Aleš Drápal

On multiplication groups of relatively free quasigroups isotopic to Abelian groups

Czechoslovak Mathematical Journal, Vol. 55 (2005), No. 1, 61–86

Persistent URL: http://dml.cz/dmlcz/127959

Czechoslovak Mathematical Journal, 55 (130) (2005), 61–86

ON MULTIPLICATION GROUPS OF RELATIVELY FREE QUASIGROUPS ISOTOPIC TO ABELIAN GROUPS

Aleš Drápal, Praha

(Received March 14, 2002)

Abstract. If Q is a quasigroup that is free in the class of all quasigroups which are isotopic to an Abelian group, then its multiplication group $\operatorname{Mlt} Q$ is a Frobenius group. Conversely, if $\operatorname{Mlt} Q$ is a Frobenius group, Q a quasigroup, then Q has to be isotopic to an Abelian group. If Q is, in addition, finite, then it must be a central quasigroup (a T-quasigroup).

Keywords: central quasigroups, T-quasigroups, multiplication groups, Frobenius groups, quasigroups isotopic to Abelian groups

MSC 2000: 20N05, 08B20

A quasigroup $Q = Q(\cdot)$ is usually defined as a binary system in which the equations

$$a \cdot x = b, \quad y \cdot a = b$$

have unique solutions for all $a, b \in Q$. One then sets $x = a \setminus b$ and $y = b/a$.

When one wishes to describe quasigroups by identities, one regards $Q = Q(\cdot, /, \setminus)$ as a set with three binary operations that are interconnected by relations

$$x \cdot (x \setminus y) = y = x \setminus (x \cdot y) \quad \text{and} \quad (x \cdot y)/y = x = (x/y) \cdot y.$$

This is the approach we shall take in this paper.

Its main result concerns quasigroups that are free in the class of all quasigroups isotopic to Abelian groups. We shall show that their multiplication groups are Frobenius groups (i.e., permutation groups that are transitive, but not regular, and where every nonidentity permutation fixes at most one point), and that the stabilizers of

This work was supported by institutional grant MSM 113200007, and by Grant Agency of Czech Republic, grant number 201/99/0263.

these groups (the so called inner mapping groups) are free. This contrasts with another result of ours, which states that a finite quasigroup with Frobenius multiplication group has to be central (i.e., a T-quasigroup).

The multiplication group $\operatorname{Mlt} Q$ is the permutation group on Q that is generated by all left translations L_a, $a \in Q$, and by all right translations R_a, $a \in Q$. We have $L_a(b) = a \cdot b = R_b(a)$, for all $a, b \in Q$.

We shall often fix some $e \in Q$ and consider the group $(\operatorname{Mlt} Q)_e$ of all $\varphi \in \operatorname{Mlt} Q$ that do not move e. If e is the unit of Q, then Q is called a *loop*, and $(\operatorname{Mlt} Q)_e$ is known as the *inner mapping group*. We shall call it the *inner mapping group at* e in the case of a general quasigroup.

Observe that a quasigroup Q is a loop with a unit e if and only if L_a is a regular permutation for each $a \in Q$, $a \neq e$ (a permutation is regular if it fixes no element).

Two quasigroups $Q_1(\cdot)$ and $Q_2(*)$ are said to be *isotopic* if and only if there exist bijections $f, g, h\colon\ Q_1 \to Q_2$ such that $f(x) * g(y) = h(x \cdot y)$ for all $x, y \in Q_1$. One of the earliest results in the quasigroup theory [1] states that a loop isotopic to a group has to be itself a group. A quasigroup Q_1 that is isotopic to a group and possesses no neutral element cannot be a group, of course. However, it is always a *principal isotope* of some group, which means that $Q_2(*)$ can be chosen to be a group, with $h\colon\ Q_1 \to Q_2$ an identity.

Here we shall be concerned with quasigroups Q that are isotopic to Abelian groups. For each such quasigroup there exists an Abelian group $Q(+)$ and bijections $\alpha, \beta\colon$ $Q \to Q$ such that the operations of the quasigroup $Q = Q(\circ, /, \backslash)$ are given by

$$x \circ y = \alpha(x) + \beta(y), \quad x/y = \alpha^{-1}(x - \beta(y)) \quad \text{and} \quad x \backslash y = \beta^{-1}(y - \alpha(x)).$$

It is not difficult to see that quasigroups isotopic to Abelian groups form a variety [13] in the sense of universal algebra. (For basic notions concerning universal algebra see [12] and [15]. For more information on loops and quasigroups see [6] and [3].)

The main results in this paper seem to be new. Some statements of Section 2 which also seem to be new can be rightly regarded as variations on earlier results. They are included with proofs to provide a selfcontained exposition of Propositions 2.8 and 2.9, and to show the usefulness of mapings $R_{b\backslash x}^{-1} L_a L_b^{-1} R_{a\backslash x}$ and $L_{x/b}^{-1} R_a R_b^{-1} L_{x/a}$. Further applications of these mappings can be found in [8], [9], [10], [11]. One can argue that these mappings induce natural proofs of some facts that were originally obtained by a formal manipulation which did not offer an interpretation beyond itself.

Section 3 describes free algebras in the variety of quasigroups isotopic to Abelian groups. The description is essentially the same as in [13], and hence the relevant proofs are presented only briefly. The main purpose of Section 3 is to develop formalism used in subsequent sections.

1. Quasigroups isotopic to Abelian groups

We start by a well known description of generators of G_ω, where G is a permutation group on Ω, $\omega \in \Omega$ (Lemma 1.1). From that one easily obtains a standard description for generators of the inner mapping group at e, $e \in Q$, Q a quasigroup (Proposition 1.2). Lemma 1.4 gives a modified system of such generators, from which there follows (via Lemmas 1.5, 1.6 and 1.7) an identity that characterizes the variety of all quasigroups isotopic to Abelian groups (Proposition 1.8). Let Q be such a quasigroup. From Proposition 1.8 one sees that then some of the generators from Lemma 1.4 turn into the identity mapping, and Proposition 1.9 describes a reduced set of generators for the inner mapping group at e.

The first identity characterizing quasigroups isotopic to Abelian groups probably belongs to Belousov [2]. His identity $x \setminus (y(u \setminus v)) = u \setminus (y(x \setminus v))$ differs from the identity we derive below.

Lemma 1.1. *Suppose that G is generated by $X \subseteq G$, and let $\Gamma \subseteq \Omega$ be the orbit of G that contains ω. Suppose that $g_\gamma \in G$ maps ω to γ, for every $\gamma \in \Gamma$. Then $\{g_{x(\gamma)}^{-1} x g_\gamma;\ x \in X$ and $\gamma \in \Gamma\}$ generates G_ω.*

Using this lemma one can easily verify that mappings $L_x^{-1}R_x$, $L_{xy}^{-1}L_xL_y$ and $R_{yx}^{-1}R_xR_y$ generate the inner mapping group of a loop. More generally, we get:

Proposition 1.2. *Let Q be a quasigroup and $e \in Q$. Then*

$$(\operatorname{Mlt} Q)_e = \big\langle R_{e\setminus y}^{-1} R_{x\setminus y} R_{e\setminus x},\ L_{y/e}^{-1} L_{y/x} L_{x/e},\ L_{x/e}^{-1} R_{e\setminus x};\ x, y \in Q \big\rangle.$$

P r o o f. Let us use Lemma 1.1 with $X = \{L_x, R_x;\ x \in Q\}$ and with $R_{e\setminus y}$ corresponding to g_y. We obtain

$$(\operatorname{Mlt} Q)_e = \big\langle R_{e\setminus(xy)}^{-1} L_x R_{e\setminus y},\ R_{e\setminus(yx)}^{-1} R_x R_{e\setminus y};\ x, y \in Q \big\rangle.$$

Now, $R_{e\setminus(xy)}^{-1} L_x R_{e\setminus y}$ can be replaced by $R_{e\setminus y}^{-1} L_{y/x} R_{e\setminus x}$ and $R_{e\setminus(yx)}^{-1} R_x R_{e\setminus y}$ by $R_{e\setminus y}^{-1} R_{x\setminus y} R_{e\setminus x}$. The permutations of the proposition fix e, and hence it remains to observe that $R_{e\setminus y}^{-1} L_{y/x} R_{e\setminus x} = (L_{y/e}^{-1} R_{e\setminus y})^{-1} (L_{y/e}^{-1} L_{y/x} L_{x/e})(L_{x/e}^{-1} R_{e\setminus x})$. □

Lemma 1.3. *Let Q be a quasigroup and $e \in Q$. Then $R_{e\backslash y}^{-1} L_x L_e^{-1} R_{x\backslash y}$ and $L_{y/e}^{-1} R_x R_e^{-1} L_{y/x}$ fix both x and e, for all $x, y \in Q$.*

Proof. Use direct verification, e.g., $R_{e\backslash y}^{-1} L_x L_e^{-1} R_{x\backslash y}(x) = R_{e\backslash y}^{-1} L_x L_e^{-1}(y) = R_{e\backslash y}^{-1} L_x(e \backslash y) = R_{e\backslash y}^{-1}(x \cdot (e \backslash y)) = x$. □

