Definability of group theoretic notions

ARI KOPONEN and KERKKO LUOSTO

Abstract

We consider logical definability of the group-theoretic notions of simplicity, nilpotency and solvability on the class of finite groups. On one hand, we show that these notions are definable by sentences of deterministic transitive closure logic DTC. These results are based on known group-theoretic results. On the other hand, we prove that simplicity, nilpotency and the normal closure of a subset of a group are not definable by single sentences of first order logic FO. In addition, we show that an isomorphism between two arbitrary finite abelian groups can be expressed by a sentence of DTC(I), where DTC(I) is DTC enhanced with the equicardinality quantifier I, and that it is not expressible by a sentence of $\mathcal{L}^{\omega}_{\infty\omega}$.

1 Introduction

Descriptive complexity theory is a branch of Finite model theory in which expressive power of various logics is studied on the class of finite models. Descriptive complexity theory and computational complexity theory have a close connection. For example on the class of ordered structures a property is definable by a sentence of deterministic transitive closure logic DTC if and only if it belongs to the complexity class LOGSPACE. In Computational group theory one studies groups using computers (see e.g. [15]). Undoubtedly, questions about computational complexity of group theoretic notions have become more and more relevant. One promising approach to these complexity issues is to use tools developed by finite model theorists in descriptive complexity theory.

In this article our aim is to study definability of group theoretic notions on the class of finite groups. Definability issues of group theoretic notions have not been studied widely. However we list some results from the literature concerning simplicity, nilpotency and solvability (see Definition 3.1). It is known (see e.g. the book [12], page 284, ex. 13) that simplicity is not definable by a sentence of FO on the class of all groups. On the other hand, J. Wilson [22] and U. Felgner [9] proved that it is definable by a sentence of FO on the class of finite non-abelian groups. The proof uses the classification of finite simple groups. A. Macintyre [14] showed, that "the subgroup generated by $x_1, \ldots, x_n$ is simple" is expressible by a formula of FO on the class of algebraically closed groups. In addition, the following is a consequence of the Indecomposability theorem of B. Zil'ber [24] (see e.g. [5]): If $\mathbb{G}$ is a group of finite Morley rank and $\mathbb{H}$ is elementarily equivalent with $\mathbb{G}$, then $\mathbb{H}$ is simple if and only if $\mathbb{G}$ is simple. X. Caicedo [6] has showed independently from us that nilpotency and solvability are definable by sentences of LFP on the class of finite groups. Christian Rauth [16] did his Masters thesis on expressibility of transitive closure

1991 *Mathematics Subject Classification* 03C13, 03C20, 20A15.

This work was supported by grant 99516044 from the Academy of Finland and by a grant from the British Council and CIMO. The first author was partially supported by a grant from the Foundation of Vilho, Yrjö and Kalle Väisälä of the Academy of Science in Finland. The second author was partially supported by a grant from the University of Helsinki.

logic on abelian groups. J. Wilson [23] pointed out that nilpotency and solvability are axiomatizable by the following infinite sets of sentences of FO

$$\{\forall x \forall y (x^a = 1 \wedge y^b = 1 \rightarrow xy = yx) : a, b \in \mathbb{N} \text{ are coprimes}\}$$

and

$$\{\forall x \forall y (x^a = 1 \wedge y^b = 1 \wedge (xy)^c = 1 \rightarrow x = 1) : a, b, c \in \mathbb{N} \text{ are coprimes}\}$$

on the class of finite groups. The former uses basic group theory and the latter follows from the classical article [21] of J. Thompson. J. Wilson continues: "It seems hard to decide whether there exist two single sentences whose classes of finite models are the class of finite nilpotent groups and the class of finite soluble groups."

Even if groups are usually thought to be models for the vocabulary $\{1, \cdot\}$ where $\cdot$ is a binary function symbol, we take groups to be models for the vocabulary $\{1, R\}$ where R is a ternary relation symbol interpreting the group operation. This is because in the usual vocabulary it is possible to express computationally complex properties so that the formula in question does not reflect to the logical structure of the sentence such as quantifier rank. By the quantifier rank of a sentence we simply mean the number of nested quantifiers in the sentence. For example the property "in a group there is an element of order n" can be expressed by a sentence

$$\exists x (x \neq 1 \wedge \ldots \wedge \overbrace{(\ldots (x \cdot x) \cdot \ldots \cdot x)}^{n-1 \ times} \neq 1 \wedge \overbrace{(\ldots (x \cdot x) \cdot \ldots \cdot x)}^{n \ times} = 1)$$

with the quantifier rank 1 in the usual vocabulary $\{1, \cdot\}$, whereas in the vocabulary $\{1, R\}$, the normal way to write down this sentence is

$$\begin{aligned} \exists x_1 \cdots \exists x_n (\quad & R(x_1, x_1, x_1) \wedge R(x_2, x_1, x_3) \wedge \ldots \wedge R(x_{n-1}, x_1, x_n) \wedge \\ & x_1 \neq 1 \wedge x_2 \neq 1 \wedge \ldots \wedge x_{n-1} \neq 1 \wedge x_n = 1 \quad) \end{aligned}$$

with the quantifier rank n. In the new vocabulary the logical structure of a formula corresponds better to the computational complexity of the property it expresses. However, even if we theoretically think of sentences as written in the relational vocabulary, we use standard group theoretic notation when we need to write down real formulas, simply for the sake of readability. The translation to the relational language is always straightforward to do.

From the point of view of computational complexity it is relevant how one represents a group as an input to a Turing machine. In computational group theory it is usual, at least when one deals with larger groups, that one gives only the generators of the group and a rule how to generate new elements. In finite model theory one uses a multiplicative table representation. So, in a Turing machine there is one input tape for the universe of a group and another for the relation. The size of the representation of a group of size n is then about $n + n^3$.

In section 2 we define the logics and the corresponding games used in this article. In section 3 we prove definability results for simplicity, nilpotency and solvability on the class of finite groups. In section 4 we prove that simplicity, nilpotency and the normal closure of a subset of a group are not definable by sentences of FO on the class of finite groups. These undefinability results use the ultraproduct constructions from classical model theory. We give a short introduction to ultraproducts in Section 4.1. In section 5 we define the Isomorphism problem of finite abelian groups and show that it is definable by a sentence of DTC(I) and, on the other hand that it is not definable by a sentence of $\mathcal{L}^{\omega}_{\infty\omega}$.

$\mathbb{N}$ is the set of natural numbers and $\mathbb{N}^* := \mathbb{N}\setminus\{0\}$. We use the normal group theoretic shorthand notation such as $\mathbb{H} \leq \mathbb{G}$ meaning that $\mathbb{H}$ is a subgroup of $\mathbb{G}$ and $\mathbb{H}\trianglelefteq\mathbb{G}$ meaning that $\mathbb{H}$ is a normal subgroup of $\mathbb{G}$.

2 Logics and games

We assume the reader has some familiarity with first order logic FO, i.e., the standard logic for predicate calculus. The formulas of FO are constructed using the connectives $\neg$, $\wedge$ and the quantifier $\exists$. The connectives $\vee$, $\rightarrow$ and $\leftrightarrow$ and the quantifier $\forall$ can be defined using the former ones. $\models$ is the satisfaction relation. For example, the meaning of the following relation is, that the group $\mathbb{G}$ is abelian:

$$\mathbb{G} \models \forall x \forall y (xy = yx).$$

We next give the definitions of deterministic transitive closure logic DTC, transitive closure logic TC, least fixpoint logic LFP, infinitary logic with finite number of variables $\mathcal{L}^{\omega}_{\infty\omega}$ and deterministic transitive closure logic enhanced with Härtig (or equicardinality) quantifier DTC(I). At the end we give the definitions of EF-game and pebble game. For a more comprehensive account to logics and games, see e.g. [8].

