Ana-Loredana Agore; Dragoş Frățilă
Crossed product of cyclic groups

Czechoslovak Mathematical Journal, Vol. 60 (2010), No. 4, 889–901

Persistent URL: http://dml.cz/dmlcz/140791

Czechoslovak Mathematical Journal, 60 (135) (2010), 889–901

CROSSED PRODUCT OF CYCLIC GROUPS

Ana-Loredana Agore, Dragoş Frăţilă, Bucharest

(Received April 1, 2009)

Abstract. All crossed products of two cyclic groups are explicitly described using generators and relations. A necessary and sufficient condition for an extension of a group by a group to be a cyclic group is given.

Keywords: cyclic groups, crossed product of groups, Chinese Remainder Theorem

MSC 2010: 20B05, 20B35, 20D06, 20D40

Introduction

One of the most frequently used results in elementary number theory is the famous ancient Chinese Remainder Theorem. The Chinese Remainder Theorem can be restated in an abstract and elegant language of group theory as follows: the direct product $H \times G$ of two groups is a cyclic group iff the groups are finite, cyclic of coprime orders. The direct product $H \times G$ is the trivial example of an extension of a group H by a group G, that is, there exists an exact sequence of groups:

$$1 \longrightarrow H \xrightarrow{i_H} H \times G \xrightarrow{\pi_G} G \longrightarrow 1$$

It is therefore natural and tempting to consider the most general problem:

Problem 1. Let (E, i, π) be an extension of H by G: i.e. E is a group, $i\colon\ H \to E$ and $\pi\colon\ E \to G$ are morphisms of groups such that the sequence

$$1 \longrightarrow H \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

is exact. Give a necessary and sufficient condition for the group E to be cyclic.

The authors were supported by CNCSIS grant 24/28.09.07 of PN II "Groups, quantum groups, corings and representation theory".

The main theorem of the paper (Theorem 3.8) gives a complete answer to the above question. From this point of view Theorem 3.8 can be considered as an interesting and non-trivial generalization of the Chinese Remainder Theorem.

To obtain this result we will go through the following steps: we will do a survey of the famous "extension problem" of Hölder [6], then we will work in an equivalent way with the crossed systems instead of exact sequences and in the end we will explicitly compute all the symmetric, normalized 2-cocycles for two fixed cyclic groups and the (crossed) twisted products associated.

The extension problem was first stated by Hölder [6]. A recent survey and new results related to the extension problem are obtained in [3]. In particular, crossed products arise naturally when dealing with group extensions. [3, Corollary 1.8] is another formulation of Schreier theorem and shows that the existence of an extension of H by G is equivalent to the existence of a normalized crossed system (H, G, α, f), where $\alpha\colon\ G \to \mathrm{Aut}(H)$ is a weak action and $f\colon\ G \times G \to H$ is an α-cocycle. The classical extension problem of Hölder was restated in [3, Problem 1] in a computational manner as follows:

Problem 2. Let H and G be two fixed groups. Describe all normalized crossed systems (H, G, α, f) and classify up to isomorphism all crossed products $H\#_\alpha^f G$.

The first notable result regarding the extension problem was given by O. L. Hölder (Theorem 2.1), who uses generators and relations to describe all crossed products of two finite cyclic groups. In Section 2 of the paper we complete the structure and we shall describe all crossed products of two cyclic groups (not necessarily finite) using generators and relations: see Theorem 2.2, Theorem 2.3, and Theorem 2.4. Related to Problem 2 another question arises:

Problem 3. Let Λ be a class of groups. Find necessary and sufficient conditions for (H, G, α, f) such that the crossed product $H\#_\alpha^f G$ belongs to Λ.

In [3, Corollary 1.15] a complete answer is given to the above problem in the case of abelian groups: the crossed product $H\#_\alpha^f G$ is an abelian group if and only if H and G are abelian groups, α is the trivial action and f is a symmetric 2-cocycle.

The present paper deals with this problem in the case of cyclic groups. In the first section we recall the construction and fundamental properties of crossed product of groups. In Section 2 we describe crossed products between all types of cyclic groups. Using the aforementioned results, in Section 3 we find necessary and sufficient conditions for a crossed product to be a cyclic group (Theorem 3.8) which is the main result of this paper.

1. Preliminaries

Let us fix the notation that will be used throughout the paper. C_n will be a cyclic group of order n generated by a: $C_n = \{1, a, a^2, \dots, a^{n-1}\}$ and $C_g = \{g^k \colon k \in \mathbb{Z}\}$ will denote a cyclic infinite group. Let H and G be two groups. $\mathrm{Aut}(H)$ denotes the group of automorphisms of a group H and $Z(H)$ the center of H. A map $f \colon G \times G \to H$ is called *symmetric* if $f(g_1, g_2) = f(g_2, g_1)$ for any $g_1, g_2 \in G$. For a map $\alpha \colon G \to \mathrm{Aut}(H)$ we shall use the notation

$$\alpha(g)(h) = g \triangleright h$$

for all $g \in G$ and $h \in H$.

The maps α and f are called *trivial* if $g \triangleright h = h$ for all $g \in G$ and $h \in H$, respectively $f(g_1, g_2) = 1$ for all $g_1, g_2 \in G$.