Lemma 1.4. *Let Q be a quasigroup and $e \in Q$. Then $(\operatorname{Mlt} Q)_e$ is generated by the union of the sets $\{R_{e\backslash y}^{-1} L_x L_e^{-1} R_{x\backslash y},\ L_{y/e}^{-1} R_x R_e^{-1} L_{y/x};\ x, y \in Q\}$ and $\{R_{xe}^{-1} L_e L_x,\ L_{ex}^{-1} R_e R_x,\ L_{x/e}^{-1} R_{e\backslash x};\ x \in Q\}$.*

Proof. We see immediately that $R_{xe}^{-1} L_e L_x(e) = e = L_{ex}^{-1} R_e R_x(e)$. In view of the left-right symmetry it suffices to show, by Proposition 1.2 and Lemma 1.3, that $L_{y/e}^{-1} L_{y/x} L_{x/e}$ is generated by the permutations of the lemma. We have $L_{y/e}^{-1} L_{y/x} L_{x/e} = (L_{y/e}^{-1} R_{e\backslash y})(R_{e\backslash y}^{-1} L_{y/x} L_e^{-1} R_x)(R_x^{-1} L_e L_{x/e})$. □

Lemma 1.4 describes a generating set of $(\operatorname{Mlt} Q)_e$ that is a union of two sets. Permutations in one of the sets always fix another element $x \in Q$, $x \neq e$, by Lemma 1.3. If $\operatorname{Mlt} Q$ happens to be a Frobenius group, then all these permutations collapse to the identity mapping. Such a collapse can be expressed by two identities using operations $\cdot$, $\backslash$ and $/$ (one identity for $R_{e\backslash y}^{-1} L_x L_e^{-1} R_{x\backslash y}$ and one for $L_{y/e}^{-1} R_x R_e^{-1} L_{y/x}$). We shall observe that each of these two identities implies the other one, and that these identities express nothing else but the fact that Q is isotopic to an Abelian group.

Lemma 1.5. *Let Q be a quasigroup and let e be its element. The following are equivalent:*

(i) *$R_{e\backslash y}^{-1} L_x L_e^{-1} R_{x\backslash y}$ is the identity mapping for all $x, y \in Q$;*
(ii) *$(xz)/(e \backslash y) = (ez)/(x \backslash y)$ for all $x, y, z \in Q$; and*
(iii) *$((ex)/y)z = ((ez)/y)x$ for all $x, y, z \in Q$.*

Proof. Express (i) as $R_{e\backslash y}^{-1} L_x = R_{x\backslash y}^{-1} L_e$. That means $(xz)/(e\backslash y) = (ez)/(x\backslash y)$. Equivalently $(xz)/(e \backslash (xy)) = (ez)/y$ and $xz = ((ez)/y)(e \backslash (xy))$. Put $v = e \backslash (xy)$. Then $x = (ev)/y$ and the latter identity turns to $((ev)/y)z = ((ez)/y)v$. □

Lemma 1.6. *Let Q be a quasigroup and let e be its element. If $((xy)/e)z = ((xz)/e)y$ for all $x, y, z \in Q$, then Q is isotopic to an Abelian group.*

Proof. Define a new operation $\circ$ by $x \circ y = (x/e) \cdot (e \backslash y)$. It is a loop operation, with ee being its neutral element. If $x, y, z \in Q$, then $((xe) \circ (ey)) \circ (ez) = ((xy)/e)z = ((xz)/e)y = ((xe) \circ (ez)) \circ (ey)$. Hence $(u \circ v) \circ w = (u \circ w) \circ v$ for all $u, v, w \in Q$. A loop satisfying such an identity has to be an Abelian group (we have $v \circ w = w \circ v$ and $(u \circ v) \circ w = (v \circ u) \circ w = (v \circ w) \circ u = u \circ (v \circ w)$). □

Lemma 1.7. *Let Q be a principal isotope of an Abelian group $A(+)$, with $x \cdot y = \alpha(x) + \beta(y)$. Then $x/y = \alpha^{-1}(x - \beta(y))$, $x \setminus y = \beta^{-1}(x - \alpha(y))$ and $((x \cdot y)/e) \cdot z = ((x \cdot z)/e) \cdot y$ for all $e, x, y, z \in Q$.*

P r o o f. It is easy to verify that x/y and $y \setminus x$ are expressed correctly. Now, $((x \cdot y)/e) \cdot z = ((\alpha(x) + \beta(y))/e) \cdot z = \alpha^{-1}(\alpha(x) + \beta(y) - \beta(e)) \cdot z = \alpha(x) + \beta(y) - \beta(e) + \beta(z) = \alpha(x) + \beta(z) - \beta(e) + \beta(y) = ((x \cdot z)/e) \cdot y$. □

By combining Lemmas 1.5, 1.6 and 1.7 we obtain:

Proposition 1.8. *Let Q be a quasigroup and let e be its element. The following are equivalent:*

(i) *Q is isotopic to an Abelian group;*
(ii) *$((xy)/e)z = ((xz)/e)y$ holds for all $x, y, z \in Q$;*
(iii) *$((xy)/v)z = ((xz)/v)y$ holds for all $x, y, v, z \in Q$;*
(iv) *the mappings $R^{-1}_{z\setminus y} L_x L_z^{-1} R_{x\setminus y}$ and $L^{-1}_{y/z} R_x R_z^{-1} L_{y/x}$ equal the identity permutation for all $x, y, z \in Q$.*

Proposition 1.9. *Let Q be a quasigroup which is isotopic to an Abelian group, and let e be its element. Then $(\mathrm{Mlt}\, Q)_e = \langle L^{-1}_{(e\cdot xe)/e} L_e L_x,\ R^{-1}_{e\setminus(ex\cdot e)} R_e R_x;\ x \in Q \rangle$, and $R^{-1}_{e\setminus x} L_{x/e} = R_e^{-1} L_e$ for all $x \in Q$.*

P r o o f. Put $H = \langle L^{-1}_{(e\cdot xe)/e} L_e L_x, R^{-1}_{e\setminus(ex\cdot e)} R_e R_x;\ x \in Q \rangle$. Setting $x = e/e$ and $x = e\setminus e$ gives $L_{e/e} \in H$ and $R_{e\setminus e} \in H$, respectively. Hence $L_{e/e}, R_{e\setminus e} \in H \cap (\mathrm{Mlt}\, Q)_e$. From Proposition 1.8 and Lemma 1.5 we see that $(xz)/(v \setminus y) = (vz)/(x \setminus y)$ for all $v, x, y, z \in Q$, and therefore $R^{-1}_{e\setminus x} L_{x/e}(z) = ((x/e)z)/(e \setminus x) = (ez)/((x/e) \setminus x) = (ez)/e = R_e^{-1} L_e(z)$ for all $x, z \in Q$. Thus $L^{-1}_{x/e} R_{e\setminus x} = L_e^{-1} R_e = L^{-1}_{e/e} R_{e\setminus e} \in H \cap (\mathrm{Mlt}\, Q)_e$ for all $x \in Q$. From $xe = e \setminus (e \cdot xe)$ and $ex = (ex \cdot e)/e$ we hence get $L^{-1}_{(e\cdot xe)/e} R_{xe}, R^{-1}_{e\setminus(ex\cdot e)} L_{ex} \in H \cap (\mathrm{Mlt}\, Q)_e$, and the equalities

$$L^{-1}_{(e\cdot xe)/e} L_e L_x = (L^{-1}_{(e\cdot xe)/e} R_{xe})(R^{-1}_{xe} L_e L_x)$$

and

$$R^{-1}_{e\setminus(ex\cdot e)} R_e R_z = (R^{-1}_{e\setminus(ex\cdot e)} L_{ex})(L^{-1}_{ex} R_e R_x)$$

yield the rest, by Lemma 1.4 and Proposition 1.8. □

2. Central quasigroups

Central quasigroups can be defined as quasigroups with a trivial central congruence. The notion of central congruence became prominent after Smith published his treatise on Mal'cev varieties [18]. His work was inspired to a large extent by study of quasigroups, and Chapter III of [7] renders those results of [18] that are relevant for them. The coincidence of central quasigroups with earlier defined T-quasigroups [16], [17] can be derived from [7] in an easy way. The explicit proof can be found in [5], where the approach via tame congruences is used. We get the result as a side effect of our investigation of $\operatorname{Mlt} Q$ (see Proposition 2.5 below). This investigation also yields an equational characterization of central quasigroups (Proposition 2.2), which is different from that of [4]. The main results of the section are Propositions 2.7, 2.8 and 2.9 (which seem to be new).

It is easy to see that an equivalence ϱ on Q, Q a quasigroup, is a congruence if and only if it is invariant under $\operatorname{Mlt} Q$. Each block of ϱ then determines ϱ uniquely. A subquasigroup is called *normal* if it is a block of some congruence ϱ. The multiplication group $\operatorname{Mlt} Q$ can also be used to characterize normal subquasigroups: one easily verifies that a subquasigroup $S \subseteq Q$ is normal if and only if $(\operatorname{Mlt} Q)_e$ preserves S for at least one (and hence for all) $e \in S$ (a proof can be found in [14]).