Transitive closure logics

Let $k \geq 1$ and X be a $2k$-ary relation on a finite set A. The deterministic transitive closure $DTC[X]$ of X is defined by

$$\begin{aligned} DTC[X] \;:=\; & \{(\overline{a},\overline{b}) \in A^{2k} : \text{there exist } n > 0 \text{ and } \overline{e_0},\ldots,\overline{e_n} \in A^k \text{ such that } \overline{a} = \overline{e_0}, \\ & \overline{b} = \overline{e_n}, \text{ and for all } i < n, \overline{e_{i+1}} \text{ is the unique } \overline{e} \text{ for which } (\overline{e_i},\overline{e}) \in X\}. \end{aligned}$$

The transitive closure $TC[X]$ of X is defined by

$$\begin{aligned} TC[X] \;:=\; & \{(\overline{a},\overline{b}) \in A^{2k} : \text{there exist } n > 0 \text{ and } \overline{e_0},\ldots,\overline{e_n} \in A^k \text{ such that } \overline{a} = \overline{e_0}, \\ & \overline{b} = \overline{e_n}, \text{ and for all } i < n, (\overline{e_i},\overline{e}_{i+1}) \in X\}. \end{aligned}$$

For a vocabulary τ the class of formulas of DTC of vocabulary τ is given by the calculus of FO with the additional rule

$$\frac{\varphi}{[\mathsf{DTC}_{\bar{x},\bar{y}}\varphi]\bar{s}\bar{t}},$$

where the variables in $\overline{x}$ and $\overline{y}$ are pairwise distinct and where the tuples $\overline{x},\overline{y},\overline{s}$ and $\overline{t}$ are all of the same length, $\overline{s}$ and $\overline{t}$ being tuples of terms. Note that we use upper case roman letters for the logic DTC, italic letters for the deterministic transitive closure of a set and sans serif letters for the deterministic transitive closure operator as a part of the syntax of the logic DTC.

For TC the last rule is replaced by the rule

$$\frac{\varphi}{[\mathsf{TC}_{\bar{x},\bar{y}}\varphi]\bar{s}\bar{t}}$$

with the same conditions for the tuples. The semantics is defined inductively with respect to the calculus above, the meaning of $\mathbb{A} \models [\mathsf{DTC}_{\overline{x},\overline{y}}\varphi(\overline{x},\overline{y})]\overline{s}\overline{t}$ and $\mathbb{A} \models [\mathsf{TC}_{\overline{x},\overline{y}}\varphi(\overline{x},\overline{y})]\overline{s}\overline{t}$ being

$$(\overline{s},\overline{t}) \in DTC[\{(\overline{x},\overline{y}) : \mathbb{A} \models \varphi(\overline{x},\overline{y})\}]$$

and

$$(\overline{s},\overline{t}) \in TC[\{(\overline{x},\overline{y}) : \mathbb{A} \models \varphi(\overline{x},\overline{y})\}],$$

respectively.

Examples: (i) The following formula of DTC defines the subgroup generated by a single element x of a group, i.e., the relation $y \in \langle x \rangle$:

$$[\mathsf{DTC}_{ab}ax = b]1y.$$

(ii) We originally proved that the subgroup generated by a subset of a group is definable by a formula of least fixed point logic LFP. When we mentioned it to A. Andersson, he observed [1], that the result can be strengthened to TC:

Lemma 2.1. *If $\mathbb{G}$ is a group, $\emptyset \neq S \subseteq G$ and the relation $x \in S$ is definable by a formula of* TC*, then also the relation $x \in \langle S \rangle$ is definable by a formula of* TC.

Proof. The formula defining the relation $x \in \langle S \rangle$ is as follows:

$$[\mathsf{TC}_{ab}\, \exists g(g \in S \wedge ag = b)](1,x). \ \square$$

Least fixpoint logic

Let $\mathbb{A}$ be a τ-model and $\varphi = \varphi(x_1,\ldots,x_k,\overline{y},X,\overline{Y})$ a $\tau \cup \{X\}$-formula where the arity of the relation variable X is k. The operation $F^\varphi : \mathcal{P}(A^k) \to \mathcal{P}(A^k)$ is defined in the following way:

$$F^\varphi(R) := \{(a_1,\ldots,a_k) \in A^k : \mathbb{A} \models \varphi(a_1,\ldots,a_k,\overline{b},R,\overline{S})\}.$$

A relation $R \subseteq A^k$ is called a fixpoint of the operation F^φ, if $F^\varphi(R) = R$. If in addition R is contained in every fixpoint of F^φ, it is called the least fixpoint of F^φ.

The operation F^φ determines a sequence

$$\emptyset, F^\varphi(\emptyset), F^\varphi(F^\varphi(\emptyset)), \ldots$$

We denote the elements of the sequence by $B_0^\varphi, B_1^\varphi, \ldots$. If there is a minimal $n_0 \in \mathbb{N}$ such that $F^\varphi(B_{n_0}^\varphi) = B_{n_0}^\varphi$, then $B_m^\varphi = B_{n_0}^\varphi$ for every $m \geq n_0$. The set $B_{n_0}^\varphi$ is then called the inductive fixpoint of F^φ and it is denoted by B_∞^φ. If there is an even number of negation symbols in front of each occurrence of X, then the operation F^φ is monotone, i.e., $F^\varphi(R) \subseteq F^\varphi(S)$ provided that $R \subseteq S \subseteq A^k$. Then the inductive fixpoint of the operation F^φ is the least fixpoint.

The class of formulas of LFP of the vocabulary τ is given by the calculus of FO with the additional rule

$$\frac{\varphi}{[\mathsf{LFP}_{\overline{x},X}\varphi]\overline{t}},$$

where, in the formula φ, we require that the number of negation symbols in front of each occurrence of X is even and where the lengths of $\overline{x}$ and $\overline{t}$ are the same and coincide with the arity of X. The semantics is defined inductively with respect to the calculus above, the meaning of $\mathbb{A} \models [\mathsf{LFP}_{\overline{x},X}\varphi]\overline{t}$ being

$$\overline{t} \in B^{\varphi}_{\infty}.$$

For example the following formula of LFP defines the subgroup generated by a subset S of a group, assuming S is definable by a formula of LFP:

$$\Big[\mathsf{LFP}_{x,X}\Big(x \in S \vee \exists y \exists z(y \in S \wedge z \in X \wedge x = yz)\Big)\Big]y.$$

Infinitary logics

The class of formulas of $\mathcal{L}_{\infty\omega}$ of the vocabulary τ is given by the calculus of FO and allowing infinitary disjunctions and conjunctions. $\mathcal{L}^{\omega}_{\infty\omega}$ is the restriction of $\mathcal{L}_{\infty\omega}$ to the class of formulas with only finite number of variables. For example the following formula of $\mathcal{L}_{\infty\omega}$ says that in a group the order of every element is finite:

$$\forall x \Bigg(\bigvee_{i \in \mathbb{N}^*} x^i = 1 \Bigg).$$

Härtig quantifier

The class of formulas of DTC(I) of the vocabulary τ is given by the calculus of DTC with the additional rule

$$\frac{\varphi(x), \psi(y)}{Ix, y(\varphi(x), \psi(y))},$$

where the Härtig quantifier I binds the variable x in $\varphi(x)$ and the variable y in $\psi(y)$. The semantics is defined inductively with respect to the calculus above, the meaning of $Ix, y(\varphi(x), \psi(y))$ being that in a model there is the same number of elements x satisfying $\varphi(x)$ as elements y satisfying $\psi(y)$. For example the following formula of DTC(I) says that in a group the number of elements in the conjugacy class of g is the same as the number of elements in the conjugacy class of h:

$$Ix, y(\exists k(x = k^{-1}gk), \exists k(y = k^{-1}hk)).$$

Games

We next define the Ehrenfeucht-Fraïssé game, which is called the EF-game for short, and the pebble game. Let $\mathbb{A}$ and $\mathbb{B}$ be τ-models and $k \in \mathbb{N}^*$.