Definition 1.1. A *crossed system* of groups is a quadruple (H, G, α, f), where H and G are two groups, $\alpha \colon G \to \mathrm{Aut}(H)$ and $f \colon G \times G \to H$ are two maps such that the following compatibility conditions hold:

$$g_1 \triangleright (g_2 \triangleright h) = f(g_1, g_2)((g_1 g_2) \triangleright h) f(g_1, g_2)^{-1}, \tag{1}$$

$$f(g_1, g_2) f(g_1 g_2, g_3) = (g_1 \triangleright f(g_2, g_3)) f(g_1, g_2 g_3) \tag{2}$$

for all $g_1, g_2, g_3 \in G$. The crossed system $\Gamma = (H, G, \alpha, f)$ is called *normalized* if $f(1, 1) = 1$. The map $\alpha \colon G \to \mathrm{Aut}(H)$ is called a *weak action* and $f \colon G \times G \to H$ is called an *α-cocycle*.

If (H, G, α, f) is a normalized crossed system then [3, Lemma 1.2]

$$f(1, g) = f(g, 1) = 1 \quad \text{and} \quad 1 \triangleright h = h \tag{3}$$

for any $g \in G$ and $h \in H$.

Let H and G be groups, $\alpha \colon G \to \mathrm{Aut}(H)$ and $f \colon G \times G \to H$ two maps. Let $H \#_\alpha^f G := H \times G$ as a set with a binary operation defined by the formula:

$$(h_1, g_1) \cdot (h_2, g_2) := \big(h_1 (g_1 \triangleright h_2) f(g_1, g_2), g_1 g_2\big) \tag{4}$$

for all $h_1, h_2 \in H$, $g_1, g_2 \in G$. Then [3, Theorem 1.3] $(H \#_\alpha^f G, \cdot)$ is a group with the unit $1_{H \#_\alpha^f G} = (1, 1)$ if and only if (H, G, α, f) is a normalized crossed system. In this case the group $H \#_\alpha^f G$ is called the *crossed product of H and G* associated to the crossed system (H, G, α, f).

The following [3, Examples 1.5] are basic examples of special cases of a crossed product of two groups.

Examples 1.2.

1. Let H and G be two groups and α, f be the trivial maps. Then $\Gamma = (H, G, \alpha, f)$ is a crossed system called the *trivial crossed system*. The crossed product $H\#_\alpha^f G = H \times G$ is the direct product of H and G.
2. Let H and G be two groups and $f\colon G \times G \to H$ the trivial map. Then (H, G, α, f) is a crossed system if and only if $\alpha\colon G \to \mathrm{Aut}(H)$ is a morphism of groups. In this case the crossed product is $H\#_\alpha^f G = H \ltimes_\alpha G$, the semidirect product of H and G.
3. Let H and G be two groups and $\alpha\colon G \to \mathrm{Aut}(H)$ the trivial action. Then (H, G, α, f) is a crossed system if and only if $\mathrm{Im}(f) \subseteq Z(H)$ and

$$f(g_1, g_2)f(g_1g_2, g_3) = f(g_2, g_3)f(g_1, g_2g_3) \tag{5}$$

for all $g_1, g_2, g_3 \in G$, that is $f\colon G \times G \to Z(H)$ is a 2-cocycle. The crossed product $H\#_\alpha^f G$ associated to this crossed system will be denoted by $H \times^f G$ and was called in [3] the *twisted product* of H and G associated to the 2-cocycle $f\colon G \times G \to Z(H)$. Explicitly, the multiplication of a twisted product of groups $H \times^f G$ is given by the formula:

$$(h_1, g_1) \cdot (h_2, g_2) := (h_1h_2f(g_1, g_2), g_1g_2) \tag{6}$$

for all $h_1, h_2 \in H$, $g_1, g_2 \in G$.

The next well-known theorem is the main application of the crossed product construction: it is a reconstruction theorem of a group from a normal subgroup and the quotient.

Theorem 1.3. *Let E be a group, $H \trianglelefteq E$ be a normal subgroup of E and $G := E/H$ be the quotient of E by H. Then there exist two maps $\alpha\colon G \to \mathrm{Aut}(H)$ and $f\colon G \times G \to H$ such that (H, G, α, f) is a normalized crossed system and $E \cong H\#_\alpha^f G$ (isomorphism of groups).*

For complete proofs and further details we refer to [2], [3, Theorem 1.6] or [8].

2. Crossed product of cyclic groups

Our purpose in this section is to describe using generators and relations all crossed products between cyclic groups. As mentioned in the introduction, the first important result in the literature for the first part of the extension problem was proved by Hölder himself [5, Theorem 12.9]. It describes the crossed product of two finite cyclic groups: for the sake of completeness we present bellow a short proof of this theorem.

Theorem 2.1 (Hölder)**.** *A finite group E is isomorphic to a crossed product $C_n\#_\alpha^f C_m$ if and only if E is the group generated by two generators a and b subject to the relations*

$$a^n = 1, \quad b^m = a^i, \quad b^{-1}ab = a^j \tag{7}$$

where $i, j \in \{0, 1, \dots, n-1\}$ are such that

$$i(j-1) \equiv 0 \pmod{n}, \quad j^m \equiv 1 \pmod{n}. \tag{8}$$

We denote this group by $C_n\#_i^j C_m$.