The diagonal $\{(x,x);\ x \in Q\}$ is a subquasigroup of $Q \times Q$ for every quasigroup Q. The quasigroup Q is called *central* if the diagonal is a normal subquasigroup.

This definition does not immediately convey a description by identities. However, it is immediate from Birkhoff's theorem that such a description exists. The description below consists of identities which express that (1) Q is isotopic to an Abelian group, that (2) for every $e \in Q$ the permutations $R_{xe}^{-1} L_e L_x$, $x \in Q$, coincide, and similarly, that (3) the permutations $L_{ex}^{-1} R_e R_x$ do not depend on the choice of $x \in Q$ (cf. Lemma 1.4; note also a similarity to a description of conjugacy closed loops [10]).

Lemma 2.1. *A central quasigroup is isotopic to an Abelian group.*

P r o o f. Let Q be a central quasigroup, and consider $e, x, y, z \in Q$. Then $\varphi = R^{-1}_{(e,e)\backslash(y,y)} L_{(e,x)} L^{-1}_{(e,e)} R_{(e,x)\backslash(y,y)}$ belongs to $(\operatorname{Mlt}(Q \times Q))_{(e,e)}$, by Lemma 1.3, and $\varphi((z,z)) = (R^{-1}_{e\backslash y} L_e L_e^{-1} R_{e\backslash y}(z), R^{-1}_{e\backslash y} L_x L_e^{-1} R_{x\backslash y}(z)) = (z, \psi(z))$, where $\psi = R^{-1}_{e\backslash y} L_x L_e^{-1} R_{x\backslash y}$. The diagonal is supposed to be a normal subquasigroup, and so ψ has to be the identity. This means that Q is isotopic to an Abelian group, by Lemma 1.5 and Proposition 1.8. □

Proposition 2.2. *Let Q be a quasigroup isotopic to an Abelian group, and let e be an element of Q. The following are equivalent:*

(i) *Q is a central quasigroup;*

(ii) $(e(xy))/(xe) = (e(ey))/(ee)$ *and* $(ex) \setminus ((yx)e) = (ee) \setminus ((ye)e)$ *for all* $x, y \in Q$; *and*

(iii) *the mappings* $L_{ex}^{-1} R_e R_x$ *and* $R_{xe}^{-1} L_e L_x$ *are independent on the choice of* $x \in Q$, *respectively.*

Proof. Parts (ii) and (iii) clearly express the same identities. The stabilizer of $\mathrm{Mlt}(Q \times Q)$ at (e, e) is generated by the mappings $R_{(xe,ye)}^{-1} L_{(e,e)} L_{(x,y)}$, $L_{(ex,ey)}^{-1} R_{(e,e)} R_{(x,y)}$ and $L_{(x/e,y\setminus e)}^{-1} R_{(e\setminus x,e\setminus y)}$, by Proposition 1.8 and Lemma 1.4. Therefore the diagonal of $Q \times Q$ is its normal subquasigroup if and only if these mappings send each (z, z) to some (u, u), and this is true precisely when $R_{xe}^{-1} L_e L_x = R_{ye}^{-1} L_e L_y$, $L_{ex}^{-1} R_e R_x = L_{ey}^{-1} R_e R_y$ and $L_{x/e}^{-1} R_{e\setminus x} = L_{y/e}^{-1} R_{e\setminus y}$, for all $x, y \in Q$. The equality $L_{x/e}^{-1} R_{e\setminus x} = L_{y/e}^{-1} R_{e\setminus y}$ holds in all quasigroups which are isotopic to an Abelian group, by Proposition 1.9, and nothing else needs to be proved. □

Lemma 2.3. *Let* φ *be a mapping* $A \to A$, *where* $A(+)$ *is an Abelian group. Then*

$$\varphi(a + b) + \varphi(c + d) = \varphi(a + c) + \varphi(b + d)$$

for all $a, b, c, d \in A$ *if and only if there exist* $\alpha \in \mathrm{End}(A)$ *and* $u \in A$ *with* $\varphi(a) = \alpha(a) + u$ *for all* $a \in A$.

Proof. The converse implication is clear; suppose that the equality holds. The choice $c = d = 0$ yields $\varphi(a + b) + \varphi(0) = \varphi(a) + \varphi(b)$, and hence by setting $\alpha(x) = \varphi(x) - \varphi(0)$ we get $\alpha(a+b) = \varphi(a+b) + \varphi(0) - 2\varphi(0) = \varphi(a) + \varphi(b) - \varphi(0) - \varphi(0) = \alpha(a) + \alpha(b)$. □

Lemma 2.4. *Suppose that* Q *is a quasigroup with* $x \cdot y = \varphi(x) + \psi(y)$ *for all* $x, y \in Q$, *and that* $Q(+)$ *is an Abelian group. The identity* $(e(xz))/(xe) = (e(yz))/(ye)$ *is satisfied in* Q *for all* $x, y, z, e \in Q$ *if and only if there exist* $\alpha \in \mathrm{Aut}(Q(+))$ *and* $u \in Q$ *with* $\psi(x) = \alpha(x) + u$ *for all* $x \in Q$.

Proof. The equality $(e(xz))/(xe) = (e(yz))/(ye)$ means $e(yz) - \psi(ye) = e(xz) - \psi(xe)$, by Lemma 1.7, and this translates to $\psi(a+b) - \psi(a+d) = \psi(b+c) - \psi(c+d)$, where $a = \varphi(y)$, $b = \psi(z)$, $c = \varphi(x)$ and $d = \psi(e)$. The rest follows from Lemma 2.3. □

We are now ready to reprove a well known description of central quasigroups. Proposition 2.2 and Lemma 2.4 (together with its left-right symmetric version) namely yield

Proposition 2.5. *Let Q be a quasigroup, where $x \cdot y = \varphi(x) + \psi(y)$ for an Abelian group $Q(+)$. Then Q is central if and only if there exist $\alpha, \beta \in \operatorname{Aut}(Q(+))$ and $u, v \in Q$ such that $\varphi(x) = \alpha(x) + u$ and $\psi(x) = \beta(x) + v$, for all $x \in Q$.*

Corollary 2.6. *A quasigroup Q is central if and only if there exist an Abelian group $Q(+)$, its automorphisms α and β, and an element $u \in Q$, such that for all $x, y \in Q$*

$$x \cdot y = \alpha(x) + \beta(y) + u.$$

Propositition 2.7. *Let Q be a quasigroup, where $x \cdot y = \varphi(x) + \psi(y)$, $Q(+)$ an Abelian group. Put $G = \operatorname{Mlt} Q$ and $N = \operatorname{Mlt} Q(+)$. Then $N \trianglelefteq G$ if and only if Q is central.*

P r o o f. Denote the translation $z \mapsto x + z$ by τ_x. Then $N = \{\tau_x;\, x \in Q\}$ and $\operatorname{Mlt} Q = \langle N, \varphi, \psi \rangle$. We wish to understand when for every $x \in Q$ there exists $y \in Q$ with $\varphi \tau_x \varphi^{-1} = r_y$. The equation $\varphi \tau_x = \tau_y \varphi$ turns into $\varphi(x + z) = y + \varphi(z)$, for all $z \in Q$, and hence there must be $y = \varphi(x) - \varphi(0)$. Thus we ask when $\varphi(x + z) + \varphi(0) = \varphi(x) + \varphi(z)$, for all $x, z \in Q$, and this is clearly the case if and only if $\alpha(x) = \varphi(x) - \varphi(0)$ defines an automorphism of $Q(+)$. The rest follows from the left-right symmetry and from Proposition 2.5. □

In this paper we are using the notion of a Frobenius group for those permutation groups which are not regular, and where only the identity fixes two or more points (unlike some other authors who require the existence of a Frobenius kernel when considering infinite Frobenius groups; recall that a Frobenius group contains the Frobenius kernel if and only if all regular permutations and the identity form a transitive subgroup).

The following statement is a direct consequence of Proposition 1.8, and was already alluded to in the paragraph following Lemma 1.4.

Proposition 2.8. *Let Q be a quasigroup and suppose that* $\operatorname{Mlt} Q$ *is a Frobenius group. Then Q is isotopic to an Abelian group.*

Finite Frobenius groups always possess the Frobenius kernel, and hence from Propositions 2.8 and 2.7 we immediately derive

Proposition 2.9. *Let Q be a finite quasigroup and suppose that* $\operatorname{Mlt} Q$ *is a Frobenius group. Then Q is central.*

The rest of the paper was motivated by the question if the finiteness assumption in Proposition 2.9 is unavoidable. The goal was to find an infinite Q which is not central and yet $\operatorname{Mlt} Q$ is a Frobenius group. We shall see that this condition is satisfied already when Q is free in the variety of all quasigroups that are isotopic to an Abelian group.