The EF-game with k rounds between the models $\mathbb{A}$ and $\mathbb{B}$ runs as follows. There are two players, the player I and the player II. For every round n, $n \leq k$, the player I chooses an element from one of the models. The player II responds by choosing an element from the other model. Suppose that the players have chosen the elements $a_1, \ldots, a_k \in A$ and the respective elements $b_1, \ldots, b_k \in B$. If $\mathbb{A} \upharpoonright \{a_1, \ldots, a_k\}$ is isomorphic with $\mathbb{B} \upharpoonright \{b_1, \ldots, b_k\}$ where the isomorphism is determined by the mapping $a_i \mapsto b_i$, $i \in \{1, \ldots, k\}$, then the player II wins the EF-game. Otherwise the player I wins.

The k-pebble game between the models $\mathbb{A}$ and $\mathbb{B}$ is as follows. There are again two players, the player I and the player II. There are k pairs of pebbles and the number of rounds is not limited. Suppose that in the round i, $i \in \mathbb{N}$, the pairs $(a_{i_1}, b_{i_1}), \ldots, (a_{i_n}, b_{i_n})$, $n \leq k$, of pebbles are placed on the elements of the models such that a_{i_j} is on the element $a'_{i_j} \in A$ and b_{i_j} is on the element $b'_{i_j} \in B$, $j \in \{1, \ldots, n\}$. The player I can either remove a pair of played pebbles (if $n > 0$) or put a pebble ($a_{i_{n+1}}$ or $b_{i_{n+1}}$) on an element ($a'_{i_{n+1}} \in A$ or $b'_{i_{n+1}} \in B$) of one of the models (if $n < k$). The player II responds by placing the corresponding element on an element of the other model. If $\mathbb{A} \restriction \{a'_{i_1}, \ldots, a'_{i_{n+1}}\}$ is not isomorphic with $\mathbb{B} \restriction \{b'_{i_1}, \ldots, b'_{i_{n+1}}\}$ where the isomorphism is determined by the mapping $a'_{i_j} \mapsto b'_{i_j}$, $j \in \{1, \ldots, n+1\}$, then the player I wins the game. Otherwise the player I continues the game in the way described above. If the player I does not win after any finite number of rounds then the player II wins.

The proofs for the following theorems can be found in [8].

Theorem 2.2. *A model class $\mathcal{C}$ is definable by a sentence of* FO *if and only if there exists $k \in \mathbb{N}$ such that if $\mathbb{A} \in \mathcal{C}$ and $\mathbb{B} \notin \mathcal{C}$, then the player I has a winning strategy in the* EF*-game with k rounds between the models $\mathbb{A}$ and $\mathbb{B}$.*

Theorem 2.3. *A model class $\mathcal{C}$ is definable by a sentence of $\mathcal{L}^{\omega}_{\infty\omega}$ if and only if there exists $k \in \mathbb{N}$ such that if $\mathbb{A} \in \mathcal{C}$ and $\mathbb{B} \notin \mathcal{C}$, then the player I has a winning strategy in the k-pebble game between the models $\mathbb{A}$ and $\mathbb{B}$.*

3 Definability results

In this section we discuss definability of simplicity, nilpotency and solvability on the class of finite groups. We first show that simplicity is definable by a sentence of DTC on the class of finite abelian groups, that it is definable by a sentence of TC on the class of all finite groups and that nilpotency and solvability are definable by sentences of LFP on the class of all finite groups. To prove these results we need only elementary facts of group theory. We then show, using celebrated group theoretic results, such as Classification Theorem of finite simple groups and Odd Order Theorem, that simplicity, nilpotency and solvability are actually all definable by sentences of DTC on the class of all finite groups.

For the record we define the central group theoretic notions used in this paper.

Definition 3.1. Let $\mathbb{G}$ be a group.

(i) If H is a subset of G, then $\langle H \rangle$ is the subgroup of $\mathbb{G}$ generated by H.

(ii) If H is a subset of G, then $C_{\mathbb{G}}(H)$ is the *centralizer* of H in $\mathbb{G}$, i.e. the set

$$\{x \in G : xy = yx \text{ for every } y \in H\}.$$

(iii) $Z(\mathbb{G})$ is the centre of $\mathbb{G}$, i.e. the set $C_{\mathbb{G}}(G)$.

(iv) If H is a subset of G, then the *normal closure* of H in $\mathbb{G}$, $H^{\mathbb{G}}$, is the smallest normal subgroup of $\mathbb{G}$ containing H.

(v) A group is *simple*, if it is non-trivial and has no non-trivial proper normal subgroups.

(vi) A sequence $(\mathbb{G}_0, \ldots, \mathbb{G}_n)$,

$$1 = \mathbb{G}_0 \trianglelefteq \mathbb{G}_1 \trianglelefteq \cdots \trianglelefteq \mathbb{G}_n = \mathbb{G}, \tag{1}$$

$i \in \{0, \ldots, n\}$, $n \in \mathbb{N}$, is called a *subnormal series* of $\mathbb{G}$, $n \in \mathbb{N}$.

(vii) If $\mathbb{G}_i \trianglelefteq \mathbb{G}$ and $\mathbb{G}_{i+1}/\mathbb{G}_i \leq Z(\mathbb{G}/\mathbb{G}_i)$ for every $i \in \{0, \ldots, n-1\}$, then (1) is a *central series* of $\mathbb{G}$. A group is *nilpotent*, if it has a central series.

(viii) A group $\mathbb{G}$ is *solvable*, if it has a subnormal series (1), where every factor $\mathbb{G}_{i+1}/\mathbb{G}_i$ is abelian, $i \in \{0, \ldots, n-1\}$.

We first consider simplicity.

Proposition 3.2. *(i) Simplicity is definable by a sentence of* DTC *on the class of finite abelian groups.*

(ii) Simplicity is definable by a sentence of TC *on the class of finite groups.*

Proof. (i) If $\mathbb{G}$ is a finite abelian group, it is simple if and only if every nontrivial element generates the whole group. Hence the following sentence of DTC defines simplicity on the class of finite abelian groups:

$$\exists x(x \neq 1) \wedge \forall x \Big(x \neq 1 \rightarrow \forall y([\mathsf{DTC}_{ab}\; ax = b](1, y)) \Big).$$

(ii) We observe that $\mathbb{G}$ is simple if and only if $\mathbb{G} \neq 1$ and $\langle x \rangle^{\mathbb{G}} = \mathbb{G}$ for every $x \in G \setminus \{1\}$. By Lemma 2.1, this leads to a characterization of simplicity by the following sentence of TC on the class of finite groups:

$$\exists x(x \neq 1) \wedge \forall x \left(x \neq 1 \rightarrow \forall y \left(\left[\mathsf{TC}_{ab} \exists g(a(g^{-1}xg) = b) \right](1, y) \right) \right). \qquad \square$$

In the following we examine nilpotency.

Definition 3.3. Let $\mathbb{G}$ be a finite group.

(i) The *commutator* of an ordered pair of elements x and y of $\mathbb{G}$ is the element $[x, y] := x^{-1}y^{-1}xy$.

(ii) If H and K are subsets of $\mathbb{G}$, then the corresponding *commutator subgroup* is

$$[\mathbb{H}, \mathbb{K}] := \langle \{[x, y] \in G : x \in H, y \in K\} \rangle.$$

(iii) *The lower central series* of $\mathbb{G}$ is defined by recursion:

$$\Gamma_n(\mathbb{G}) := \begin{cases} \mathbb{G} & \text{, if } n = 1, \\ [\Gamma_{n-1}(\mathbb{G}), \mathbb{G}] & \text{, if } n > 1. \end{cases}$$

Because $\mathbb{G}$ is supposed to be finite, there exists an integer n_0 such that $\Gamma_n(\mathbb{G}) = \Gamma_{n_0}(\mathbb{G})$ for every integer $n \geq n_0$.

Proposition 3.4. *Nilpotency is definable by a sentence of* LFP *on the class of finite groups.*

Proof. It is well-known (see e.g. [17]) that the following two properties are equivalent:

(i) $\mathbb{G}$ is nilpotent;

(ii) $\Gamma_n(\mathbb{G}) = 1$ for some integer $n > 0$.