P r o o f. Assume first that E is isomorphic to a crossed product $C_n\#_\alpha^f C_m$. Hence $C_n \trianglelefteq E$ and $E/C_n \simeq C_m$. It follows that $C_n = \langle a \mid a^n = 1\rangle \trianglelefteq E$ and there exists $b \in E$ such that $E/C_n = \{C_n, bC_n, \dots, b^{m-1}C_n\}$ and $b^m \in C_n$. That is, there exists $i \in \{0, 1, \dots, n-1\}$ such that

$$b^m = a^i. \tag{9}$$

Since $C_n \trianglelefteq E$ we obtain that $b^{-1}ab \in C_n$ and so there exists $j \in \{0, 1, \dots, n-1\}$ such that

$$b^{-1}ab = a^j. \tag{10}$$

A direct computation shows that

$$b^{-1}a^ib \overset{(9)}{=} b^{-1}b^mb = b^m \overset{(9)}{=} a^i \quad \text{and} \quad b^{-1}a^ib \overset{(10)}{=} a^{ij}.$$

It follows from here that $a^{i(j-1)} = 1$ and so $i(j-1) \equiv 0 \pmod{n}$. In a similar way we obtain

$$b^{-m}ab^m \overset{(10)}{=} a^{-i}aa^i = a \quad \text{and} \quad a^{j^2} \overset{(10)}{=} (b^{-1}ab)^j = b^{-1}a^jb \overset{(10)}{=} b^2ab^2,$$

and by induction $b^{-m}ab^m = a^{j^m}$. Hence $a = a^{j^m}$, that is $j^m \equiv 1 \pmod{n}$.

Conversely, assume that the relations (7) and (8) hold. We need to show that $C_n \trianglelefteq E$, that is $xa^tx^{-1} \in C_n$ for every $x \in E$ and $t \in \{0, 1, \dots, n-1\}$. Since $x \in E$ we have $x = x_1x_2 \dots x_k$ where $k \in \mathbb{N}$, $x_s \in \{a, b, a^{-1}, b^{-1}\}$ and $s \in \{0, 1, \dots, k\}$. We obtain that $ga^tg^{-1} = x_1x_2 \dots x_ka^t(x_k)^{-1} \dots (x_1)^{-1}$. It is easy to see by a direct computation that $x_ka^t(x_k)^{-1} \in C_n$ for every $x_k \in \{a, b, a^{-1}, b^{-1}\}$ and so, by induction it follows that $ga^tg^{-1} \in C_n$. Hence $C_n \trianglelefteq E$. In a similar way, it can be showed that every element of the group E can be written as a^pb^q for $p, q \in \mathbb{Z}$. Hence $|E| = mn$ and so $|E/C_n| = m$, $E/C_n = \{C_n, C_nb, \dots, C_nb^{m-1}\}$, that is, the group E has a normal subgroup C_n and $E/C_n \simeq C_m$. By Theorem 1.3, there exists (C_n, C_m, α, f) a crossed system such that $E \simeq C_n\#_\alpha^f C_m$. □

Theorem 2.2. *A group E is isomorphic to a crossed product $C_n\#_\alpha^f C_g$ if and only if there exists $t \in \mathbb{Z}$, $(t,n)=1$ such that $E \simeq \langle a, g \mid a^n = 1,\ g^{-1}ag = a^t\rangle$.*

P r o o f. Suppose first that $E \simeq C_n\#_\alpha^f C_g$. Hence $C_n \trianglelefteq E$ and $E/C_n \simeq C_g$. That is $E/C_n = \{g^k C_n\colon\ k \in \mathbb{Z}\}$. Since $C_n \trianglelefteq E$ we obtain that $C_n = \langle a \mid a^n = 1\rangle \subseteq E$ and $g^{-1}ag \in C_n$. That is, there exists $t \in \{0, 1, \ldots, n-1\}$ such that

$$g^{-1}ag = a^t \tag{11}$$

Suppose now that $(t,n) = d > 1$. It follows from here that there exist $t_1, n_1 \in \mathbb{N}$ such that $t = dt_1$, $n = dn_1$ and $(t_1, n_1) = 1$. From (11) we obtain $g^{-1}a^{n_1}g = a^{nt_1} = 1$, that is $a^{n_1} = 1$, which is a contradiction with a having order n and $n_1 < n$. Hence $(t,n) = 1$ and $E \simeq \langle a, g \mid a^n = 1, g^{-1}ag = a^t\rangle$.

Now let $E \simeq \langle a, g \mid a^n = 1,\ g^{-1}ag = a^t\rangle$ for some $t \in \mathbb{Z}$, $(t,n) = 1$. By Theorem 1.3 we only need to prove that $C_n \trianglelefteq E$ and $E/C_n \simeq C_g$. For any $g' \in E$ we have $g' = x_1x_2\ldots x_k$, for some $k \in \mathbb{N}$, $x_i \in \{a, g, a^{-1}, g^{-1}\}$, $i \in \{1, 2, \ldots, k\}$. That is, to prove that $C_n \trianglelefteq E$ we only need to show that $g^{-1}a^l g \in C_n$ and $ga^l g^{-1} \in C_n$ for any $l \in \mathbb{Z}$. From (11) we obtain, by induction, that $g^{-1}a^l g = a^{tl} \in C_n$. Since $(t,n) = 1$ there exist $\alpha, \beta \in \mathbb{Z}$ such that $\alpha t + \beta n = 1$. We obtain from (11) that $a = ga^t g^{-1}$ and it follows from here that $a^\alpha = ga^{\alpha t}g^{-1}$. Since $ga^{\beta n}g^{-1} = 1$ we obtain that $ga^{\alpha t+\beta n}g^{-1} = a^\alpha$, that is $gag^{-1} = a^\alpha$. It follows from here that $ga^l g^{-1} = a^{\alpha l}$ for any $l \in \mathbb{Z}$. Hence $C_n \trianglelefteq E$. It follows by a simple calculation that every element $g' \in E$ can be written as $g^p a^q$ for some $p, q \in \mathbb{Z}$. That is $gC_n = g^p a^q C_n =^p C_n$. Hence $E/C_n \subseteq C_g$. Now suppose that there exist $\alpha, \beta \in \mathbb{Z}$, $\alpha \neq \beta$ such that $g^\alpha C_n = g^\beta C_n$, that is $g^{\alpha-\beta} = a^\gamma$ for some $\gamma \in \{0, 1, \ldots, n-1\}$. It follows from here that $g^{(\alpha-\beta)n} = a^{\gamma n} = 1$ which is a contradiction with C_g being an infinite cyclic group. Hence $E/C_n \simeq C_g$. □