3. Relatively free quasigroup

The aim of this section is to develop free objects in the variety of quasigroups isotopic to Abelian groups. The idea is the same as that of [13]. Formal aspects differ because of the need to prepare for applications in the subsequent sections. We start by a somewhat nonstandard notation for elements of a free Abelian group with a base X. Such a group can be regarded as a set of all mappings $\alpha\colon X \to \mathbb{Z}$ with finite support, where $(\alpha+\beta)(x) = \alpha(x)+\beta(x)$ for all $x \in X$. One usually identifies $x \in X$ with a mapping $\alpha\colon X \to \mathbb{Z}$, $\alpha(x) = 1$ and $\alpha(y) = 0$ for all $y \in X$, $y \neq x$, and then identifies elements of the group with formal sums over $\pm X$, in which x and $-x$ appear together for no $x \in X$. The meaning of $+$ within these formal sums can be separated from the meaning of $+$ when the addition is actually performed (one can speak about a 'constitutional' and an 'operational' plus). We shall use $\oplus$ to denote the 'constitutional' plus. The free Abelian group $F(X)$ over X is thus formed by all sums $a_1 \oplus \dots \oplus a_k$ where either $a_i = x$, or $a_i = -x$, for some $x \in X$, and where for no $i, j \in \{1,\dots,k\}$, $i \neq j$, there exists $x \in X$ with $a_i = x$ and $a_j = -x$. Let us stress that $\oplus$ is not the operation of $F(X)$ (which remains to be denoted by $+$). Hence some terms constructed by means of $\oplus$ need not be elements of $F(X)$. If $x, y \in X$, then, e.g., $x \oplus y = x + y \in F(X)$, $(x \oplus y) - y = (x \oplus y) + (-y) = x = x + y - y$, and $(x \oplus y) \oplus (-y) \notin F(X)$. We shall write $u \ominus v$ in place of $u \oplus (-v)$. The following lemma is clear.

Lemma 3.1. *Assume $w = u + v$, where $u, v \in F(X)$, and assume $0 \notin \{u, v, w\}$. Then exactly one of the following cases applies:*
(1) *$w = u \oplus v$;*
(2) *$u = t \ominus v$ for some $t \in F(X)$, $t \neq 0$;*
(3) *$v = t \ominus u$ for some $t \in F(X)$, $t \neq 0$;*
(4) *$u = u' \oplus t$ and $v = v' \ominus t$ for some $u', v', t \in F(X) \setminus \{0\}$, and $u' \oplus v' \in F(X)$.*

We shall now construct words using not only $\oplus$, but also operators $\alpha^{\pm 1}[-]$ and $\beta^{\pm 1}[-]$. If U is a set of words, then $\Gamma(U)$ will consist of all words $\gamma[u]$, where γ is α

or α^{-1} or β or β^{-1}, and $u \in U$ is not of the form $\gamma^{-1}[u']$ (we assume $(\alpha^{-1})^{-1} = \alpha$ and $(\beta^{-1})^{-1} = \beta$).

For a set of variables X define $B_0 \subseteq B_1 \subseteq \ldots$ in such a way that $B_0 = X$ and $B_{i+1} = \Gamma(F(B_i)) \cup B_i$. Put $B = \bigcup_{i>0} B_i$ and denote $F(B)$ by $W(X)$.

Lemma 3.2. *$B_{i+1} = X \cup \Gamma(F(B_i))$ for every $i \geqslant 0$.*

Proof. We shall show that $B_j \subseteq X \cup \Gamma(F(B_i))$ for all $j \leqslant i+1$. The case $j = 0$ is clear. If $j \leqslant i$ and $B_j \subseteq X \cup \Gamma(F(B_i))$, then $B_j \subseteq B_i$ implies $\Gamma(F(B_j)) \subseteq \Gamma(F(B_i))$, and hence $B_{j+1} \subseteq X \cup \Gamma(F(B_i))$. □

We see from Lemma 3.2 that the elements of B which are not from X have the form $\gamma[t]$, where $\gamma = \alpha^{\pm 1}$ or $\gamma = \beta^{\pm 1}$, and $t \in W(X)$. There is no other restriction to the form of t, but the fact that it is not of the form $\gamma^{-1}[t']$.

There is $W(X) = F(B)$, and hence on $W(X)$ there are defined a binary operation $+$ and a unary operation $-$. For $\gamma = \alpha^{\pm 1}$ or $\gamma = \beta^{\pm 1}$ define $\gamma(t)$, $t \in W(X)$, in such a way that $\gamma(t) = \gamma[t]$ if t is not of the form $\gamma^{-1}[t']$, and $\gamma(t) = t'$, if $t = \gamma^{-1}[t']$.

Define, furthermore, operations $\circ$, $/$ and $\backslash$ on $W(X)$ by $s \circ t = \alpha(s) + \beta(t)$, $s/t = \alpha^{-1}(s - \beta(t))$ and $s \backslash t = \beta^{-1}(t - \alpha(s))$ (cf. Lemma 1.7). These operations turn $W(X)$ into a quasigroup. Denote by $Q(X)$ the subquasigroup of $W(X)$ that is generated by X.

Lemma 3.3. *The quasigroups $W(X)$ and $Q(X)$ are isotopic to an Abelian group.*

Proof. The quasigroup $W(X)$ is a principal isotope of $F(B)$ by the definition. Quasigroups isotopic to an Abelian group form a variety, by Proposition 1.8, and hence every subquasigroup of $W(X)$ is also isotopic to an Abelian group. □

Proposition 3.4. *Let Q be a quasigroup which is isotopic to an Abelian group and let $\varphi\colon X \to Q$ be a mapping. Then there exists $\psi\colon W(X) \to Q$ which is a homomorphism of quasigroups and which extends φ.*

Proof. The quasigroup Q is assumed to be isotopic to an Abelian group, and hence there exist permutations f and g, and an Abelian group operation $+$, such that $uv = f(u) + g(v)$ for all $u, v \in Q$.

The homomorphism ψ will be defined inductively on $X = B_0 \subseteq B_1 \subseteq \ldots$ and on $F(B_0) \subseteq F(B_1) \subseteq \ldots$ in such a way that one obtains the compatibility of the binary operation $+$ and of the unary operations α, α^{-1}, β and β^{-1} (which correspond to f, f^{-1}, g and g^{-1}, respectively). These operations appear as partially defined during the induction process. However, at its end the compatibility of partially defined operations turns into the compatibility of full operations, and the compatibility of the quasigroup operations follows immediately.

The first step of the induction is determined by φ. Let ψ be defined on B_i. Extend it to get a homomorphism of Abelian groups $F(B_i) \to Q(+)$, and send every $\alpha^{\pm 1}[t] \in \Gamma(F(B_i)) \setminus F(B_i)$ to $f^{\pm 1}(\psi(t))$, and $\beta^{\pm 1}[t]$ to $g^{\pm 1}(\psi(t))$. In this way one clearly retains the required compatibility, and nothing else is needed. □

Corollary 3.5. *The quasigroup $Q(X)$ is free in the variety of all quasigroups that are isotopic to Abelian groups.*

The precise interaction of $Q(X)$ and $W(X)$ offers various questions. It is quite easy, e.g., to prove that 0 never occurs as a subterm in any $t \in Q(X)$. Nevertheless, I am not aware of any algorithm that decides when a term $t \in W(X)$ belongs to $Q(X)$.

4. The depth and its changes

For a term $t \in W(X)$ define its *depth* $d(t)$ inductively by $d(x) = d(0) = 0$ for all $x \in X$, $d(-t) = d(t)$ for all $t \in W(X)$, $d(t_1 \oplus t_2) = \max\{d(t_1), d(t_2)\}$ whenever t_1, t_2 and $t_1 \oplus t_2$ belong to $W(X)$, and $d(\gamma^{\pm 1}[t]) = d(t) + 1$ whenever $t, \gamma^{\pm 1}[t] \in W(X)$ and γ stands for α or β.

The depth $d(t)$ thus corresponds to the longest chain of embedded operators $\alpha^{\pm 1}$ and $\beta^{\pm 1}$.

Let us assume $X \neq \emptyset$, and let us fix some $e \in X$. We shall be considering the group $H = (\mathrm{Mlt}\, W(X))_e$. For $v \in W(X)$ put $\lambda_v = L^{-1}_{(e\circ(v\circ e))/e} L_e L_v$ and $\varrho_v = R^{-1}_{e\backslash((e\circ v)\circ e)} R_e R_v$. Then $H = \langle \lambda_v, \varrho_v;\, v \in W(X)\rangle$, by Proposition 1.9, and we have $(e \circ (v \circ e))/e = \alpha^{-1}(\beta(\alpha(v) + \beta(e)) + \alpha(e) - \beta(e))$ and $e \backslash ((e \circ v) \circ e) = \beta^{-1}(\alpha(\beta(v) + \alpha(e)) + \beta(e) - \alpha(e))$. Direct calculations yield:

Lemma 4.1. *Consider $u, v \in W(X)$. Then:*

(i) $\varrho_v(u) = \alpha^{-1}(\alpha(\beta(v) + \alpha(u)) - \alpha(\beta(v) + \alpha(e)) + \alpha(e))$;

(ii) $\varrho_v^{-1}(u) = \alpha^{-1}(\alpha^{-1}(\alpha(\beta(v) + \alpha(e)) - \alpha(e) + \alpha(u)) - \beta(v))$;

(iii) $\lambda_v(u) = \beta^{-1}(\beta(\alpha(v) + \beta(u)) - \beta(\alpha(v) + \beta(e)) + \beta(e))$; *and*

(iv) $\lambda_v^{-1}(u) = \beta^{-1}(\beta^{-1}(\beta(\alpha(v) + \beta(e)) - \beta(e) + \beta(u)) - \alpha(v))$.