Hence, nilpotency is definable by a sentence that says that every nontrivial element of $\mathbb{G}$ belongs to the set $G \setminus \Gamma_n(G)$ for some $n \in \mathbb{N}^*$, i.e., by the sentence

$$\forall x\Big(x \neq 1 \to [\mathsf{LFP}_{x,X}\varphi(x,X)]x\Big)$$

of LFP, where

$$\varphi(x,X) := \neg\Bigg(\Big[\mathsf{LFP}_{x,Y}\exists y \exists z\Big((\neg Xy \wedge [y,z]=x) \vee (Yy \wedge Yz \wedge yz = x)\Big)\Big]x\Bigg).$$

By an easy induction, it follows that $B_n^{\varphi} = G \setminus \Gamma_{n+1}(\mathbb{G})$ after n rounds of iteration. Indeed, given that the interpretation of X is $G \setminus \Gamma_{n+1}(\mathbb{G})$, the least fixed point operator in $\varphi(x,X)$ generates the elements of the form $[y_1,z_1]\dots[y_k,z_k]$, $k \in \mathbb{N}^*$, where $y_i \in \Gamma_{n+1}(\mathbb{G})$ and $z_i \in G$, $i \in \{1,\dots,k\}$. □

We next prove a corresponding result for solvability.

Definition 3.5. *The derived series* of a finite group G is defined by recursion:

$$\mathbb{G}^{(n)} := \begin{cases} \mathbb{G} & \text{, if } n = 0, \\ [\mathbb{G}^{(n-1)}, \mathbb{G}^{(n-1)}] & \text{, if } n > 0. \end{cases}$$

Because $\mathbb{G}$ is supposed to be finite, there exists an integer n_0 such that $\mathbb{G}^{(n)} = \mathbb{G}^{(n_0)}$ for every integer $n \geq n_0$.

Proposition 3.6. *Solvability is definable by a sentence of* LFP *on the class of finite groups.*

Proof. It is well-known that the following two properties are equivalent:

(i) $\mathbb{G}$ is solvable;

(ii) $\mathbb{G}^{(n)} = 1$ for some $n \in \mathbb{N}$.

Complementing each side of the equation (ii) we see that solvability is definable by the sentence

$$\forall x\Big(x \neq 1 \to [\mathsf{LFP}_{x,X}\varphi(x,X)]x\Big)$$

of LFP, where

$$\varphi(x,X) := \neg\Bigg(\Big[\mathsf{LFP}_{x,Y}\exists y \exists z\Big((\neg Xy \wedge \neg Xz \wedge [y,z]=x) \vee (Yy \wedge Yz \wedge yz = x)\Big)\Big]x\Bigg).$$

By an easy induction, it follows that $B_n^{\varphi} = G \setminus G^{(n)}$ after n rounds of iteration. Indeed, given that the interpretation of X is $G \setminus G^{(n)}$, the least fixed point operator in $\varphi(x,X)$ generates the elements of the form $[y_1,z_1]\dots[y_k,z_k]$, $k \in \mathbb{N}^*$, where $y_i, z_i \in G^{(n)}$ and $i \in \{1,\dots,k\}$. □

Thus far we have only used elementary facts of group theory. At the end of this section we show that simplicity, nilpotency and solvability are actually definable by sentences of DTC on the class of finite groups. The results use the classification of finite simple groups and a corollary of the main theorem of the article by J. Thompson [21]. The article [21] is a successor of the article of W. Feit and J. Thompson [11], where they proved the celebrated Odd Order Theorem.

The following theorem is proved by J. Wilson [22] and U. Felgner [9]. The essential point, which uses the classification, is that the commutator subgroup of a finite non-abelian simple group is definable by a sentence of FO, i.e., there exists an integer k such that any element in any finite non-abelian simple group is a product of at most k commutators.

Theorem 3.7. *Simplicity is definable by a sentence of* FO *on the class of finite nonabelian groups.*

Thus we get the following.

Corollary 3.8. *Simplicity is definable by a sentence of* DTC *on the class of finite groups.*

Proof. This follows directly from (i) of 3.2 and 3.7. □

The order of an element x of a group is denoted by $o(x)$. Note that we can express that the order of x divides the order of y by the following formula of DTC:

$$o(x) \mid o(y) := \forall z([\mathsf{DTC}_{acbd}\ ax = b \wedge cy = d](1,1,z,1) \to z = 1).$$

It says that if in the sequence

$$(1,1),(x,y),(x^2,y^2),\dots,(x^n,y^n),\dots$$

the element y^n is the neutral element, then so is x^n.

The following theorem is proved for example in [20].

Theorem 3.9. *Suppose that* $\mathbb{G}$ *is a finite group. Then the following properties are equivalent:*

(i) G *is nilpotent;*

(ii) if $x, y \in G$ *and* $\gcd(o(x), o(y)) = 1$, *then* $xy = yx$.

Thus we get the following.

Corollary 3.10. *Nilpotency is definable by a sentence of* DTC *on the class of finite groups.*

Proof. By Theorem 3.9 the following sentence of DTC defines nilpotency on the class of finite groups:

$$\forall x \forall y \Big(\forall z \Big((o(z) \mid o(x)) \wedge (o(z) \mid o(y)) \to z = 1 \Big) \to xy = yx \Big). \ \square$$

The following is proved by J. Thompson [21].

Theorem 3.11. *Suppose that* $\mathbb{G}$ *is a finite group. Then the following properties are equivalent:*

(i) G *is solvable;*

(ii) if $x, y, z \in G \setminus \{1\}$ *and* $\gcd(o(x), o(y)) = \gcd(o(x), o(z)) = \gcd(o(y), o(z)) = 1$, *then* $xyz \neq 1$.

As in corollary of 3.10, we get the following.

Corollary 3.12. *Solvability is definable by a sentence of* DTC *on the class of finite groups.* □

4 Undefinability results

In this section we prove using ultraproducts that simplicity, nilpotency and the normal closure of a subset of a group are not definable by sentences of FO on the class of finite groups. It may be worth noting that we use infinite models to prove undefinability results on the class of finite models.

4.1 Ultraproducts

A comprehensive introduction to ultraproducts can be found in C. Chang's and H. Keisler's book [7]. We represent the central facts of ultraproducts tailored for groups as they are represented in the article of J. Wilson [23].

Let I be an infinite set and $U \subsetneq \mathcal{P}(I)$. U is a *filter* over I, if I is one of the elements of U and if U is closed under intersections and supersets. If, in addition, for every $X \in \mathcal{P}(I)$,

$$X \in U \text{ if and only if } I \setminus X \notin U,$$

the filter U is an *ultrafilter* over I. If an ultrafilter U is generated by a single element of $\mathcal{P}(I)$, i.e., $U = \{X \subseteq I : a \in X\}$ for some $a \in I$, U is *principal.* Otherwise it is *non-principal.* It is well-known that if I is an arbitrary infinite set, there exists a non-principal ultrafilter over I. Then U contains the filter

$$\{X \in \mathcal{P}(I) : I \setminus X \text{ is finite}\}.$$

Suppose that U is an ultrafilter over an infinite set I, and that $\mathbb{G}_i$, $i \in I$, are groups. The cartesian product of the groups $\mathbb{G}_i$, $i \in I$, is the group

$$\mathbb{G} := \prod_{i \in I} \mathbb{G}_i$$

where the elements are functions

$$g : I \to \bigcup_{i \in I} G_i$$

such that $g(i) \in G_i$ for every $i \in I$ and where the group operation is the natural generalization of the group operation of the direct product of two groups. The elements $g, h \in G$ are U-equivalent, $g \equiv_U h$, if

$$\{i \in I : g(i) = h(i)\} \in U.$$

Note that $\equiv_U$ is an equivalence relation over the set G. The equivalence class determined by $g \in G$ is denoted by g_U. It is easy to see, that

$$\mathbb{K} = \{g \in G : g \equiv_U 1_{\mathbb{G}}\} \trianglelefteq \mathbb{G}.$$

The *ultraproduct* of groups $\mathbb{G}_i$, $i \in I$, is the group

$$\prod_U \mathbb{G}_i := \mathbb{G}/\mathbb{K}.$$

If I is countably infinite, U is a non-principal ultrafilter over I, and $\mathbb{G}_i$, $i \in I$, are countable, then the ultraproduct $\prod_U \mathbb{G}_i$ is either finite or has the size of continuum. For the proof see e.g. [7].