Theorem 2.3. *A group E is isomorphic to a crossed product $C_g\#_\alpha^f C_n$ if and only if:*

(i) $E \simeq \langle g, h \mid gh = hg,\ h^n = g^t,\ \in \mathbb{Z}\rangle$ *for n odd;*

(ii) $E \simeq \langle g, h \mid gh = hg,\ h^n = g^t,\ t \in \mathbb{Z}\rangle$ *or* $E \simeq \langle g, h \mid h^n = 1,\ ghg = h\rangle$ *for n even.*

P r o o f. Suppose first that $E \simeq C_g\#_\alpha^f C_n$. Hence $C_g \trianglelefteq E$ and $E/C_g \simeq C_n$. That is, there exists $h \in E$ such that $E/C_g = \{C_g, hC_g, \ldots, h^{n-1}C_g\}$ and $h^n \in C_g$. Hence there exists $t \in \mathbb{Z}$ such that $h^n = g^t$. Since $C_g \trianglelefteq E$ we obtain $h^{-1}gh \in C_g$, that is $h^{-1}gh = g^s$ for some $s \in \mathbb{Z}$. It follows that $h^{-1}g^t h = g^{st}$ and using $h^n = g^t$ we obtain $g^{ts} = g^t$ that is $g^{t(s-1)} = 1$. Since C_g is an infinite cyclic group we must have $t(s-1) = 0$. Using again $h^{-1}gh = g^s$ we obtain $h^{-1}g^s h = g^{s^2}$, that is $h^{-2}gh^2 = g^{s^2}$

and by induction $h^{-n}gh^n = g^{s^n}$. Thus, from $h^n = g^t$ we obtain $g^{s^n-1} = 1$ and since C_g is an infinite cyclic group we must have $s^n = 1$. Therefore if n is odd $E \simeq \langle g, h \mid gh = hg,\ h^n = g^t\rangle$ for some $t \in \mathbb{Z}$ and if n is even $E \simeq \langle g, h \mid gh = hg,\ h^n = g^t\rangle$ for some $t \in \mathbb{Z}$ or $E \simeq \langle g, h \mid h^n = 1,\ ghg = h\rangle$.

We assume now that $E \simeq \langle g, h \mid gh = hg,\ h^n = g^t,\ t \in \mathbb{Z}\rangle$. Since E is abelian $C_g \trianglelefteq E$. $E/C_g = \{g'C_g \mid g' \in E\}$ and since every element $g' \in E$ can be written as $g' = h^p g^q$ we obtain that $g'C_g = h^p g^q C_g = h^p C_g$, that is $E/C_g \subseteq \{C_g, hC_g, \ldots, h^{n-1}C_g\} \simeq C_n$. Now suppose that there exists $\alpha, \beta \in \{0, 1, \ldots, n-1\}$, $\alpha > \beta$, such that $h^\alpha C_g = h^\beta C_g$ that is $h^{\alpha-\beta} = g^\gamma$ for some $\gamma \in \mathbb{Z}$. Since $\alpha - \beta < n$ we obtain a contradiction with $h^n = g^t$. Hence $E/C_g \simeq C_n$ and by Theorem 1.3 there exists (C_g, C_n, α, f) a crossed system such that $E \simeq C_g \#_\alpha^f C_n$.

Suppose now that n is even and $E \simeq \langle g, h \mid h^n = 1,\ ghg = h\rangle$. By Theorem 1.3 we only need to prove that $C_g \trianglelefteq E$ and $E/C_g \simeq C_n$. For any $g' \in E$ we have $g' = x_1 x_2 \ldots x_k$ for some $k \in \mathbb{N}$, $x_i \in \{g, h, g^{-1}, h^{-1}\}$ and $i \in \{1, 2, \ldots, k\}$. That is, to prove that $C_g \trianglelefteq E$ we only need to show that $hg^l h^{-1} \in C_g$ and $h^{-1}g^l h \in C_g$ for any $l \in \mathbb{Z}$. Since $h^{-1}gh = g^{-1}$ we obtain, by induction, that $h^{-1}g^l h = g^{-l} \in C_g$. Also from $hg^l h^{-1} = h^{-n+1}g^l h^{n-1} = (h^{-1})^{n-1}g^l h^{n-1} = (h^{-1})^{n-2}g^{-l}h^{n-2}$ we obtain by induction $hg^l h^{-1} = g^{-l} \in C_g$. Hence $C_g \trianglelefteq E$. $E/C_g = \{g'C_g \mid g' \in E\}$ and since any element $g' \in E$ can be written as $h^p g^q$ for some $p, q \in \mathbb{Z}$ it follows from here that $g'C_g = h^p g^q C_g = h^p C_g$. Hence $E/C_g \subseteq C_n$. Now suppose that there exist $\alpha, \beta \in \{0, 1, \ldots, n-1\}$, $\alpha > \beta$ such that $h^\alpha C_g = h^\beta C_g$, that is $h^{\alpha-\beta} = g^\gamma$ for some $\gamma \in \mathbb{Z}$. It follows from here that $g^{n\gamma} = (h^n)^{\alpha-\beta} = 1$ and since C_g is an infinite cyclic group we must have $n\gamma = 0$, that is $\gamma = 0$. Hence $h^{\alpha-\beta} = 1$ which is a contradiction since the order of h is n and $0 < \alpha - \beta < n$. Therefore $E/C_g = C_n$. □