Our goal is to show that if $\varphi \in H$ fixes some $u_0 \neq e$ then φ has to be the identity. Every $\varphi \in H$ can be expressed as $\mu_k \dots \mu_1$, where each μ_i, $1 \leqslant i \leqslant k$, is equal to $\lambda_{v_i}^{\pm 1}$ or $\varrho_{v_i}^{\pm 1}$, $v_i \in W(X)$. Assume $\varphi(u_0) = u_0$ and put $u_i = \mu_i \dots \mu_1(u_0)$. The mapping $i \mapsto d(u_i)$, $0 \leqslant i \leqslant k$, attains a maximum at some j, $1 \leqslant j \leqslant k$, as $u_0 = u_k$. Set $u = u_j$, $\psi_1 = \mu_{j+1}$ (where $\mu_{k+1} = \mu_1$) and $\psi_2 = \mu_j^{-1}$. Then $d(\psi_1(u)) \leqslant d(u)$ and $d(\psi_2(u)) \leqslant d(u)$. We can assume $\psi_1 \neq \psi_2$. It will be shown that the existence of u,

ψ_1 and ψ_2 with such properties is possible only under very specific circumstances, and from that it will follow that $\varphi = \mu_k \dots \mu_1$ has to equal the identity.

The strategy described in the preceding paragraph requires a rather detailed description of cases with $d(\varrho_v^{\pm 1}(u)) \leqslant d(u)$ or $d(\lambda_v^{\pm 1}(u)) \leqslant d(u)$. This is not difficult, but quite lengthy. In order to deal efficiently with the list of all possible cases, some additional structural notions will be defined.

Consider $w \in W(X)$. Then $w_1 \in W(X)$ is said to be an *additive factor* of $w \in W(X)$, if there exists $w_2 \in W(X)$ such that $w = w_1 \oplus w_2$. We have $W(X) = F(B)$, and so each $w \neq 0$ can be expressed as $w_1 \oplus \dots \oplus w_k$, $k \geqslant 1$, where $w_i \in \pm B$, $1 \leqslant i \leqslant k$. Call each w_i a *base factor* of w. Every additive factor is clearly a non-empty sum of base factors. Suppose now that the base factors $w_1, \dots, w_k$ are ordered in such a way that $d(w_1) \geqslant d(w_2) \geqslant \dots \geqslant d(w_k)$, and let h, $1 \leqslant h \leqslant k$, be the greatest integer with $d(w_1) = d(w_h)$. Then $w_1 \oplus \dots \oplus w_h \in W(X)$ will be called *the leading part* of w. A leading part of 0 is, by definition, 0 again.

We shall be mostly dealing with $w \in W(X)$ that are of the form $\alpha^{-1}[w']$ or $\beta^{-1}[w']$, in which we shall investigate the structure of w'. That is why we also define the *α-leading part* of w as the leading part of $\alpha(w)$, and, similarly, the *β-leading part* of w as the leading part of $\beta(w)$.

One has $\lambda_{e/e} = L_{e/e}$ and $\varrho_{e\backslash e} = R_{e\backslash e}$. This makes the cases $v = e/e$ and $v = e \setminus e$ somewhat special, and they will be often treated separately in the discussions below.

Lemma 4.2. *Consider $u, v \in W(X)$ and assume $u \neq e$, $v \neq e \setminus e$ and $d(\varrho_v(u)) \leqslant d(u)$. Then exactly one of the following alternatives takes place.*

(1) *There exist $u', v' \in W(X)$ such that $d(u') = d(v') = 0$, $u' \neq 0$, $v' \neq e$, $u = \alpha^{-1}(\alpha(e) - u')$, $v = \beta^{-1}(v' - \alpha(e))$ and $\varrho_v(u) = \alpha^{-1}(\alpha(v' - u') - \alpha(v') + \alpha(e))$.*
(2) *There exist $u', v' \in W(X)$ such that $d(u') = d(v') = 0$, $v' \neq e$, $u = \alpha^{-1}(\alpha^{-1}(u') - v' + \alpha(e))$, $v = \beta^{-1}(v' - \alpha(e))$ and $\varrho_v(u) = \alpha^{-1}(u' - \alpha(v') + \alpha(e))$.*
(3) *There exist $u', v' \in W(X)$ such that $d(u') = d(v') = 0$, $u = \alpha^{-1}(\alpha(e) + u' - \alpha^{-1}(v'))$, $v = \beta^{-1}(\alpha^{-1}(v') - \alpha(e))$ and $\varrho_v(u) = \alpha^{-1}(\alpha(u') - v' + \alpha(e))$.*
(4) *There is $\alpha[\alpha(e) + \beta(v)] \in W(X)$ and there exist $u' \in W(X)$ such that $d(\beta(v)) \leqslant d(u')$, $1 \leqslant d(u')$, $u = \alpha^{-1}[\alpha^{-1}[u'] - \beta(v)]$ and $\varrho_v(u) = \alpha^{-1}(u' - \alpha[\alpha(e) + \beta(v)] + \alpha(e))$.*
(5) *There is $\alpha[\alpha(u) + \beta(v)] \in W(X)$ and there exist $u', v' \in W(X)$ such that $d(u') \leqslant d(v')$, $1 \leqslant d(v')$, $u = \alpha^{-1}[u' - \alpha^{-1}[v']]$, $v = \beta^{-1}[\alpha^{-1}[v'] \ominus \alpha(e)]$ and $\varrho_v(u) = \alpha^{-1}(\alpha[u' - \alpha(e)] - v' + \alpha(e))$.*
(6) *There exist $u', v' \in W(X)$ such that $u = \alpha^{-1}[\alpha^{-1}[u'] \ominus \alpha^{-1}[v'] \oplus \alpha(e)]$, $v = \beta^{-1}[\alpha^{-1}[v'] \ominus \alpha(e)]$ and $\varrho_v(u) = \alpha^{-1}(u' - v' + \alpha(e))$.*

Proof. Let us first consider the case $\beta(v) = 0$. Lemma 4.1 (i) then gives $\varrho_v(u) = \alpha^{-1}(\alpha^2(u) - \alpha^2(e) + \alpha(e))$. We assume $u \neq e$, and hence $\varrho_v(u)$ equals

$\alpha^{-1}[\alpha^2(u) \ominus \alpha^2(e) \oplus \alpha(e)]$ if there exists no $u_1 \in W(X)$ such that $u = \alpha^{-2}[u_1]$. Then $d(\varrho_v(u)) \geqslant 1 + d(\alpha^2(u)) \geqslant 1 + d(u)$, and so there must exist $u_1 \in W(X)$ with $u = \alpha^{-2}[u_1]$. However, that is a special case of the alternative (4), and we can assume $\beta(v) \neq 0$ in the rest of the proof.

From $e \backslash e = \beta^{-1}(e - \alpha(e))$ and $v \neq e \backslash e$ we obtain $\beta(v) + \alpha(e) \neq e$. Since $\beta(v) \neq 0$, only one case of Lemma 3.1 gets applicable if $0 \neq \beta(v) \oplus \alpha(e) \notin W(X)$. Thus $\beta(v) \oplus \alpha(e) \notin W(X)$ precisely when there exists $v_1 \in W(X)$ with $v = \beta^{-1}[v_1 - \alpha(e)]$. (Note that this covers also the case $\beta(v) + \alpha(e) = 0$.) We also see that such a v_1 has to exist, if $\alpha[\beta(v) + \alpha(e)] \notin W(X)$, and in such a situation it equals $\alpha^{-1}[v']$, for some $v' \in W(X)$. Then $v = \beta^{-1}[\alpha^{-1}[v'] \ominus \alpha(e)]$, and this will be called the *exceptional e-case*. There is $\alpha[\beta(v) + \alpha(e)] \in W(X)$ in the other situations, and they will be referred to as the *general e-case*.

Note that the inequality $d(\alpha(\beta(v)) + \alpha(e)) \geqslant d(v)$ does not hold in the general e-case only when $v = \beta^{-1}[v_1 - \alpha(e)]$ and $d(v_1) = 0$. Let us consider this situation. Then $d(v) = 2$, $\alpha(\beta(v) + \alpha(e)) = \alpha[v_1]$ and $v_1 \neq e$. Furthermore, $e \neq u$ implies $\alpha(\beta(v) + \alpha(u)) \neq \alpha(\beta(v) + \alpha(e))$. This means that either there exists such a $u_1 \in W(X)$ that $\beta(v) + \alpha(u) = v_1 - \alpha(e) + \alpha(u)$ equals $\alpha^{-1}[u_1]$, or $\alpha^{-1}[\alpha[\beta(v) + \alpha(u)] \ominus \alpha[\beta(v) + \alpha(e)] \oplus \alpha(e)] \in W(X)$. The latter case can satisfy $d(\varrho_v(u)) \leqslant d(u)$ precisely when the depth of $\beta(v) + \alpha(u) = v_1 - \alpha(e) + \alpha(u)$ is zero. However, that happens if and only if there exists $u' \in W(X)$ with $u = \alpha^{-1}(\alpha(e) - u')$ and $d(u') = 0$. In this way we obtain the alternative (1) of our lemma, and we can consider the situation when $\alpha^{-1}[u_1] = v_1 - \alpha(e) + \alpha(u)$. This leads to $u = \alpha^{-1}[\alpha^{-1}[u_1] - v_1 + \alpha(e)]$ and $\varrho_v(u) = \alpha^{-1}(u_1 - \alpha(v_1) + \alpha(e))$, which constitutes the alternative (2) when $d(u_1) = 0$, and gives a special case of the alternative (4), when $d(u_1) \geqslant 1$.