Łoś's theorem is the main theorem of ultraproducts. The following is Łoś's theorem formulated for groups.

Theorem 4.1. *Suppose that $\mathbb{G}_i$, $i \in I$, are groups, U is an ultrafilter over I and*

$$\mathbb{G} = \prod_U \mathbb{G}_i.$$

Then for every formula $\varphi(x_1, \ldots, x_n) \in FO$ and for all elements $g_{1U}, \ldots, g_{nU} \in G$ the following holds:

$$\mathbb{G} \models \varphi(g_{1U}, \ldots, g_{nU}) \textit{ if and only if } \{i \in I : \mathbb{G}_i \models \varphi(g_1(i), \ldots, g_n(i))\} \in U.$$

4.2 Simplicity

Let $\mathbb{G}$ be an abelian group, $\mathbb{Z}$ the set of integers and $\mathbb{Q}$ the set of rational numbers. We use the standard vocabulary $\{0, +\}$ when we are discussing abelian groups.

Note that a group is torsionfree, if it satisfies the axiom $\theta_n := \forall x(nx = 0 \to x = 0)$ for every $n \in \mathbb{N}^*$, and divisible, if it satisfies the axiom $\delta_n := \forall x \exists y(ny = x)$ for every $n \in \mathbb{N}^*$.

We use Łoś's theorem to prove the following theorem. $\mathbb{P}$ is the set of prime numbers.

Theorem 4.2. *Simplicity is not definable by a sentence of* FO *on the class of finite groups.*

Proof. It is well-known that the theory of torsionfree divisible abelian groups is κ-cathegorical for every uncountable κ (see e.g. [12]). Also it is obvious that $\mathbb{Z}_p$ is simple and $\mathbb{Z}_{p^2}$ is not simple for every $p \in \mathbb{P}$.

Antithesis: There is a sentence φ of FO such that φ defines simplicity on the class of finite groups. Let U be a non-principal ultrafilter on $\mathbb{P}$, and let

$$\mathbb{G}_1 := \prod_U \mathbb{Z}_p \text{ and } \mathbb{G}_2 := \prod_U \mathbb{Z}_{p^2}.$$

Let $n \in \mathbb{N}^*$ be fixed. $\mathbb{Z}_p \models \theta_n$, $\mathbb{Z}_p \models \delta_n$, $\mathbb{Z}_{p^2} \models \theta_n$ and $\mathbb{Z}_{p^2} \models \delta_n$ for every prime number $p > n$. This implies that

$$\{p \in \mathbb{P} : \mathbb{Z}_p \models \theta_n \text{ and } \mathbb{Z}_p \models \delta_n\} \in U$$

and

$$\{p \in \mathbb{P} : \mathbb{Z}_{p^2} \models \theta_n \text{ and } \mathbb{Z}_{p^2} \models \delta_n\} \in U,$$

since the sets are cofinite and U is non-principal. By Łoś's theorem the abelian groups $\mathbb{G}_1$ and $\mathbb{G}_2$ are torsionfree and divisible. Because

$$|G_1| = |G_2| = 2^\omega,$$

by the cathegoricity $\mathbb{G}_1 \cong \mathbb{G}_2$. On the other hand $\mathbb{G}_1 \models \varphi$ and $\mathbb{G}_2 \not\models \varphi$. A contradiction. $\square$

By the proof of proposition 3.2 simplicity can be characterized using the notion of normal closure on the class of finite groups. By the theorem 3.7 simplicity is definable by a sentence of FO on the class of finite non-abelian groups. One might think that also the normal closure, which is closely related to simplicity, could be defined by a sentence of FO on the class of finite non-abelian groups. We show in the section 4 that this is not the case. So the result of Wilson and Felgner is even more surprising.

4.3 Nilpotency

A dihedral group $\mathbb{D}_n$ is defined to be an abstract group which is isomorphic with the automorphism group of the cycle with n nodes. Obviously the order of $\mathbb{D}_n$ is $2n$ and it is generated by the elements ρ and ϵ, where the order of ρ is n and the order of ϵ is two. By the following lemma elementary equivalence of dihedral groups $\mathbb{D}_m$ and $\mathbb{D}_n$ can be reduced to the study of elementary equivalence of groups $\mathbb{Z}_m$ and $\mathbb{Z}_n$.

Lemma 4.3. *If $\mathbb{Z}_m \equiv_l \mathbb{Z}_n$, then $\mathbb{D}_m \equiv_l \mathbb{D}_n$.*

Proof. By Theorem 2.2 it is enough to show that the player II has a winning strategy in the EF-game of l rounds between groups $\mathbb{D}_m$ and $\mathbb{D}_n$. The idea of the proof is, that simultaneously with the actual play, one also plays an imaginary phantom play between groups $\mathbb{Z}_m$ and $\mathbb{Z}_n$. Suppose that $\mathbb{D}_m$ is generated by the elements ϵ_1 and ρ_1 and $\mathbb{D}_n$ is generated by ϵ_2 and ρ_2, $o(\epsilon_1) = o(\epsilon_2) = 2$, $o(\rho_1) = m$ and $o(\rho_2) = n$.

Suppose that the player I chooses an element $\epsilon_1^i \rho_1^j \in D_m$, $i \in \{0, 1\}$ and $j \in \{0, \ldots, m-1\}$. In the phantom play one chooses the element $j \in Z_m$. The player II has a winning strategy in the EF-game of l rounds between groups $\mathbb{Z}_m$ and $\mathbb{Z}_n$. Thus one chooses the element $k \in Z_n$ given by the winning strategy. Now the player II chooses $\epsilon_2^i \rho_2^k \in D_n$. If the player I chooses an element from D_n instead of choosing an element from D_m, one plays in a similar way.

Suppose that the players have chosen the elements $x_1, \ldots, x_{l'} \in D_m$ and $y_1, \ldots, y_{l'} \in D_n$, $l' \in \{1, \ldots, l\}$, and that the elements $x'_1, \ldots, x'_{l'} \in Z_m$ and $y'_1, \ldots, y'_{l'} \in Z_n$ correspond to the elements $x_1, \ldots, x_{l'}$ and $y_1, \ldots, y_{l'}$. By the assumption $x'_{i_1} x'_{i_2} = x'_{i_3}$ if and only if $y'_{i_1} y'_{i_2} = y'_{i_3}$, $i_1, i_2, i_3 \in \{1, \ldots, l'\}$. The aim is to show that $x_{i_1} x_{i_2} = x_{i_3}$ if and only if $y_{i_1} y_{i_2} = y_{i_3}$. The first equation is true only if there are modulo two the same number of ϵ_1 in both sides of the first equation, and the second equation is true only if there are modulo two the same number of ϵ_2 in both sides of the second equation. Thus it is enough to go through the following four cases. In the rest of the eight cases the equivalence trivially holds. Suppose that $j_1, j_2, j_3 \in \{0, \ldots, m-1\}$ and $k_1, k_2, k_3 \in \{0, \ldots, n-1\}$.