Theorem 2.4. *A group E is isomorphic to a crossed product $C_{g_1} \#_\alpha^f C_{g_2}$ if and only if $E \simeq \langle g_1, g_2 \mid g_1 g_2 = g_2 g_1\rangle$ or $E \simeq \langle g_1, g_2 \mid g_1 g_2 g_1 = g_2\rangle$.*

P r o o f. Suppose first that $E \simeq C_{g_1} \#_\alpha^f C_{g_2}$. Hence $C_{g_1} \trianglelefteq E$ and $E/C_{g_1} \simeq C_{g_2}$. That is $E/C_{g_1} = \{g_2^k C_{g_1} \mid k \in \mathbb{Z}\}$. Since $C_{g_1} \trianglelefteq E$ we obtain that $g_2^{-1}g_1 g_2 \in C_{g_1}$ and $g_2 g_1 g_2^{-1} \in C_{g_1}$. That is, there exist $s, t \in \mathbb{Z}$ such that

$$g_2^{-1}g_1 g_2 = g_1^t \tag{12}$$

and

$$g_2 g_1 g_2^{-1} = g_1^s. \tag{13}$$

From (12) we obtain, that $g_2^{-1}g_1^s g_2 = g_1^{st}$. It follows from here, using (13), that $g_1^{st} = g_1$. Since C_{g_1} is an infinite cyclic group, we obtain that $st = 1$, that is $(s, t) \in \{(1, 1), (-1, -1)\}$. Hence $E \simeq \langle g_1, g_2 \mid g_1 g_2 = g_2 g_1\rangle$ or $E \simeq \langle g_1, g_2 \mid g_1 g_2 g_1 = g_2\rangle$.

Conversely, if $E \simeq \langle g_1, g_2 \mid g_1 g_2 = g_2 g_1 \rangle$ then it is obvious that $E \simeq \mathbb{Z} \times \mathbb{Z} \simeq C_{g_1} \# C_{g_2}$ the crossed system being the trivial one.

Now let $E \simeq \langle g_1, g_2 \mid g_1 g_2 g_1 = g_2 \rangle$. Also by Theorem 1.3 we only need to prove that $C_{g_1} \trianglelefteq E$ and $E/C_{g_1} \simeq C_{g_2}$. For any $g \in E$ we have $g = x_1 x_2 \dots x_k$ for $k \in \mathbb{N}$, $x_i \in \{g_1, g_2, g_1^{-1}, g_2^{-1}\}$ and $i \in \{1, 2, \dots, k\}$. Therefore, to prove $C_{g_1} \trianglelefteq E$, we only need to show that $g_2 g_1^l g_2^{-1} \in C_{g_1}$ and $g_2^{-1} g_1^l g_2 \in C_{g_1}$ for any $l \in \mathbb{Z}$. From $g_1 g_2 g_1 = g_2$ we obtain $g_2 g_1 g_2^{-1} = g_1^{-1} = g_2^{-1} g_1 g_2$ and $g_2 g_1^l g_2^{-1} = g_1^{-l} = g_2^{-1} g_1^l g_2$ for any $l \in \mathbb{Z}$. Hence $C_{g_1} \trianglelefteq E$. In a similar way it can be shown that every element g of the group E can be written as $g_2^p g_1^q$ for some $p, q \in \mathbb{Z}$. It follows from here that $gC_{g_1} = g_2^p g_1^q C_{g_1} = g_2^p C_{g_1}$. Hence $E/C_{g_1} \leqslant C_{g_2}$. Since any non trivial subgroup of an infinite cyclic group is infinite cyclic we obtain that $E/C_{g_1} \simeq C_{g_2}$ which finishes the proof. □

3. When is a crossed product a cyclic group?

Our aim in the present section is to give a necessary and sufficient condition for a crossed product to be a cyclic group. For this it is necessary that both groups should be cyclic since any subgroup and any quotient of a cyclic group are cyclic groups. Hence the problem is reduced to deciding which of the crossed products between two cyclic groups described in the previous section are cyclic groups and under what conditions.

It is obvious that the crossed product between a finite cyclic group C_n and an infinite cyclic group C_g described in Theorem 2.2 cannot be a cyclic group since an infinite cyclic group does not have torsion elements. By the same argument we can conclude that the crossed product $\langle g, h \mid h^n = 1,\ ghg = h \rangle$ obtained in Theorem 2.3 cannot be a cyclic group. Also, the crossed product between the two infinite cyclic groups described in Theorem 2.4 cannot be a cyclic group because a nontrivial quotient of an infinite cyclic group must be finite.

Therefore, the only crossed products left to deal with are: $C_n \#_i^j C_m$ described in Theorem 2.1 and $\langle g, h \mid gh = hg,\ h^n = g^t,\ t \in \mathbb{Z} \rangle$ from Theorem 2.3.

