LOGICALLY CYCLIC FINITE GROUPS ARE CYCLIC

M. SHAHRYARI

Abstract. A group $G$ is called logically cyclic, if it contains an element $s$ such that every element of $G$ can be defined by a first order formula with parameter $s$. We will prove that if such a group is also finite, then it is cyclic in the ordinary sense.

AMS Subject Classification Primary 20A15, Secondary 03C07 and 03C98.

Key Words Definability; Elementary extensions; Logically cyclic groups; Svenonius’s theorem.

Let $\mathcal{L} = (\cdot, ^{-1}, 1)$ be the language of groups. Suppose $G$ is a group and $S \subseteq G$. We extend $\mathcal{L}$ to a new language $\mathcal{L}(S)$, by attaching new constant symbols $a_s$, for any $s \in S$. So we have $\mathcal{L}(S) = \mathcal{L} \cup \{a_s : s \in S\}$. Then, $G$ becomes an $\mathcal{L}(S)$-structure if we let $s$ be the interpretation of $a_s$ in $G$. Now, suppose $g \in G$ is an arbitrary element and there exists a first order formula $\varphi(x)$ in the language $\mathcal{L}(S)$ (with a free variable $x$), such that

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

Then we say that $g$ is definable by the elements of $S$ or $S$-definable for short. Let $\text{def}_S(G)$ be the set of all $S$-definable elements of $G$. Clearly this subset is a subgroup. If we have $\text{def}_S(G) = G$, then we say that $S$ logically generates $G$. A logically cyclic group is a group which is logically generated by a single element. A cyclic group is then clearly logically cyclic as every element can be defined as a power of the generator. The converse is not true, for example the additive group of rationales, $G = (\mathbb{Q}, +)$, is logically cyclic as every element $g = m/n$ can be defined by the formula $nx = m$, which is clearly a first order formula having $s = 1$ as a parameter. In this note, we will prove that if a finite group is logically cyclic, then it is cyclic in the ordinary sense.

1. Preliminaries

We can use the definability theorem of Svenonius to study definable elements in groups. For the case of finite group, a version of this theorem
will be used which can be proved by an elementary argument. We briefly
discuss this well-known result of the model theory. Let $\mathcal{L}$ be a first order
language and $M$ be a structure in $\mathcal{L}$. An $n$-ary relation $R \subseteq M^n$
is said to be definable, if there exists a formula $\varphi(x_1,\ldots,x_n)$ in the language $\mathcal{L}$, such that

$$R = \{(x_1,\ldots,x_n) \in M^n : M \models \varphi(x_1,\ldots,x_n)\}.$$ 

It is easy to see that if $R$ is definable, then every automorphism of $M$
preserves $R$. To see what can be said about the converse, we need the
concept of elementary extension. For any $\mathcal{L}$-structure $M$, suppose $\text{Th}(M)$
is the first order theory of $M$, i.e. the set of all first order sentences, which
are true in $M$. We say that an $\mathcal{L}$-structure $M'$ is an elementary extension of $M$, if $M$
is a sub-structure of $M'$ and $\text{Th}(M) \subseteq \text{Th}(M')$. We are now ready
to review the theorem of Svenonius.

**Theorem 1.1.** A relation $R \subseteq M^n$ is definable if and only if every auto-
morphism of every elementary extension of $M$ preserves $R$.

For a proof, the reader can see [2]. Suppose we want to use this theorem in
the case of groups; we must assume that $G$ is a group, $S \subseteq G$ is an arbitrary
subset, and $\mathcal{L}(S)$ is the extended language of groups with parameters from $S$. Clearly a singleton set $\{g\}$ is a unary relation in $G$, so we can restate the
above theorem, for $S$-definability of elements in $G$.

**Corollary 1.2.** An element $g$ is $S$-definable in $G$ if and only if, for any
elementary extension $G'$ of $G$ and every automorphism $\alpha : G' \to G'$, if $\alpha$
fixes elements of $S$, then it fixes also $g$.

