generalization of [Theorem 1.1](#) to the case of locally finite nilpotent groups.

Proposition 1.2. *Let G be a locally finite nilpotent group and $S \subseteq G$. If every element of G is S -definable by a quantifier-free formula, then $G = \langle S \rangle$.*

For the case of non-abelian free groups, we have the following result. Recall that by the seminal work of Kharlampovich-Miyasnikov and Sela, any two non-abelian free groups are elementary extensions of each other, see [\[4\]](#). Consequently, if a subgroup $\mathbb{E}$ of a non-abelian free group $\mathbb{F}$ is a free factor, then the inclusion map $\mathbb{E} \rightarrow \mathbb{F}$ is an elementary embedding.

Theorem 1.3. *Let S be a subset of a non-abelian free group $\mathbb{F}$ such that $\mathbb{F} = \text{def}_{\mathbb{F}}(S)$. Then $\langle S \rangle = \mathbb{F}$ or $\langle S \rangle$ is not a free factor of $\mathbb{F}$.*

In [\[5\]](#) it is shown that if $\langle S \rangle$ is abelian then the group $G = \text{def}_G(S)$ is abelian. Then, it is asked if the same is true for the case of nilpotent $\langle S \rangle$. The answer is negative as the Sylow 2-subgroup H of $K = \text{SL}_2(3)$ (the special linear group of 2×2 matrices over the field with 3 elements) defines K logically: since we have $C_{\text{Aut}(K)}(H) = 1$ (see also [\[1\]](#), last paragraph of Section 1), and hence, using [\[5, Corollary 1.3\]](#) we see that H defines K . But obviously K is not nilpotent. To show that $C_{\text{Aut}(K)}(H) = 1$, one may use GAP [\[6\]](#) by applying the following codes.

```
H:=SL(2,3);
K:=SylowSubgroup(H,2);
A:=AutomorphismGroup(H);
Size(Filtered(A,x->Size(Set(Filtered(K,k->k^x=k)))=8))=8);
```

As a final note, we have to mention that there is a connection between logical generation of groups and the so called concept of Aut-basis which is studied in [\[1\]](#). If $G = \text{def}_G(H)$ then the subgroup H is an Aut-basis of G in terms of [\[1\]](#), i.e., every automorphism of G which is identity on H , is already identity on G . The converse is not true of course, because the notion of logical generation is stronger than the property of being Aut-basis: in logical generation, every automorphism of every elementary extension which is identity on H is also identity on G , but in the case of Aut-basis, we only consider the automorphisms of the original group G . We give an example of an Aut-basis which is not logical generator. This means that the property $G = \text{def}_G(H)$ for subgroup H is stronger than being Aut-basis

for H . However, two concepts are the same in the case of finite groups. This example is proposed to us by Emil Jerabek.

Example. Consider the additive group of profinite integers $G = (\hat{\mathbb{Z}}, +)$. Then the subset $S = \{1\}$ is an Aut-basis of this group. However, G is not logically generated by S as it is not countable. The same is also true for the case of the additive group of p -adic integers for every prime p . As Emil Jerabek mentioned us, here we have an intermediate property: every pair of distinct elements in these groups can be distinguished by a first order formula with parameters from S . This means that for each distinct pair $a, b \in G$, there is a first order formula $\varphi(x, S)$ having parameters in S , such that $\varphi(a, S)$ is true in G but $\varphi(b, S)$ is not (see [3]). This is already called the property of being Leibnizian by A. Enayat, [2].

2. Proofs

We start with the proof of the first theorem. Recall that for a finite nilpotent group, all of its maximal subgroups are normal of a prime index.

Proof of Theorem 1.1. For any $j \in \Lambda$, suppose S_j is the projection of S in G_j . We prove that $G_j = \text{def}_{G_j}(S_j)$. We know that $G = (\text{Dr}_{i \neq j} G_i) \times G_j$. If $G_j \neq \text{def}_{G_j}(S_j)$ then there will be a non-trivial automorphism α of G_j such that $\alpha(s) = s$ for every $s \in S_j$. Consider $\varphi = (\text{id}, \alpha)$ which is a non-trivial automorphism of G . Obviously, for any $s \in S$ we have $\varphi(s) = s$ and this is a contradiction, showing that G_j is logically generated by S_j .

Now, suppose $H = \langle S \rangle$ and $H \neq G$. Suppose there exists an index j such that $\pi_j(H)$, the projection of H on the j -th components is not whole G_j . This means that there exists a maximal subgroup $M \leq G_j$ such that G_j/M is the cyclic group of order p_j and $\pi_j(H) \subseteq M$. Note that $M \neq 1$ as otherwise we could have $\pi_j(H) = 1$ which implies that $S_j = \{1\}$. But this means that G_j is logically definable by the empty set. This happens only in the case when $G_j = 1$ or $\mathbb{Z}_2$. So $M \neq 1$. Let $g \in G_j \setminus M$ be an arbitrary element. Then every element of G_j has a unique decomposition of the form mg^k for some k with $0 \leq k \leq p_j - 1$ and $m \in M$. Let z be an arbitrary central element of G_j with the order p_j . We may also assume that $z \in M$ as M intersects the center of G_j non-trivially. Define a map $\alpha : G_j \rightarrow G_j$ by $\alpha(mg^k) = m(gz)^k$. It can be verified that this map is a non-trivial automorphism of G_j . But the restriction of α to M is identity and consequently, its restriction to S_j is already identity. This violates the fact that S_j is a logical generator of G_j . As a result, for every j we have $\pi_j(H) = G_j$ and this means that $G_j = \langle S_j \rangle$ and consequently