In what follows we investigate under what conditions these two crossed products are cyclic groups.

In order to prove our next result we need the following technical lemma:

Lemma 3.1. *Let m, n, i be rational integers such that $(m, n, i) = 1$. Then there exist some $u, v, w \in \mathbb{Z}$ such that $um + vi + wn = 1$ and $(m, v) = 1$, where (r, s) denotes the greatest common divisor of the integers r and s.*

P r o o f. Let $d = (m, n)$. Then $(d, i) = 1$. Let $m' \mid m$ be such that $(m', d) = 1$ and $m'd$ contains all the prime factors of m. Using the Chinese Remainder Theorem we can find $v \in \mathbb{Z}$ such that $d \mid vi - 1$ and $m' \mid v - 1$ (if $m' = 1$ the last condition is trivially fulfilled). We observe that $(m, v) = 1$ because all the prime divisors of m are in $m'd$ and $(m'd, v) = 1$.

Since $d = (m, n)$ there exist $u', w' \in \mathbb{Z}$ such that $u'm + w'n = d$. From the way we chose v it follows that there exists $r \in \mathbb{Z}$ such that $vi + rd = 1$. Now put $u = ru'$, $w = rw'$. From the above we have $vi + r(u'm + w'n) = 1$, thus $vi + um + wn = 1$. □

Proposition 3.2. *A crossed product $E = C_n \#_i^j C_m$ is a cyclic group if and only if $j = 1$ and $(m, n, i) = 1$.*

P r o o f. We know from Theorem 2.1 that E has a presentation of the form

$$E = \langle a, b \mid a^n = 1,\ b^m = a^i,\ b^{-1}ab = a^j \rangle.$$

Suppose first that E is a cyclic group. It follows from here that $j = 1$ since every cyclic group is abelian. If E is cyclic then there exist some $u, v \in \mathbb{Z}$ such that $E = \langle a^u b^v \rangle$. $a^u b^v$ has order mn, hence $(a^u b^v)^m$ has order n. It is well known that in a cyclic group for any divisor of the order of the group there exists a unique subgroup of that order, thus $\langle (a^u b^v)^m \rangle = \langle a \rangle$ and therefore there exists some $k \in \mathbb{Z}$ such that $(a^{uk} b^{vk})^m = a$. Using the relation $b^m = a^i$ and the fact that a has order n we obtain that $ukm + vki - 1$ is divisible by n, that is $(m, n, i) = 1$.

For the converse we will use the previous lemma and we obtain that there exist $u, v, w \in \mathbb{Z}$ such that $um + iv + wn = 1$ and $(m, v) = 1$. We will prove that $a^u b^v$ has order mn in E and that finishes the proof. For this it is enough to prove that $a, b \in \langle a^u b^v \rangle$. By a simple calculation we get: $(a^u b^v)^m = a^{um} a^{vi} = a^{um+vi} = a^{1-wn} = a$, that is $a \in \langle a^u b^v \rangle$. Since $(m, v) = 1$, there exists $l \in \mathbb{Z}$ such that $m \mid vl - w$. Now let $k = i + ln$.

Finally $(a^u b^v)^k = (a^u b^v)^i (a^u b^v)^{ln} = b^{um} b^{vi} b^{vln} = b^{um+vi+vln} = b^{1-wn+vln} = bb^{n(vl-w)} = b$ because $n(vl - w)$ is divisible by mn and $|E| = mn$. Hence $b \in \langle a^u b^v \rangle$. □

Proposition 3.3. *The group $E = \langle g, h \mid h^n = g^t,\ hg = gh \rangle$, where $n \geqslant 2$, $t \in \mathbb{Z}$ is cyclic if and only if $(n, t) = 1$.*

P r o o f. Denote by $d = (n, t)$ and by $Z_{n,t} = \mathbb{Z} + (t/n)\mathbb{Z}$ which is an abelian group and is isomorphic to $(n, t)\mathbb{Z} \simeq \mathbb{Z}$ by the morphism $u \mapsto nu$.

Define $\theta\colon E \to Z_{n,t}$ by $h \mapsto t/n$ and $g \mapsto 1$. It is easy to see that this is a morphism of groups and moreover it is surjective. In order to have E isomorphic

to $\mathbb{Z}$ (i.e. E cyclic infinite), θ must be an isomorphism, otherwise we get a surjective endomorphism of $\mathbb{Z}$ which is not injective and this is impossible.

So $E \simeq \mathbb{Z}$ iff θ is injective and this happens iff $(n,t)=1$. Indeed $h^r g^{-s} \mapsto rt/n - s = 0 \Leftrightarrow rt = ns \Leftrightarrow r = kn/d$, $s = kt/d$, $k \in \mathbb{Z}$ so $\ker(\theta) = \{(h^{n/d} g^{-t/d})^k \colon k \in \mathbb{Z}\}$ and then $\ker(\theta) = 0$ iff $h^{n/d} = g^{t/d}$, i.e. $d = 1$. □

Our next goal is to describe, in the language of crossed systems, all cyclic crossed products. That is, to identify the properties that (H, G, α, f) has to verify in order to obtain a cyclic crossed product $H\#_\alpha^f G$. As we already noticed, both H and G must be cyclic groups. Since $H\#_\alpha^f G$ is, in particular, an abelian group it follows from [3, Corollary 1.15] that α must be trivial and f a symmetric 2-cocycle. In order to find necessary and sufficient conditions on f such that $H\#^f G$ is cyclic we describe bellow all the possible symmetric 2-cocycles.