If $G$ is a finite group, then the only elementary extension of $G$ is $G$ itself,
because there exists a first order sentence which says that $G$ has $m$ elements
($m$ is the order of $G$), so any elementary extension of $G$ must have order $m$.
Hence, for the case of finite groups, we have

**Corollary 1.3.** An element $g$ is $S$-definable in a finite group $G$ if and only
if, for any automorphism $\alpha : G \to G$, if $\alpha$ fixes elements of $S$, then it fixes
also $g$.

Note that this very special case of Svenonius’s theorem can be proved
independently by an elementary argument. Here is the proof.

**Proof.** Let $g \in G$ be invariant under every automorphism which fixes ele-
ments of $S$. Let

$$G = \{g_1, g_2,\ldots,g_n\}$$

be an enumeration of the elements of $G$ such that $g_1 = 1$, $\{g_2,\ldots,g_m\} = S$
and $g_{m+1} = g$. Consider the Cayley table of $G$, i.e. determine the unique
numbers $\sigma(i,j)$ such that $g_ig_j = g_{\sigma(i,j)}$. Now we introduce a formula $\varphi(y)$
in the language $\mathcal{L}(S)$ as

$$\exists x_1, \ldots, x_n : (\bigwedge_{i \neq j} x_i \neq x_j) \land (\bigwedge_{i=2}^m x_i = g_i) \land x_1 = 1 \land (\bigwedge_{i,j} x_i x_j = x_{\sigma(i,j)}) \land (y = x_{m+1}).$$

We show that $\varphi(y)$ defines $g$. Let $a \in G$ be an element such that $G \models \varphi(a)$. Therefore there exist distinct elements $b_1, \ldots, b_n \in G$ such that

1- $b_1 = 1$ and $b_2 = g_2, \ldots, b_m = g_m$.
2- $b_{m+1} = a$.
3- $b_ib_j = b_{\sigma(i,j)}$.

Now, the map $f : G \rightarrow G$ defined by $f(g_i) = b_i$ is an automorphism, and for all $g_i \in S$ we have $f(g_i) = b_i = g_i$. So, $f$ must preserve $g$. Hence, we have $g = f(g) = f(g_{m+1}) = b_{m+1} = a$. This completes the proof. □

An automorphism $\alpha : G \rightarrow G$ is said to be an $S$-automorphism, if it fixes $S$ elementwise. If we work in the semidirect product $\hat{G} = \text{Aut}(G) \ltimes G$, then the set of all $S$-automorphisms of $G$ is just the centralizer $C_{\text{Aut}(G)}(S)$. We will use this type of centralizer notation in the rest of the article. So, for an arbitrary group, we have

$$\text{def}_S(G) \subseteq C_G(A),$$

where $A = C_{\text{Aut}(G)}(S)$. If $G$ is finite, then by the corollary 1.3, we have the equality

$$\text{def}_S(G) = C_G(A).$$

Suppose $G$ is logically cyclic. So $G = \text{def}_s(G)$ for some $s$. This shows that $G = C_G(A)$, therefore we have the implication

$$\forall \alpha \in \text{Aut}(G) : \alpha(s) = s \Rightarrow \alpha = \text{id}_G.$$  

For finite groups, 1.3 implies that the converse is also true, i.e. if there exists an element $s$ satisfying the above implication, then $G$ is logically cyclic. We prove that every logically cyclic group is abelian. Note that a similar argument shows that for any group $G$ and every element $s \in G$, the subgroup $\text{def}_s(G)$ is also abelian (see the discussion in the next section).

**Proposition 1.4.** Every logically cyclic group is abelian.

**Proof.** Let $G = \text{def}_s(G)$. Then as above

$$\forall \alpha \in \text{Aut}(G) : \alpha(s) = s \Rightarrow \alpha = \text{id}_G.$$  

So, considering the inner automorphism $\alpha : x \mapsto sx^{-1}$, we obtain $s \in Z(G)$. Now, let $g \in G$ be an arbitrary element and let $\beta : x \mapsto gxg^{-1}$. Since $[g, s] = 1$, so $\beta(s) = s$ and therefore $\beta = \text{id}_G$. This shows that $g \in Z(G)$ and hence $G$ is abelian. □
Note that if every element of $G$ is definable in the language of groups, $\mathcal{L}$, then we must have
\[ G = C_G(\text{Aut}(G)), \]
and in this case we have $\text{Aut}(G) = 1$, which shows that $G = 1, \mathbb{Z}_2$. So, the groups $1$ and $\mathbb{Z}_2$ are the only groups, every element in which, is definable in the language of groups.