(*i*) $x_{i_1} = \rho_1^{j_1}$, $x_{i_2} = \rho_1^{j_2}$, $x_{i_3} = \rho_1^{j_3}$, $y_{i_1} = \rho_2^{k_1}$, $y_{i_2} = \rho_2^{k_2}$, $y_{i_3} = \rho_2^{k_3}$:

$$\rho_1^{j_1} \rho_1^{j_2} = \rho_1^{j_3} \text{ iff } j_1 +_m j_2 = j_3 \text{ iff } k_1 +_n k_2 = k_3 \text{ iff } \rho_2^{k_1} \rho_2^{k_2} = \rho_2^{k_3}.$$

(*ii*) $x_{i_1} = \epsilon_1 \rho_1^{j_1}$, $x_{i_2} = \rho_1^{j_2}$, $x_{i_3} = \epsilon_1 \rho_1^{j_3}$, $y_{i_1} = \epsilon_2 \rho_2^{k_1}$, $y_{i_2} = \rho_2^{k_2}$, $y_{i_3} = \epsilon_2 \rho_2^{k_3}$:

$$\epsilon_1 \rho_1^{j_1} \rho_1^{j_2} = \epsilon_1 \rho_1^{j_3} \text{ iff } j_1 +_m j_2 = j_3 \text{ iff } k_1 +_n k_2 = k_3 \text{ iff } \epsilon_2 \rho_2^{k_1} \rho_2^{k_2} = \epsilon_2 \rho_2^{k_3}.$$

(*iii*) $x_{i_1} = \rho_1^{j_1}$, $x_{i_2} = \epsilon_1 \rho_1^{j_2}$, $x_{i_3} = \epsilon_1 \rho_1^{j_3}$, $y_{i_1} = \rho_2^{k_1}$, $y_{i_2} = \epsilon_2 \rho_2^{k_2}$, $y_{i_3} = \epsilon_2 \rho_2^{k_3}$:

$$\rho_1^{j_1} \epsilon_1 \rho_1^{j_2} = \epsilon_1 \rho_1^{j_3} \text{ iff } j_2 = j_1 +_m j_3 \text{ iff } k_2 = k_1 +_n k_3 \text{ iff } \rho_2^{k_1} \epsilon_2 \rho_2^{k_2} = \epsilon_2 \rho_2^{k_3}.$$

(*iv*) $x_{i_1} = \epsilon_1 \rho_1^{j_1}$, $x_{i_2} = \epsilon_1 \rho_1^{j_2}$, $x_{i_3} = \rho_1^{j_3}$, $y_{i_1} = \epsilon_2 \rho_2^{k_1}$, $y_{i_2} = \epsilon_2 \rho_2^{k_2}$, $y_{i_3} = \rho_2^{k_3}$:

$$\epsilon_1 \rho_1^{j_1} \epsilon_1 \rho_1^{j_2} = \rho_1^{j_3} \text{ iff } j_2 = j_1 +_m j_3 \text{ iff } k_2 = k_1 +_n k_3 \text{ iff } \epsilon_2 \rho_2^{k_1} \epsilon_2 \rho_2^{k_2} = \rho_2^{k_3}. \square$$

The proofs for the following theorems can be found in the book of I. Kaplansky [13]. For the original or first published proofs he refers to R. Baer [3], [4] and L. Zippin [25]

Theorem 4.4. *A divisible subgroup of an abelian group is a direct summand.*

Theorem 4.5. *Any abelian group $\mathbb{G}$ has a unique largest divisible subgroup $\mathbb{H}$, and $\mathbb{G} = \mathbb{K} + \mathbb{H}$ where $\mathbb{K}$ has no divisible subgroups.*

Let $\mathbb{N}^+$ be the set $\mathbb{N} \setminus \{0, 1, 2\}$. The definition of a function p in the next lemma is the following:

$$p : \mathbb{N}^+ \to \mathbb{N},\ p(i) \text{ is the least prime number greater than } i.$$

Lemma 4.6. *If U is a non-principal ultrafilter on the set $\mathbb{N}^+$,*

$$\mathbb{G}_1 := \prod_U \mathbb{Z}_{2^i} \text{ and } \mathbb{G}_2 := \prod_U \mathbb{Z}_{2^i p(i)},$$

then $\mathbb{G}_1 \cong \mathbb{G}_2$.

Proof. By the previous theorem $\mathbb{G}_1 \cong \mathbb{V}_1 + \overline{\mathbb{V}}_2$, where $\mathbb{V}_1$ does not contain divisible subgroups and $\overline{\mathbb{V}}_2$ is the unique largest divisible subgroup of $\mathbb{G}_1$. The torsion subgroup $\mathbb{V}_2$ of $\overline{\mathbb{V}}_2$ is divisible, so by Theorem 4.4 we have that $\overline{\mathbb{V}}_2 \cong \mathbb{V}_2 + \mathbb{V}_3$. The numbers 2^i and $p(i)$ are relative primes for every $i \in \mathbb{N}^+$. If $\mathbb{V}_4 := \prod_U \mathbb{Z}_{p(i)}$, then

$$\mathbb{G}_2 = \prod_U \mathbb{Z}_{2^i p(i)} \cong \prod_U (\mathbb{Z}_{2^i} + \mathbb{Z}_{p(i)}) = \mathbb{G}_1 + \mathbb{V}_4.$$

Because the cardinality of the set of torsionfree divisible elements in $\mathbb{G}_1$ is 2^ω, the torsionfree divisible abelian groups $\mathbb{V}_3$ and $\mathbb{V}_3 + \mathbb{V}_4$ are of the same uncountable cardinality. Thus they are isomorphic and

$$\mathbb{G}_1 \cong \mathbb{V}_1 + \mathbb{V}_2 + \mathbb{V}_3 \cong \mathbb{V}_1 + \mathbb{V}_2 + \mathbb{V}_3 + \mathbb{V}_4 \cong \mathbb{G}_2. \square$$

We use Łoś's theorem and the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ defined in the previous lemma to prove the following theorem.

Theorem 4.7. *Nilpotency is not definable by a sentence of* FO *on the class of finite groups.*

Proof. Antithesis: There is a sentence φ of FO such that φ defines nilpotency on the class of finite groups. Suppose that the quantifier rank of φ is l. For $i \in \mathbb{N}^+$, $\mathbb{D}_{2^i}$ is nilpotent but $\mathbb{D}_{2^i p(i)}$ is not. Thus $\mathbb{D}_{2^i} \not\equiv_l \mathbb{D}_{2^i p(i)}$ for all $i \in \mathbb{N}^+$. By Lemma 4.3 also $\mathbb{Z}_{2^i} \not\equiv_l \mathbb{Z}_{2^i p(i)}$. There is up to equivalence only a finite number of sentences with quantifier rank at most l. Hence there is at least one sentence ψ of FO with quantifier rank l such that

$$\{i \in \mathbb{N}^+ : \mathbb{Z}_{2^i} \models \psi\} \in U$$

and

$$\{i \in \mathbb{N}^+ : \mathbb{Z}_{2^i p(i)} \models \psi\} \notin U.$$

By Łoś's theorem $\mathbb{G}_1 \models \varphi$ and $\mathbb{G}_2 \not\models \varphi$, in contradiction with Lemma 4.6. $\square$

4.4 Normal closure

Centres of finite nonabelian simple groups are trivial. As we mentioned in chapter 3, simplicity is definable by a sentence of FO on the class of finite nonabelian groups. In this section we show that the normal closure of a subset of a group, a notion which is closely related to simplicity, is not definable by a formula of FO even on the class of finite groups with trivial centres.

Proposition 4.8. *The normal closure of a single element x of a group is not definable by a formula $\varphi(x, y)$ of* FO

(i) on the class of finite groups, or even

(ii) on the class of finite groups with trivial centres.

Here the non-definability means that there is $\mathbb{G}$ in the corresponding class such that $\langle\{x\}\rangle^{\mathbb{G}} \neq \{y \in G : \mathbb{G} \models \varphi(x, y)\}$.

Proof. (i) Suppose that there is such a $\varphi(x, y)$ with quantifier rank k. By the proof of Theorem 4.2 it is clear that there is $p \in \mathbb{P}$ such that $\mathbb{Z}_p \equiv_{k+2} \mathbb{Z}_{p^2}$. Hence, there is $g \in \mathbb{Z}_p \setminus \{0\}$ such that $\langle \mathbb{Z}_p, g\rangle \equiv_{k+1} \langle \mathbb{Z}_{p^2}, p\rangle$. Note that there is an automorphism that maps g onto the element 1. This implies

$$\langle \mathbb{Z}_p, 1\rangle \equiv_{k+1} \langle \mathbb{Z}_p, g\rangle \equiv_{k+1} \langle \mathbb{Z}_{p^2}, p\rangle.$$

On the other hand, the normal closure of 1 is the whole group in $\mathbb{Z}_p$, and that of p is $\mathbb{G} \cong \mathbb{Z}_p$ in $\mathbb{Z}_{p^2}$. Hence

$$\mathbb{Z}_p \models \forall y \varphi(1, y) \text{ and } \mathbb{Z}_{p^2} \not\models \forall y \varphi(p, y).$$

Since the quantifier rank of $\forall y \varphi(x, y)$ is $k + 1$, this is a contradiction.