For $m \geqslant 2$ and $n \geqslant 2$ or $n = \infty$ define $\Sigma_{m,n} = \{\varphi \colon \mathbb{Z} \to \mathbb{Z}_n \colon \varphi(0) = 0, \varphi(t+m) = \varphi(t), \forall\, t \in \mathbb{Z}\}$ with the convention that $\mathbb{Z}_\infty = \mathbb{Z}$.

Proposition 3.4. *The symmetric normalized 2-cocycles $f \colon C_m \times C_m \to C_n$ are in bijection with the set $\Sigma_{m,n}$.*

P r o o f. Let $\varphi \in \Sigma_{m,n}$ and consider x a generator of C_m and a a generator of C_n.

Denote $S_k^\varphi = S_k = \varphi(0) + \ldots + \varphi(k-1)$, $\forall\, k \geqslant 1$.

We define $f(x^k, x^l) = a^{S_{k+l} - S_k - S_l}$ for $k, l \geqslant 1$ (observe that if $n \neq \infty$ then a^t is well defined for $t \in \mathbb{Z}_n$ since a has order n).

It is easy to verify that $f(x^{k+sm}, x^l) = f(x^k, x^{l+tm}) = f(x^k, x^l)$, $(\forall)\, s, t \geqslant 0$, $(\forall)\, l, k \geqslant 1$. Observe also that $f(x, x^k) = a^{\varphi(k)}$. This will be useful for the converse.

f is obviously symmetric.

We need to prove that f is a 2-cocycle, that is:

$$\begin{aligned} f(x^k, x^l) f(x^{k+l}, x^p) &= f(x^l, x^p) f(x^k, x^{l+p}), \\ a^{S_{k+l} - S_k - S_l + S_{k+l+p} - S_p - S_{k+l}} &= a^{S_{p+l} - S_p - S_l + S_{k+l+p} - S_k - S_{l+p}}, \\ a^{S_{k+l+p} - S_k - S_l - S_p} &= a^{S_{k+l+p} - S_k - S_l - S_p}, \ (\forall)\, k, l, p \geqslant 1, \end{aligned}$$

and the latter is clearly true.

So to each $\varphi \in \Sigma_{m,n}$ we have associated a symmetric 2-cocycle.

Now suppose f is a symmetric 2-cocycle. Define $\varphi_f = \varphi$ such that $a^{\varphi(k)} = f(x, x^k)$, $k \in \mathbb{Z}$. It is obvious that $\varphi \in \Sigma_{m,n}$ because x has order m and f is normalized.

Define $S_k^\varphi = S_k = \varphi_f(0) + \ldots + \varphi_f(k-1)$.

Using the cocycle condition on f and straightforward computation it follows that $f(x^l, x^k) = a^{S_{k+l} - S_k - S_l}$, $(\forall)\, k, l \geqslant 1$.

Hence, the map that associates to each cocycle the function φ_f is a bijective map between the cocycles and $\Sigma_{m,n}$. □

Proposition 3.5. *A crossed product $C_n\#^f C_m, m, n \geqslant 2$ is a cyclic group if and only if $(S_m, m, n) = 1$, where $S_k = \varphi(0)+\ldots+\varphi(k-1)$, $\varphi\colon \mathbb{Z} \to \mathbb{Z}_n$, $a^{\varphi(k)} = f(x, x^k)$ and x is a generator for C_m.*

Remark 3.6. Observe that S_m is not a number, but a class (modulo n); however (S_m, m, n) does not depend on the choice of a representative for S_m.

P r o o f. We will prove that $C_n\#^f C_m$ is isomorphic to $C_n\#_i^1 C_m$ where $i \in \{0, 1, \ldots, n-1\}$ such that $S_m = i \pmod n$. The conclusion will follow from Proposition 3.2.

Let i be the unique representative of S_m from $\{0, 1, \ldots, n-1\}$.

Denote by $E = \langle a, b \mid a^n = 1, b^m = a^i, ab = ba\rangle$ and by $F = C_n\#^f C_m$ the twisted product associated to the 2-cocycle f (see Examples 1.2).

Define $\theta\colon E \to F$ by $\theta(a) = (a, 1)$ and $\theta(b) = (1, x)$.

It is straightforward to see that $(1, x)^k = (a^{S_k}, x^k)$, $\forall k \geqslant 1$ hence $(1, x)^m = (a^{S_m}, x^m) = (a^i, 1) = (a, 1)^i$ and $(1, x)^k \notin \langle a\rangle$, $\forall k \in \{1, \ldots, m-1\}$. Also $(a, 1)^n = 1$ and $(a, 1)(1, x) = (a, x) = (1, x)(a, 1)$. That is $(a, 1)$ and $(1, x)$ verify the same relations in F as a and b do in E. Hence θ is a morphism of groups.

Let us observe that $(a, 1)$ and $(1, x)$ generate the group F. Indeed consider $(a^u, x^k) \in F$. Then

$$(a^u, x^k) = (a^u, 1)(1, x^k) = (a^{u-S_k}, 1)(a^{S_k}, x^k) = (a, 1)^{u-S_k}(1, x)^k.$$

Therefore the morphism θ is also surjective and since the groups are finite it is an isomorphism. □

Proposition 3.7. *A crossed product $C_g\#^f C_m$, $m \geqslant 2$, is cyclic iff $(S_m, m) = 1$, where $S_m = \varphi(0) + \ldots + \varphi(m-1)$, $\varphi\colon \mathbb{Z} \to \mathbb{Z}$, $g^{\varphi(k)} = f(x, x^k)$, $\langle x\rangle = \mathbb{Z}_m$.*

P r o o f. We will prove that $C_g\#^f C_m$ is isomorphic to $E = t\langle g, h \mid h^m = g^{S_m}, gh = hg\rangle$ hence the conclusion follows from Proposition 3.3.