In the further investigation of the general e-case we can therefore assume $d(\alpha(\beta(v) + \alpha(e))) \geqslant d(v)$. Let us first deal with the subcase $\alpha[\beta(v) + \alpha(u)] \in W(X)$. From $u \neq e$ and $\alpha(e) \neq \alpha(\beta(v) + \alpha(e))$ we get $\varrho_v(u) = \alpha^{-1}[\alpha[\beta(v) + \alpha(u)] \ominus \alpha[\beta(v) + \alpha(e)] \oplus \alpha(e)]$. If $d(\beta(v)) \neq d(\alpha(u))$, then $d(\beta(v) + \alpha(u)) = \max\{d(\beta(v)), d(\alpha(u))\}$, and one easily obtains $d(\varrho_v(u)) > d(u)$. If $d(\beta(v)) = d(\alpha(u)) > 1$, then $d(\varrho_v(u)) \geqslant 2 + d(\beta(v)) \geqslant 1 + d(u) > d(u)$ as well, and $d(\varrho_v(u)) > d(u)$ also when $d(u) \leqslant 1$. Hence $d(\beta(v)) = d(\alpha(u)) = 1$ and $d(u) = 2$. There must be $d(v) = 2$, as $d(v) = 0$ gives $d(\varrho_v(u)) \geqslant 2 + d(\beta[v] + \alpha[e]) = 3$. Recall that we are assuming $d(\alpha(\beta(v) + \alpha(e)) \geqslant d(v) = 2$, and so $d(\varrho_v(u)) \geqslant 1 + d(v) = 3 > d(u)$ in the remaining case as well.

Therefore $\alpha[\beta(v) + \alpha(u)] \notin W(X)$, and there either exists $v' \in W(X)$ such that $\alpha^{-1}[v']$ is a base factor of $\beta(v) = \alpha^{-1}[v'] - \alpha(u)$, or there exists $u' \in W(X)$ such that $\alpha^{-1}[u']$ is a base factor of $\alpha(u) = \alpha^{-1}[u'] - \beta(v)$. In the former case we obtain $\varrho_v(u) = \alpha^{-1}[(\alpha(e) + v') \ominus \alpha[\alpha^{-1}[v'] \oplus (\alpha(e) - \alpha(u))]]$, as $d(\alpha(e) + v') \leqslant d(\alpha^{-1}[v'] \oplus (\alpha(e) - \alpha(u)))$. This means $d(u) \geqslant d(\varrho_v(u)) \geqslant 3$, $d(\alpha(e) - \alpha(u)) = d(\alpha(u)) \geqslant d(u) - 1$

and $d(\varrho_v(u)) \geqslant 2 + d(\alpha(e) - \alpha(u)) \geqslant 1 + d(u)$, a contradiction. Hence we can assume the latter case, in which $u = \alpha^{-1}[\alpha^{-1}[u'] - \beta(v)]$ for some $u' \in W(X)$. This corresponds to the alternative (4) of the lemma. However, in that alternative one also requires $d(\beta(v)) \leqslant d(u')$, which we shall now prove.

Assume $d(u') < d(\beta(v))$ and note that then $d(u) \leqslant 1 + d(\beta(v))$ and $\varrho_v(u) = \alpha^{-1}(u' - \alpha[\beta(v) + \alpha(e)] + \alpha(e))$. If $d(\beta(v) + \alpha(e)) \geqslant d(\beta(v))$, then $d(\varrho_v(u)) = 2 + d(\beta(v)) > d(u)$, and hence $d(\beta(v) + \alpha(e)) < d(\beta(v))$ can be assumed. Then $d(\beta(v)) = 1$, $d(u') = 0$ and $v = \beta^{-1}[v' - \alpha(e)]$, where $d(v') = 0$. But this is a situation that has already been considered, as $d(v) = 2 > 1 = d(\alpha(\beta(v) + \alpha(e)))$.

From $d(u') \geqslant d(\beta(v))$ one gets $d(u') = 1$, as $d(u') = d(\beta(v)) = 0$ yields $d(u) = 2 < 3 = d(\varrho_v(u))$. This completes our investigation of the general e-case.

Let us now turn to the exceptional e-case. Then there exists $v' \in W(X)$ such that $v = \beta^{-1}[\alpha^{-1}[v'] \ominus \alpha(e)]$, and $\varrho_v(u) = \alpha^{-1}(\alpha(\alpha^{-1}[v'] - \alpha(e) + \alpha(u)) - v' + \alpha(e))$. Suppose first $\alpha[\alpha^{-1}[v'] - \alpha(e) + \alpha(u)] \notin W(X)$. This means that $\alpha^{-1}[v'] - \alpha(e) + \alpha(u) = \alpha^{-1}[w]$ for some $w \in W(X)$. Apply Lemma 3.1 to $(\alpha^{-1}[v'] \ominus \alpha(e)) + \alpha(u)$ and note that only case (3) of the lemma can take place, as $u \neq e$. Therefore $u = \alpha^{-1}[\alpha^{-1}[u'] \ominus \alpha^{-1}[v'] \oplus \alpha(e)]$ for some $u' \in W(X)$, and in this way we get the alternative (6).

For the rest of the proof $\alpha[\alpha^{-1}[v'] - \alpha(e) + \alpha(u)] \in W(X)$ can be assumed. Put $w = \alpha^{-1}[v'] - \alpha(e) + \alpha(u)$. If $\alpha(u) = 0$ or if $w = \alpha^{-1}[v'] \ominus \alpha(e) \oplus \alpha(u)$, then $d(\alpha[w]) > d(\alpha(e) - v')$, and hence $\varrho_v(u) = \alpha^{-1}[\alpha[w] \oplus (\alpha(e) - v')]$, which gives $d(\varrho_v(u)) > d(u)$. There is $u \neq e$, and therefore u has to equal $\alpha^{-1}[u_1]$ for some $u_1 \in W(X)$, if the latter situation is to be avoided. One also gets $d(u_1) \geqslant 1$, and we shall start with the case $d(u_1) = 1$. If $d(v') \geqslant 1$, then $w = \alpha^{-1}[v'] \oplus (\alpha(u) - \alpha(e))$, and $d(\varrho_v(u)) \geqslant 4 > 2 = d(u)$ follows. Hence $d(u_1) = 1$ implies $d(v') = 0$. If $d(w) \geqslant 1$, then $\varrho_v(u) = \alpha^{-1}[\alpha[w] \oplus (\alpha(e) - v')]$, and $d(\varrho_v(u)) \geqslant 3 > 2 = d(u)$. Therefore $d(w) = 0$ and $u_1 = \alpha(e) - \alpha^{-1}[w'] + w$, which gives the alternative (3).

Finally, assume $d(u_1) > 1$. Suppose first that neither $u_1 = -\alpha^{-1}[v']$, nor $u_1 = u' \ominus \alpha^{-1}[v']$ for some $u' \in W(X)$. Then $d(w) = \max\{d(v') + 1, d(u) - 1\}$, $\varrho_v(u) = \alpha^{-1}[\alpha[w] - v' + \alpha(e)]$ and $d(\varrho_v(u)) \geqslant d(u) + 1 > d(u)$. If $u_1 = u' \ominus \alpha^{-1}[v']$, where $d(u') > d(v')$, then one gets the same conclusion, and hence there has to be $d(u') \leqslant d(v')$. We have obtained the alternative (5).

It is easy to check that no two alternatives can take place simultaneously. In fact it suffices to compare each of the alternatives (1)–(5) to the alternative (6), as other cases can be handled immediately by using the observation contained in the following corollary. □

Corollary 4.3. *In the situation of Lemma 4.2 there always exists $w \in W(X)$ such that $u = \alpha^{-1}[w]$. The α-leading part of u is equal, in the alternatives* (1)–(5), *to* (1) $\alpha(e)$, (2) $\alpha(e) \oplus \alpha^{-1}(u')$, (3) $\alpha(e) \ominus \alpha^{-1}(v')$, (4) $\alpha^{-1}[u']$ *and* (5) $-\alpha^{-1}[v']$, *respectively. Furthermore,* $d(\alpha(u)) = 1$ *in the alternatives* (1)–(3), *and* $d(\alpha(u)) > 1$ *in the alternatives* (4)–(5).

Lemma 4.4. *Consider* $u, v \in W(X)$ *and assume* $u \neq e$, $v \neq e \backslash e$, *and* $d(\varrho_v^{-1}(u)) \leqslant d(u)$. *Then exactly one of the following alternatives takes place.*

(1) *There exist* $u', v' \in W(X)$ *such that* $d(u') = d(v') = 0$, $u' \neq 0$, $u = \alpha^{-1}(\alpha(e) + u')$, $v = \beta^{-1}(\alpha^{-1}(v') - \alpha(e))$ *and* $\varrho_v^{-1}(u) = \alpha^{-1}(\alpha^{-1}(u' + v') - \alpha^{-1}(v') + \alpha(e))$.