(ii) Suppose that there is such a $\varphi(x, y)$ with quantifier rank k, and suppose that $\mathbb{D}_n$ is a dihedral group of order $2n$, where $n \in \mathbb{N} \setminus \{0, 1, 2\}$ is odd. Because the rotation subgroup of $\mathbb{D}_n$ does not contain involutions, it is easy to see that any involution of $\mathbb{D}_n$ does not commute with any element of the rotation subgroup. Hence the centre of $\mathbb{D}_n$ is trivial.

As in the case (i), it can be shown that there is $p \in \mathbb{P}$ such that $\langle \mathbb{Z}_{p^2}, 1\rangle \equiv_{k+1} \langle \mathbb{Z}_{p^2}, p\rangle$. By the proof of 4.3, we have that $\langle \mathbb{D}_{p^2}, \rho\rangle \equiv_{k+1} \langle \mathbb{D}_{p^2}, \rho^p\rangle$, where ρ is a generator of the rotation subgroup of $\mathbb{D}_{p^2}$. However, the normal closure of ρ is $\mathbb{G} \cong \mathbb{Z}_{p^2}$ in $\mathbb{D}_{p^2}$, and that of ρ^p is $\mathbb{G}' \cong \mathbb{Z}_p$ in $\mathbb{D}_{p^2}$. Hence

$$\mathbb{D}_{p^2} \models \forall y(y^2 \neq 1 \to \varphi(\rho, y)) \text{ and } \mathbb{D}_{p^2} \not\models \forall y(y^2 \neq 1 \to \varphi(\rho^p, y)).$$

Since the quantifier rank of $\forall y(y^2 \neq 1 \to \varphi(x, y))$ is $k + 1$, this is a contradiction. □

5 The Isomorphism problem of finite abelian groups

In this section we define the Isomorphism problem of finite abelian groups, show that it is definable by a sentence of DTC(I), and that it is not definable by a sentence of $\mathcal{L}^{\omega}_{\infty\omega}$.

For groups $\mathbb{G}$ and $\mathbb{H}$ the disjoint pair $\mathbb{G} \sqcup \mathbb{H}$ is the model

$$(G \sqcup H, G, H, +_G \sqcup +_H, 0_G, 0_H)$$

of the vocabulary $\{A, B, R, 0, 0'\}$, where $G \sqcup H$ is the disjoint union of the universes of $\mathbb{G}$ and $\mathbb{H}$, A and B are unary relations interpreting the universes of $\mathbb{G}$ and $\mathbb{H}$, R is a ternary relation interpreting the disjoint union of the group operations of $\mathbb{G}$ and $\mathbb{H}$, and 0 and $0'$ are elements corresponding to the neutral elements of $\mathbb{G}$ and $\mathbb{H}$.

The Isomorphism problem of groups is simply the question whether two arbitrarily chosen groups are isomorphic or not. The Isomorphism problem of groups is definable by a sentence of a logic $\mathcal{L}$, if the following condition is satisfied: there is a sentence φ of $\mathcal{L}$ such that for all groups $\mathbb{G}$ and $\mathbb{H}$,

$$\mathbb{G} \sqcup \mathbb{H} \models \varphi \text{ if and only if } \mathbb{G} \cong \mathbb{H}.$$

In the Isomorphism problem of finite abelian groups we restrict to the class of finite abelian groups.

For $n \in \mathbb{N}^*$, denote by G_n the set of elements of the group $\mathbb{G}$ of order n. If $p \in \mathbb{P}$, $\mathbb{G}^p$ is the subgroup of $\mathbb{G}$ generated by the elements of the set $G_p \cup G_{p^2} \cup \cdots$.

Proposition 5.1. *Let $\mathbb{G}$ and $\mathbb{H}$ be finite abelian groups. If $|G_{p^i}| = |H_{p^i}|$ for every $p \in \mathbb{P}$ and $i \in \mathbb{N}$, then $\mathbb{G} \cong \mathbb{H}$.*

Proof. It is well-known that every finite abelian group is isomorphic to a group of the form

$$\underbrace{(\mathbb{Z}_{p_1^{a_{11}}} \times \cdots \times \mathbb{Z}_{p_1^{a_{1b_1}}})}_{G^{p_1}} \times \cdots \times \underbrace{(\mathbb{Z}_{p_n^{a_{n1}}} \times \cdots \times \mathbb{Z}_{p_n^{a_{nb_n}}})}_{G^{p_n}},$$

where $n, p_i, a_{ij}, b_i \in \mathbb{N}$, p_i is the i'th prime, $j \in \{1, \ldots, b_i\}$, $i \in \{1, \ldots, n\}$ and $a_{ik} \leq a_{il}$ if and only if $k \leq l$, $k, l \in \{1, \ldots, b_i\}$.

Antithesis: $\mathbb{G} \ncong \mathbb{H}$. Suppose that p is the greatest prime such that $\mathbb{G}^p \ncong \mathbb{H}^p$. Then the preceding characterization implies that $\mathbb{G}^p \cong \mathbb{G}' \times \mathbb{G}''$ and $\mathbb{H}^p \cong \mathbb{H}' \times \mathbb{H}''$, where $\mathbb{G}'' \cong \mathbb{H}''$, $\mathbb{G}' \ncong \mathbb{H}'$ and for some positive integer s, the order of every element of $\mathbb{G}'$ is less than p^s, the order of every element of $\mathbb{H}'$ is at most p^s and the order of some element of $\mathbb{H}'$ is p^s. Let $l = |\{x \in H' : o(x) = p^s\}| \neq 0$ and $k = |\{x \in H'' : o(x) = p^s\}|$. The number of elements of order p^s in $\mathbb{G}$ is $k|\mathbb{G}'|$ contradicting the fact that the number of elements of order p^s in $\mathbb{H}$ is $k|\mathbb{H}'| + l|\mathbb{H}''| - kl$. □

Corollary 5.2. *The Isomorphism problem of finite abelian groups is definable by a sentence of* DTC(I).

Proof. By the previous theorem the isomorphism class of an abelian group $\mathbb{G}$ is determined by the numbers $|G_n|$, $n \in \mathbb{N}^*$. Hence the Isomorphism problem of finite abelian groups can be defined by the following sentence of DTC(I):

$$\forall x \Big(Iyz\Big(A(y) \wedge (o(y) \mid o(x)) \wedge (o(x) \mid o(y)), B(z) \wedge (o(z) \mid o(x)) \wedge (o(x) \mid o(z))\Big)\Big)$$

where

$$o(x) \mid o(y) := \forall z([\mathsf{DTC}_{acbd}\ a + x = b \wedge c + y = d](0, 0, z, 0) \rightarrow z = 0). \ \square$$

The following is proved in [18]: if p is an odd prime, there is a pair of nonisomorphic groups of order p^3 with the same number of elements of each order. Hence the sentence in the previous proof does not define e.g the Isomorphism problem of finite nilpotent groups.

By the following theorem the Isomorphism problem of finite abelian groups is not definable by a sentence of DTC, TC, LFP or $\mathcal{L}^{\omega}_{\infty\omega}$.

Theorem 5.3. *If $\mathbb{G} = \overbrace{\mathbb{Z}_2 + \cdots + \mathbb{Z}_2}^{n \text{ times}}$ and $\mathbb{H} = \overbrace{\mathbb{Z}_2 + \cdots + \mathbb{Z}_2}^{n+1 \text{ times}}$, $n \in \mathbb{N}^*$, then $\mathbb{G} \equiv_{\mathcal{L}^n_{\infty\omega}} \mathbb{H}$ and consequently $\mathbb{G} \sqcup \mathbb{G} \equiv_{\mathcal{L}^n_{\infty\omega}} \mathbb{G} \sqcup \mathbb{H}$.*

Proof. The groups $\mathbb{G}$ and $\mathbb{H}$ can be considered as n- and $n+1$-dimensional vector spaces over the field $\mathbb{Z}_2$. By Theorem 2.3 it is enough to show that the player II has a winning strategy in the n-pebble game between the groups $\mathbb{G}$ and $\mathbb{H}$.