$$G = \langle \bigcup_{j \in \Lambda} S_j \rangle.$$

Now, we show that for every j we have $S_j \subseteq \langle S \rangle$. Suppose $x \in S_j$. Then there exists a sequence $(x_i)_{i \in \Lambda} \in S$ such that $x_j = x$ and $x_i = 1$ for almost all $i \in \Lambda$. Suppose $|G_i| = p_i^{n_i}$ and let

$$m = \prod_{i \neq j, x_i \neq 1} p_i^{n_i}.$$

Then we have $(x_i)^m = x^m$. But m and $p_j^{n_j}$ are coprime. Therefore, we have $x = (x_i)^{mk} \in S$ for some integer k . This shows that S is contained in $\langle \bigcup_j S_j \rangle$ and hence

$$\langle \bigcup_j S_j \rangle = \langle S \rangle.$$

This contradicts our assumption $H \neq G$ and hence S is an algebraic generator of G .

Proof of Proposition 1.2. Let $g \in G$ be an arbitrary element. By our assumption, there exists a quantifier-free formula $\varphi(x, s_1, \dots, s_n)$ with parameters $s_1, \dots, s_n \in S$ such that

$$\{g\} = \{u \in G : G \models \varphi(u, s_1, \dots, s_n)\}.$$

Let

$$\overline{G} = \langle g, s_1, \dots, s_n \rangle,$$

and consider the subset $\bar{S} = \{s_1, \dots, s_n\}$. Then $\bar{G}$ is finite and nilpotent. As the formula φ does not have any quantifier, so

$$\{g\} = \{u \in \bar{G} : \bar{G} \models \varphi(u, s_1, \dots, s_n)\}.$$

So, g is $\bar{S}$ -definable in $\bar{G}$. Consequently, every group word $w(g, s_1, \dots, s_n)$ is also $\bar{S}$ -definable in $\bar{G}$. This means that $\bar{G} = \text{def}_{\bar{G}}(\bar{S})$. So, by [Theorem 1.1](#), we have $\bar{G} = \langle \bar{S} \rangle$. This shows that g is a word in the generator $s_1, \dots, s_n$, and hence $G = \langle S \rangle$.

Proof of Theorem 1.3. Consider a non-abelian free group $\mathbb{F}$ and suppose $\text{def}_{\mathbb{F}}(S) = \mathbb{F}$ and $\langle S \rangle = \mathbb{E}$ (recall that any subgroup of a free group is free). Suppose also that $\mathbb{E}$ is a free factor of $\mathbb{F}$. We show that $\mathbb{E} = \mathbb{F}$. Suppose $g \in \mathbb{F}$. As g is S -definable in $\mathbb{F}$, there is a formula $\varphi(x, S)$ such that

$$\mathbb{F} \models \forall x(x = g \leftrightarrow \varphi(x, S)).$$

Suppose now that $\mathbb{E} \models \forall x \neg \varphi(x, S)$. By Kharlampovich-Myasnikov-Sela $\mathbb{E}$ is an elementary subgroup of $\mathbb{F}$ so, we have $\mathbb{F} \models \forall x \neg \varphi(x, S)$, contradicting the fact $\mathbb{F} \models \varphi(g, S)$. Hence there is an element $h \in \mathbb{E}$ such that $\mathbb{E} \models \varphi(h, S)$, and again we conclude that $\mathbb{F} \models \varphi(h, S)$. By uniqueness, we see that $g = h$ and this means that $g \in \mathbb{E}$, proving $\mathbb{E} = \mathbb{F}$.

As a final note, we have to emphasize that the above result will be false if we drop the assumption of being free factor for $\mathbb{E}$. As an example, consider the free group $\mathbb{F}_2 = \langle a, b \rangle$. Then $S = \{a, b^2\}$ generates $\mathbb{F}_2$ logically but obviously not algebraically.

Acknowledgments

We would like to thank the referee for his/her comments and suggestions.

References

- [1] Cutolo, G., Nicotera, Ch. (2003). Subgroups defining automorphisms in locally nilpotent groups. *Forum Math.* 15(4):489–506.
- [2] Enayat, A. (2004). Leibnizian models of set theory. *J. Symbolic Logic* 69(3):775–789.
- [3] Jerabek, E. (2019). Rigid models of Presburger arithmetic. *Math. Logic Q.* 65(1):108–115.
- [4] Kharlampovich, O., Myasnikov, A. (1998). Tarski's problem about elementary theory of free groups has a positive solution. *Electron. Res. Announcements Amer. Math. Soc.* 4:101–108.
- [5] Shahryari, M. (2015). On logically cyclic groups. *J. Group Theory* 18(2):263–272.
- [6] The GAP Group. (2022). GAP – Groups, Algorithms, and Programming, Version 4.12.2. <https://www.gap-system.org>.