As a final remark in this section, note that a finite group $G$, is logically cyclic, if and only if there exists an element $s \in G$ such that for all non-identity automorphism $\alpha$, we have $\alpha(s) \neq s$. In this case, if we consider the action of $\text{Aut}(G)$ on $G$, then
\[ |\text{Orb}(s)| = |\text{Aut}(G)|, \]
so, for finite logically cyclic groups, we have
\[ |\text{Aut}(G)| \leq |G|. \]

2. The main theorem

We are now ready to prove our main theorem.

**Theorem 2.1.** Let $G$ be a finite logically cyclic group. Then $G$ is cyclic.

**Proof.** As we said before, $G$ is abelian and so it is a direct product of abelian $p$-groups of the form
\[ H_p = \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_t}}, \]
where $p$ is a prime (ranging in the set of all prime divisors of $|G|$) and $1 \leq e_1 \leq \cdots \leq e_t$ are depending on $p$. Note that if a finite group $G = G_1 \times G_2$ is logically cyclic, then both $G_1$ and $G_2$ are logically cyclic. This is because, if for example $G_1$ is not logically cyclic, then (by 1.3) for all $s_1 \in G_1$, there exists a non-identity automorphism $\varphi_1 \in \text{Aut}(G_1)$, such that $\varphi_1(s_1) = s_1$. Hence for all $(s_1, s_2) \in G$, there exists the non-identity $(\varphi_1, \text{id}_{G_2}) \in \text{Aut}(G)$, such that
\[ (\varphi_1, \text{id}_{G_2})(s_1, s_2) = (s_1, s_2), \]
and this violates the logically cyclicity of $G$. The converse is also true if the orders of $G_1$ and $G_2$ are co-prime, since, in this case we have
\[ \text{Aut}(G) = \text{Aut}(G_1) \times \text{Aut}(G_2). \]

This argument shows that it is enough to assume that $G$ has the form
\[ \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_t}}. \]
By [1], the order of $\text{Aut}(G)$ can be computed as follows. Let
\[ d_i = \max\{j : e_j = e_i\}, \quad c_i = \min\{j : e_j = e_i\}. \]
Then we have
\[ |\text{Aut}(G)| = \prod_{i=1}^{t}(p^{d_i} - p^{i-1})p^{e_i(t-d_i)+(e_i-1)(t-c_i+1)}. \]
Suppose $t \geq 2$. Since $G$ is logically cyclic, so by the above observation, $A = \mathbb{Z}_{p^{d_1}} \times \mathbb{Z}_{p^{d_2}}$ is logically cyclic. We compute the order of $\text{Aut}(A)$, using the above formula. Note that, in the case of the group $A$, we have

$$1 \leq d_1 \leq 2, \quad d_2 = 2, \quad c_1 = 1, \quad 1 \leq c_2 \leq 2.$$ 

So, we have

$$|\text{Aut}(A)| = (p^{d_1} - 1)(p - 1)p^{d_1 + 3e_2 - d_1e_1 - 2c_2 + c_2 - 4}.$$ 

Applying the requirement $|\text{Aut}(A)| \leq |A|$, we obtain

$$(p^{d_1} - 1)(p - 1)p^{d_1 + 3e_2 - d_1e_1 + (2 - c_2)e_2 + 2} \leq p^4,$$

so we can consider some possibilities for $d_1$ and $d_2$.

1- First, note that the case $d_1 = 1$ and $c_2 = 1$ is impossible.

2- If $d_1 = 1$ and $c_2 = 2$, then we have

$$(p^{d_1} - 1)(p - 1)p^{3e_2 - e_1 - 2e_2 + 2} \leq p^4,$$

and hence

$$(p - 1)^2p^{2e_2 + 2} \leq p^4.$$ 

Now the case $e_1 > 1$ is impossible and hence $e_1 = 1$. This shows that $p = 2$ and hence $A = \mathbb{Z}_2 \times \mathbb{Z}_{2^f}$ for some $f \geq 2$. It is easy to see that $|\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_{2^f})| = 2^{f+1}$ and therefore the whole the group $A = \mathbb{Z}_2 \times \mathbb{Z}_{2^f}$ must be the orbit of $s$ under the action of its automorphism group, which is not the case. So, we get a contradiction.