(2) *There exist* $u', v' \in W(X)$ *such that* $d(u') = d(v') = 0$, $v' \neq e$, $u = \alpha^{-1}(u' - \alpha(v') + \alpha(e))$, $v = \beta^{-1}(v' - \alpha(e))$ *and* $\varrho_v^{-1}(u) = \alpha^{-1}(\alpha^{-1}(u') - v' + \alpha(e))$.

(3) *There exist* $u', v' \in W(X)$ *such that* $d(u') = d(v') = 0$, $u = \alpha^{-1}(\alpha(u') - v' + \alpha(e))$, $v = \beta^{-1}(\alpha^{-1}(v') - \alpha(e))$ *and* $\varrho_v^{-1}(u) = \alpha^{-1}(u' - \alpha^{-1}(v') + \alpha(e))$.

(4) *There is* $\alpha[\alpha(e)+\beta(v)] \in W(X)$, *and there exists* $u' \in W(X)$ *such that* $d(\alpha(e)+\beta(v)) \geqslant d(u')$, $\alpha^{-1}[u'-\alpha(e)] \in W(X)$, $d(\alpha(e)+\beta(v)) \geqslant 1$, $u = \alpha^{-1}[u'-\alpha[\alpha(e)+\beta(v)]]$ *and* $\varrho_v^{-1}(u) = \alpha^{-1}(\alpha^{-1}[u' - \alpha(e)] - \beta(v))$.

(5) *There exist* $u', v' \in W(X)$ *such that* $d(v') \leqslant d(u')$, $d(u') \geqslant 1$, $u = \alpha^{-1}[\alpha[u'] \ominus v' \oplus \alpha(e)]$, $v = \beta^{-1}[\alpha^{-1}[v'] \ominus \alpha(e)]$ *and* $\varrho_v^{-1}(u) = \alpha^{-1}(u' - \alpha^{-1}[v'] + \alpha(e))$.

(6) *There exists* $u' \in W(X)$ *such that* $u = \alpha^{-1}[\alpha[u'] \oplus \alpha(e) \ominus \alpha[\alpha(e) + \beta(v)]]$ *and* $\varrho_v^{-1}(u) = \alpha^{-1}(u' - \beta(v))$.

P r o o f. Suppose first $\beta(v) = 0$. Lemma 4.1 (ii) gives $\varrho_v^{-1}(u) = \alpha^{-2}(\alpha^2(e) + \alpha(u) - \alpha(e))$, and if there exists no $u_1 \in W(X)$ with $u = \alpha^{-1}[u_1]$, then $\alpha^2(e) \oplus \alpha[u] \ominus \alpha(e) \in W(X)$, as $u \neq e$. However, that leads to $d(\varrho_v^{-1}(u)) > d(u)$, and so the existence of the considered $u_1 \in W(X)$ can be assumed. Now, $\alpha^2(e) + u_1 - \alpha(e)$ is of the form $\alpha[u']$ if and only if $u_1 = \alpha[u'] \oplus \alpha(e) \ominus \alpha^2(e)$ for some $u' \in W(X)$, and this yields a special case of (6). Assume $\alpha^{-1}[\alpha^2(e) + u_1 - \alpha(e)] \in W(X)$. To avoid $d(\varrho_v^{-1}(u)) > d(u)$ we must have $d(u_1) > d(\alpha^2(e) + u_1 - \alpha(e))$, which stipulates the existence of $u' \in W(X)$ with $u_1 = u' - \alpha^2(e)$ and $d(u') \leqslant 1$. We have obtained a special case of the alternative (4), and we can assume $\beta(v) \neq 0$ for the rest of the proof.

As in the proof of Lemma 4.2 we shall distinguish between the general e-case when $\alpha[\beta(v) + \alpha(e)] \in W(X)$, and the exceptional e-case when there exists $v' \in W(X)$ with $v = \beta^{-1}[\alpha^{-1}[v'] \ominus \alpha(e)]$. Recall that $v \neq e \setminus e$ is equivalent to $e \neq \alpha(e) + \beta(v)$.

Consider first the general e-case, and put $w = \alpha[\alpha(e) + \beta(v)] + \alpha(u) - \alpha(e)$. If $\alpha^{-1}[w] \notin W(X)$, then there clearly must exist $u' \in W(X)$ with $u = \alpha^{-1}[\alpha^{-1}[u'] \oplus \alpha(e) \ominus \alpha[\alpha(e) + \beta(v)]]$, which gives the alternative (6). Hence $\alpha^{-1}[w] \in W(X)$ can be assumed.

From the proof of Lemma 4.2 we can also use the observation that $d(\alpha[\beta(v) + \alpha(e)]) \geqslant d(v)$, with the exception of the situation when there exists $v_1 \in W(X)$ with $d(v_1) = 0$ and $v = \beta^{-1}[v_1 - \alpha(e)]$.

Let us consider this situation. Then $v_1 \neq e$, $u \neq e$, $w = \alpha[v_1] + \alpha(u) - \alpha(e)$ and $\varrho_v^{-1}(u) = \alpha^{-1}[\alpha^{-1}[w] - v_1 + \alpha(e)]$. If $d(\alpha(u)) \geqslant 2$ or $d(\alpha(u)) = 0$, then clearly $d(\varrho_v^{-1}(u)) > d(u)$. Since $d(\varrho_v^{-1}(u)) = 3$ when $d(u) = 0$, there must exist $u_1 \in W(X)$ with $d(u_1) = 1$ and $u = \alpha^{-1}[u_1]$. Thus $d(u) = 2$, and since $d(\varrho_v^{-1}(u)) \geqslant 3$ when $d(w) \geqslant 1$, there must be $d(w) = 0$. Hence $u_1 = u' - \alpha(v') + \alpha(e)$ for some $u' \in W(X)$ with $d(u') = 0$. We have obtained the alternative (2).

Let us continue in the investigation of the general e-case. We can now assume $d(\alpha[\alpha(e) + \beta(v)]) \geqslant d(v)$. The inequality $d(\alpha[\alpha(e) + \beta(v)]) \geqslant d(\beta(v)) + 1$ is obvious when $\beta[v] \in W(X)$, and in the case $\beta[v] \notin W(X)$ we get it from $d(\alpha[\alpha(e) + \beta(v)]) \geqslant d(v)$. We have $\alpha[\alpha(e)+\beta(v)] \oplus \alpha(e) \in W(X)$, and the depth of the latter element is the same as the depth of $\alpha[\alpha(e)+\beta(v)]$. If that depth exceeds $d(\alpha(u))$, then the depth of $\varrho_v^{-1}(u) = \alpha^{-1}(\alpha^{-1}[w] - \beta(v))$ exceeds $d(u) \leqslant d(\alpha(u)) + 1$. Similarly, $d(u) > d(\varrho_v^{-1}(u))$ when $d(\alpha(u)) > d(\alpha[\alpha(e)+\beta(v)])$. Hence $d(\alpha(u)) = d(\alpha[\alpha(e)+\beta(v)])$. Furthermore, $d(\alpha(u)) = d(w)$ implies $d(\varrho_v^{-1}(u)) = d(\alpha(u)) + 2 > d(u)$ (there is $d(w) > d(\beta(v))$), and so there must exist $u' \in W(X)$ such that $u = \alpha^{-1}[u' - \alpha[\alpha(e)+\beta(v)]]$ and $d(w) = d(u' - \alpha(e)) < d(\alpha(u)) = d[\alpha(e) + \beta(v)] + 1$. Hence $d(u' - \alpha(e)) \leqslant d(\alpha(e) + \beta(v))$, and to get the alternative (4) it suffices to verify $d(\alpha(e)+\beta(v)) \geqslant d(u')$. This is clear when $d(\alpha(e) + \beta(v)) \geqslant 1$. Above we have proved that $d(\alpha(e) + \beta(v)) \geqslant d(\beta(v))$, and so $d(\alpha(e) + \beta(v)) \geqslant 1$ holds both for $d(\beta(v)) > 0$ and $d(\beta(v)) = 0$.