Denote by $F = C_g\#^f C_m$ the twisted product associated to the 2-cocycle f (see Examples 1.2).

Define $\theta\colon E \to F$ by $\theta(g) = (g, 1)$ and $\theta(h) = (1, x)$. It is easy to see that $(g, 1)(1, x) = (g, x) = (1, x)(g, 1)$ and $(1, x)^k = (g^{S_k}, x^k)$. Hence $(1, x)^m = (g^{S_m}, 1) = (g, 1)^{S_m}$. Therefore θ is a morphism of groups. Moreover, since

$(g^k, x^l) = (g,1)^{k-S_l}(1,x)^l$ we obtain that θ is a surjection. Furthermore:

$$\begin{aligned}
\ker(\theta) &= \{g^k h^l \colon\ k,l \in \mathbb{Z},\ \theta(g^k h^l) = (1,1)\} \\
&= \{g^k h^l \colon\ k,l \in \mathbb{Z},\ (g,1)^k (1,x)^l = (1,1)\} \\
&= \{g^k h^l \colon\ k,l \in \mathbb{Z},\ (g^{k+S_l}, x^l) = (1,1)\} \\
&= \{g^k h^l \colon\ k,l \in \mathbb{Z},\ m \mid l,\ k = -S_l\} \\
&= \{g^k h^l \colon\ k,l \in \mathbb{Z},\ l = sm,\ k = -sS_m\} \\
&= \{(g^{-S_m} h^m)^s \colon\ s \in \mathbb{Z}\} = \{1\}.
\end{aligned}$$

Hence θ is a bijection. □

In conclusion, with the above notation, we have proved the following theorem:

Theorem 3.8. *A normalized crossed product $E = H\#_\alpha^f G$ is a cyclic group if and only if one of the following are true:*
(1) *$H \simeq C_n$, $G \simeq C_m$, for some $m, n \geqslant 2$, α is trivial and $(S_m, m, n) = 1$;*
(2) *$H \simeq C_g$, $G \simeq C_m$, for some $m \geqslant 2$, α is trivial and $(S_m, m) = 1$.*

Let us consider a numerical example. Define $\varphi \in \Sigma_{3,\infty}$ by $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(2) = 1$ and consider the corresponding symmetric 2-cocycle $f \colon \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}$ (cf. Proposition 3.4).

An easy computation leads us to

$$\begin{gathered}
f(\hat{0}, \hat{u}) = f(\hat{u}, \hat{0}) = f(\hat{2}, \hat{2}) = 0,\ \forall \hat{u} \in \mathbb{Z}_3, \\
f(\hat{1}, \hat{1}) = f(\hat{1}, \hat{2}) = f(\hat{2}, \hat{1}) = 1.
\end{gathered}$$

Since $S_3 = 2$ it follows from Theorem 3.8 that $\mathbb{Z} \times^f \mathbb{Z}_3 \simeq \mathbb{Z}$.

We can also find the generator of $\mathbb{Z} \times^f \mathbb{Z}_3$, namely $(0, \hat{2})$. Indeed:

$$(0,\hat{2})^2 = (0 + 0 + f(\hat{2},\hat{2}), \hat{2} + \hat{2}) = (0,\hat{1})$$

and

$$(0,\hat{2})^3 = (0 + 0 + f(\hat{1},\hat{2}), \hat{2} + \hat{1}) = (1,\hat{0}).$$

Acknowledgement. We wish to thank Professor Gigel Militaru, who suggested the problem studied here, for his great support and for the useful comments from which this manuscript has benefitted.

References

[1] *A. Adem, R. J. Milgram*: Cohomology of Finite Groups, 2nd Edition. Springer, Berlin, 2004.

[2] *A. L. Agore*: Constructions in group theory. Dissertation. University of Bucharest, Bucharest, 2008.

[3] *A. L. Agore, G. Militaru*: Crossed product of groups applications. Arabian J. Sci. Eng. *33* (2008), 1–17.

[4] *H. Bechtell*: The Theory of Groups. Addison-Wesley Publishing Company, Reading, 1971.

[5] *P. A. Grillet*: Abstract Algebra, 2nd Edition. Graduate Texts in Mathematics 242. Springer, New York, 2007.

[6] *O. Hölder*: Bildung zusammengesetzter Gruppen. Math. Ann. *46* (1895), 321–422.

[7] *J. Rotman*: An introduction to the theory of groups, 4th Edition. Graduate Texts in Mathematics 148. Springer, New York, 1995.

[8] *C. Weibel*: An Introduction to Homological Algebra. Cambridge Univ. Press, Cambridge, 1994.

Authors' addresses: A.-L. Agore, Faculty of Mathematics and Computer Science, University of Bucharest, Str. Academiei 14, RO-010014 Bucharest 1 and Dept. of Math., Academy of Economic Studies, Piata Romana 6, RO-010374 Bucharest 1, Romania, e-mail: ana.agore@fmi.unibuc.ro; D. Frăţilă, Faculty of Mathematics and Computer Science, University of Bucharest, Str. Academiei 14, RO-010014 Bucharest 1, Romania, dragos.fratila@gmail.com.