3- Let $d_1 = 2$ and $c_2 = 1$. This shows that $e_1 = e_2$, and hence

$$(p^2 - 1)(p - 1)p^{2e_1 + 1} \leq p^4.$$ 

Again, the case $e_1 > 1$ is impossible and the case $e_1 = 1$ implies $(p^2 - 1)(p - 1) \leq p$ which is contradiction.

4- Finally, note that the case $d_1 = 2$ and $c_2 = 2$ is also impossible.

This argument shows that in all the cases, $t \geq 2$ is not valid. So $G$ is a direct product of cyclic groups of co-prime orders and hence it is cyclic. 

□

A caution is necessary here: the subgroup $\text{def}_s(G)$ is strongly dependent to $G$. If we are not careful about this dependence, we may obtain wrong conclusions. As an example, let $H = \text{def}_s(G)$. Since every element of $H$ is definable by the parameter $s$, so one may concludes that $H$ is logically cyclic. In the other words, one may convince that by 2.1, for any finite group $G$ and any $s \in G$ the group $C_G(C_{\text{Aut}(G)}(s))$ is cyclic. This is not true, since for example, if we let $G$ be a $p$-group of class 2 with an odd $p$, and if we assume that $\text{Aut}(G)$ is also $p$-group such that $\Omega_1(G)$ is not included.
in the center, then we can choose \( s \) to be a non-central element of order \( p \) and \( u \in C_{\text{Aut}(G)}(G) \cap Z(G) \) with order \( p \). Now, it is easy to see that \( \langle s, u \rangle \subseteq C_G(C_{\text{Aut}(G)}(s)) \), and so this subgroup is not cyclic. Note that for the case \( p = 2 \), the dihedral group of order 8 is also a counterexample. These counterexamples show that in general \( \text{def}_s(G) \) is not logically cyclic. To see the reason, note that if \( H \leq G \) and \( s \in H \), then there is no trivial relations between \( \text{def}_s(G) \) and \( \text{def}_s(H) \). If \( g \in \text{def}_s(H) \), and \( \varphi(x) \) is a formula defining \( g \) in \( H \), then we may have

\[
|\{ a \in G : G \models \varphi(a) \}| > 1,
\]
or even, we may have \( G \models \neg \varphi(a) \). This shows that in general \( \text{def}_s(H) \) is not contained in \( \text{def}_s(G) \). On the other hand, if \( g \in H \cap \text{def}_s(G) \), then we may have not \( g \in \text{def}_s(H) \) by a similar argument. Hence, the subgroup \( \text{def}_s(G) \) behaves not so simply despite its abelianness.

Two more problems remain unsolved; the first one is the classification of infinite logically cyclic groups. As we said before, the additive group of rationales is not finitely generated, however it is logically cyclic. There may be other infinitely generated groups having this property and a classification must be exists. The second problem concerns finite algebraic structures other than groups. An algebra \( A \) in an algebraic language \( \mathcal{L} \), is said to be cyclic if it is generated by a single element. It is called logically cyclic if every element of \( A \) can be defined by a first order formula containing a fixed parameter from \( A \). If \( A \) is finite, then clearly \( A \) is the only elementary extension of itself. So an element \( a \in A \) is definable using a parameter \( s \), if and only if every automorphism of \( A \) which fixes \( s \), fixes already \( a \). How can we obtain the relation between cyclic and logically cyclic algebras? This may need further efforts because in general we have a few information about \( \text{Aut}(A) \).

**Acknowledgement:** The author would like to thank Geoff Robinson, Khalid Bou Rabee and Emil Jeřábek for useful discussions.

**References**

[1] C. J. Hillar, D. L. Rhea, *Automorphisms of finite abelian groups*, American Math. Monthly, Vol. 114, No. 10, (2007).

[2] B. Poizat, *A Course in Model Theory: an introduction to contemporary mathematical logic*, Springer, (2000).