Suppose that before the round i, $i \in \mathbb{N}$, the players have chosen the elements $x_{i_1}, \dots, x_{i_m} \in G$ and $y_{i_1}, \dots, y_{i_m} \in H$, $m \in \{0, \dots, n\}$. Assume as an induction hypothesis that there is an isomorphism f_i between the subspaces $\overline{G}$ and $\overline{H}$ generated by the chosen elements such that the restriction to $\{x_{i_1}, \dots, x_{i_m}\}$ is the following partial isomorphism:

$$0_G \mapsto 0_H \text{ and } x_{i_j} \mapsto y_{i_j},\ j \in \{1, \dots, m\}.$$

If the player I puts a pebble on $x \in \overline{G}$, the player II puts a pebble on $y \in \overline{H}$; and if the player I puts a pebble on $y \in \overline{H}$, the player II puts a pebble on $x \in \overline{G}$, where $f_i(x) = y$. If the player I removes a pebble, the player II acts in a corresponding way. The remaining case is that the player I puts a pebble on $x \in G \setminus \overline{G}$ (or on $y \in H \setminus \overline{H}$, which is treated similarly). The cardinality of a generating set of H is $n+1$. Hence the player II is able to put a pebble on $y \in H \setminus \overline{H}$. Because x and y are linearly independent from $x_{i_1}, \dots, x_{i_m}$ and $y_{i_1}, \dots, y_{i_m}$, the isomorphism f_i can be extended to an isomorphism

$$f_{i+1} : \overline{\overline{G}} \cong \overline{\overline{H}},$$

where $\overline{\overline{G}}$ and $\overline{\overline{H}}$ are generated by $x_{i_1}, \dots, x_{i_m}, x$ and $y_{i_1}, \dots, y_{i_m}, y$, and the restriction of f_{i+1} to $\{x_{i_1}, \dots, x_{i_m}, x\}$ satisfies the following partial isomorphism:

$$0_G \mapsto 0_H,\ x_{i_j} \mapsto y_{i_j},\ j \in \{1, \dots, m\},\ x \mapsto y. \ \square$$

6 Conclusion

We have collected the results from sections 3, 4 and 5 to the following table. The notation '$-$' means undefinability and '$+$' means definability on the class of finite groups.

	FO	DTC	TC	LFP	$\mathcal{L}^{\omega}_{\infty\omega}$	DTC(I)
Normal closure	$-$	?	$+$	$+$	$+$	?
Simplicity (abelian)	$-$	$+$	$+$	$+$	$+$	$+$
Simplicity (non-abelian)	$+$	$+$	$+$	$+$	$+$	$+$
Nilpotency	$-$	$+$	$+$	$+$	$+$	$+$
Solvability	?	$+$	$+$	$+$	$+$	$+$
Isom. problem (abelian)	$-$	$-$	$-$	$-$	$-$	$+$

At the end we list some open problems:

(i) It seems that the normal closure of a subset of a group is not definable by a sentence of DTC on the class of finite groups.

(ii) J. Wilson posed the question in [23] whether nilpotency and solvability are definable by single sentences of FO on the class of finite groups or not. The answer is negative for nilpotency, but the question for solvability is still open.

(iii) The undefinability results of simplicity and nilpotency are proved indirectly. It would be interesting to see a winning strategy for duplicator in EF-game e.g. between groups $\mathbb{Z}_p$ and $\mathbb{Z}_p \times \mathbb{Z}_p$, $p \in \mathbb{P}$, which would be a direct proof for undefinability of simplicity in FO on the class of finite groups.

(iv) The application of the deterministic transitive closure operator in the formula $o(x) \mid o(y)$ is vectorized in the sense that the corresponding relation is between pairs (x, y) of elements. Jörg Flum posed a question whether such formulas can be replaced with ones without vectorization.

Acknowledgement

This article is based on the Licentiate thesis of the first author in the University of Helsinki 1998. We are grateful to Anders Andersson, Lauri Hella and Juha Nurmonen for their valuable comments and suggestions on the manuscript of the paper. We also want to give a special thank to Iain Stewart who made it possible to collaborate with people at the Department of Mathematics and Computer science in the University of Leicester.

References

[1] A. ANDERSSON, Personal communication.

[2] M. ASCHBACHER and R. GURALNICK, 'Some applications of the first cohomology group', *J. Algebra* 90 (1984) 446-460.

[3] R. BAER, 'The subgroup of elements of finite order of an abelian group', *Ann. of Math.* 37 (1936) 766-781.

[4] R. BAER, 'Abelian groups that are direct summands of every containing abelian group', *Bull. Amer. Math. Soc.* 46 (1940) 800-806.

[5] A. BOROVIK and A. NESIN, *Groups of Finite Morley Rank* (Oxford University Press, New York, 1994).

[6] X. CAICEDO, 'Finite model theory and computational complexity', *Apuntes matematicos* 32, Universidad de los Andes, 1995.

[7] C. C. CHANG and H. J. KEISLER, *Model Theory* (North Holland, Amsterdam-New York, 1973).

[8] H-D EBBINGHAUS and J. FLUM, *Finite model theory* (Springer, Berlin, 1995).

[9] U. FELGNER, 'Pseudo-endliche Gruppen', *Proceedings of the 8th Easter Conference on Model Theory* (Humboldt-Universität, Berlin, 1990) 82-96.

[10] L. FUCHS, *Infinite abelian groups* (Academic Press, 1970).

[11] W. FEIT and J. THOMPSON, 'Solvability of groups of odd order', *Pacific J. Math.* 13 (1963) 775-1029.

[12] W. HODGES, *Model theory* (Cambridge University Press, 1993).

[13] I. KAPLANSKY, *Infinite abelian groups* (The University of Michigan Press, 1960).

[14] A. MACINTYRE, 'On algebraically closed groups', *Ann. of Math.* (2) 96 (1972) 53-97.

[15] J. NEUBUSER, 'An invitation to computational group theory', *Groups '93 - Galway/St. Andrews, volume 212 of London Math. Soc. Lecture Note Ser.*, pages 457-475 (ed. C. M. Campbell, T. C. Hurley, E. F. Robertson, S. J. Tobin and J. J. Ward, Cambridge University Press, 1995).

[16] C. RAUTH, *Zur Ausdrucksstärke der Transitiven-Hülle-Logik in abelschen Gruppen*, Diplomarbeit, Universität Freiburg, 1994.

[17] J. S. ROSE, *A course on group theory*, (Dover, 1994).

[18] R. SCAPELLATO, 'Finite groups with the same number of elements of each order', *Rendiconti di Matematica*, Serie VII, Volume 8, Roma (1988) 339-344.

[19] M. SUZUKI, *Group theory I* (Springer-Verlag, 1982.

[20] M. SUZUKI, *Group theory II* (Springer-Verlag, 1986).

[21] J. G. THOMPSON, 'Nonsolvable finite groups all of whose local subgroups are solvable (Part I)', *Bull.Amer.Math.Soc.* 74 (1968) 383-437.

[22] J. WILSON, 'On simple pseudofinite groups', *J. London Math. Soc.* (2) 51 (1995) 471-490.

[23] J. WILSON, 'First-Order Group Theory', *Infinite Groups '94* (ed. de Giovanni and Newell, Walter de Gruyter & Co, Berlin-New York, 1995).

[24] B. ZIL'BER, 'Groups and rings whose theory is categorical', *Fund. Math.* 95 (1977) 173-188. In Russian.

[25] L. ZIPPIN, 'Countable torsion groups', *Ann. of Math.* 36 (1935) 86-99.

Department of Mathematics
P.O. Box 4 (Yliopistonkatu 5)
00014 University of Helsinki
Finland
email: {ari.koponen, kerkko.luosto}@helsinki.fi