Let us now turn to the exceptional e-case. Then $v = \beta^{-1}[\alpha^{-1}[v'] \ominus \alpha(e)]$ and $\varrho_v^{-1}(u) = \alpha^{-1}(\alpha^{-1}(v' + \alpha(u) - \alpha(e)) - \alpha^{-1}[v'] + \alpha(e))$. Consider first the case $\alpha^{-1}[v' + \alpha(u) - \alpha(e)] \in W(X)$. From $u \neq e$ we get $\alpha^{-1}[v' + \alpha(u) - \alpha(e)] \neq \alpha^{-1}[v']$, and thus in this case $\varrho_v^{-1}(u) = \alpha^{-1}[\alpha^{-1}[v' + \alpha(u) - \alpha(e)] \ominus \alpha^{-1}[v'] \oplus \alpha(e)]$. If $d(\alpha(u)) > d(v' - \alpha(e))$ or if $d(\alpha(u)) \leqslant d(v')$, then clearly $d(\varrho_v^{-1}(u)) > d(u)$. Suppose $d(\alpha(u)) > d(v')$ and $d(\alpha(u)) \leqslant d(v' - \alpha(e))$. Then $d(v' - \alpha(e)) > d(v')$, which gives $d(v') = 0$ and $d(\alpha(u)) \leqslant 1$. There is clearly $d(u) \neq 0$, and $d(\alpha(u)) = 0$ leads to $d(u) = 1 < 3 = d(\varrho_v^{-1}(u))$. Thus $d(u) = d(\alpha(u)) + 1 = 2$, and there must be $d(\alpha(u) - \alpha(e)) = 0$, as otherwise we would get $d(\varrho_v^{-1}(u)) = 3$ again. Hence there must exist $u' \in W(X)$ with $d(u') = 0$ and $u = \alpha^{-1}[u' + \alpha(e)]$. This is the alternative (1).

It remains to assume $\alpha^{-1}[v' + \alpha(u) - \alpha(e)] \notin W(X)$, and then $v' + \alpha(u) - \alpha(e) = \alpha[w]$ for some $w \in W(X)$. Since $\alpha(u) \neq \alpha(e)$ and $v' \neq \alpha(e)$, $\alpha[w]$ has to be an additive factor of $\alpha(u)$ or of v'. Assume first the latter case. Then $v' = \alpha[w] \oplus (\alpha(e) - \alpha(u))$, $v = \beta^{-1}[\alpha^{-1}[\alpha[w] \oplus (\alpha(e) - \alpha(u))] \ominus \alpha(e)]$, and $\varrho_v^{-1}(u) = \alpha^{-1}[(w + \alpha(e)) \ominus \alpha^{-1}[\alpha[w] \oplus (\alpha(e) - \alpha(u))]]$. If $d(\alpha(e) - \alpha(u)) \geqslant d(\alpha(u))$, then $d(\varrho_v^{-1}(u)) \geqslant 2 + d(\alpha(u)) > d(u)$. Hence $d(\alpha(u)) \leqslant 1$, and $d(u) \leqslant 2$. Since $d(\varrho_v^{-1}(u))$ is clearly at least 3, we see that $\alpha[w]$ cannot be an additive factor of v'.

Hence it is an additive factor of $\alpha(u)$, and so $u = \alpha^{-1}[\alpha[w] \oplus (\alpha(e) - v')]$ and $\varrho_v^{-1}(u) = \alpha^{-1}(w - \alpha^{-1}[v'] + \alpha(e))$. Let us assume $d(v') > d(w)$. Then $d(u) = d(v') + 1$, and $d(\varrho_v^{-1}(u)) = 2 + d(v')$. Thus $d(v') > d(w)$ leads to $d(\varrho_v^{-1}(u)) > d(u)$, and $d(v') \leqslant d(w)$ can be assumed. Setting $u' = w$ we obtain the alternative (3) when $d(w) = 0$, and the alternative (5) when $d(w) \geqslant 1$. These cases are set apart as different alternatives since they yield different kinds of α-leading parts.

By analyzing all steps of the proof we can verify that no two alternatives can hold simultaneously. However, rather than analysing the proof it seems more efficient to use the following Corollary 4.5 which classifies α-leading parts. It is clear from the corollary that no two of the alternatives (1)–(5) can be satisfied at the same time. Thus one has to compare just the alternative (6) with the other alternatives, and it is easy to see that they are never compatible. □

Corollary 4.5. *In the situation of Lemma* 4.4 *there always exists* $w \in W(X)$ *such that* $u = \alpha^{-1}[w]$. *The α-leading part of u is equal, in the alternatives* (1)–(5), *to* (1) $\alpha(e)$, (2) $\alpha(e) \ominus \alpha(v')$, (3) $\alpha(e) \oplus \alpha(u')$, (4) $-\alpha[\alpha(e) + \beta(v)]$ *and* (5) $\alpha[u']$, *respectively. Furthermore,* $d(\alpha(u)) = 1$ *in the alternatives* (1)–(3), *and* $d(\alpha(u)) > 1$ *in the alternatives* (4)–(5).

5. Depth changes and fixed-point translations

Our goal is to show that the group $H = \langle \lambda_v, \varrho_v;\, v \in W(X)\rangle$ acts semiregularly on $W(X) \setminus \{e\}$. The general idea of the proof has been sketched in the paragraph after Lemma 4.1. The rest of Section 4 was devoted to the description of the cases when $d(\varrho_v^{\pm 1}(u)) \leqslant d(u)$, $v \neq e \setminus e$. By symmetry, in this way we also get a description of the cases with $d(\lambda_v^{\pm 1}(u)) \leqslant d(u)$, $v \neq e \setminus e$. In this section we shall not prove the semiregularity of H yet. Nevertheless, this and the preceding section contain all situations that require a detailed case-by-case investigation.

The main results of this section are concerned with the mappings $R_{e\setminus e}^{\pm 1}$ and $L_{e/e}^{\pm 1}$. If γ is such a mapping, and $d(\gamma(u)) \leqslant d(u)$ for some $u \in W(X)$, then the depths of $\varrho_v^{\pm 1}(\gamma(u))$, $v \neq e \setminus e$, and $\lambda_v^{\pm 1}(\gamma(u))$, $v \neq e/e$, will also become relevant. The first two lemmas prepare ground for such considerations.

Lemma 5.1. *Let* $u \in W(X)$ *be such that* $\alpha[u] \in W(X)$ *and* $u \neq e$. *Then* $d(\varrho_v(u)) \geqslant 3 + d(u)$ *for every* $v \in W(X)$, $v \neq e \setminus e$.

P r o o f. Use Lemma 4.1 (i) to express $\varrho_v(u)$. If $\alpha[\beta(v) + \alpha(e)] \notin W(X)$, then $v = \beta^{-1}[\alpha^{-1}[v'] - \alpha(e)]$ for some $v' \in W(X)$, $\varrho_v(u) = \alpha^{-1}[\alpha[\alpha^{-1}[v'] \ominus \alpha(e) \oplus \alpha[u]] \oplus (\alpha(e) - v')]$ and $d(\varrho_v(u)) \geqslant d(u) + 3$. Hence $\alpha[\beta(v) + \alpha(e)] \in W(X)$ can be assumed for the rest of the proof.

If $\alpha[\beta(v)+\alpha(u)] \in W(X)$, then $\varrho_v(u) = \alpha^{-1}[\alpha[\beta(v)+\alpha[u]]\ominus\alpha[\beta(v)+\alpha(e)]\oplus\alpha(e)]$, by $u \neq e$ and $v \neq e \setminus e$. Thus $d(\varrho_v(u)) \geqslant d(u) + 3$ when $\beta(v) \oplus \alpha[u] \in W(X)$ or $\beta(v) = 0$. If none of these two cases holds, then $v = \beta^{-1}[v' \ominus \alpha[u]]$, where $\alpha[v'] \in W(X)$. We get $\varrho_v(u) = \alpha^{-1}(\alpha[v'] - \alpha[v' + \alpha(e) - \alpha[u]] + \alpha[e])$. Now, there is $v' \neq v' + \alpha(e) - \alpha(u)$, by $u \neq e$, and $-\alpha[u]$ is a basic factor of $v' + \alpha(e) - \alpha[u]$, by $v' \ominus \alpha[u] \in W(X)$ and $u \neq e$. Hence $d(\varrho_v(u)) \geqslant 3 + d(u)$ again.

Finally, suppose $\alpha[\beta(v) + \alpha[u]] \notin W(X)$. Then $\beta(v) = \alpha^{-1}[v'] \ominus \alpha[u]$ for some $v' \in W(X)$, and $\varrho_v(u) = \alpha^{-1}(v' - \alpha[\alpha^{-1}[v']\ominus\alpha[u]\oplus\alpha(e)]+\alpha(e))$, as $u \neq e$. Therefore $d(\varrho_v(u)) \geqslant 3 + d(u)$ in this case as well. □

Lemma 5.2. *Let $u \in W(X)$ be such that $\alpha[u] \in W(X)$ and $u \neq e$. Then $d(\varrho_v^{-1}(u)) \geqslant 3 + d(u)$ for every $v \in W(X)$, $v \neq e \setminus e$.*

Proof. Use Lemma 4.1 (ii) to express $\varrho_v^{-1}(u)$. If $\alpha[\beta(v) + \alpha(e)] \notin W(X)$, then $v = \beta^{-1}[\alpha^{-1}[v'] - \alpha(e)]$, $\varrho_v^{-1}(u) = \alpha^{-1}(\alpha^{-1}(v' - \alpha[e] + \alpha[u]) - \alpha^{-1}[v'] + \alpha(e))$, and $d(\varrho_v^{-1}(u)) \geqslant d(u) + 3$ follows from $u \neq e$ and from the following analysis: If $\alpha^{-1}[v' - \alpha(e) + \alpha[u]] \in W(X)$, then $\pm\alpha[u]$ appears as a basic factor of v' or of $v' - \alpha(e) + \alpha[u]$. If $\alpha^{-1}[v' - \alpha(e) + \alpha[u]] \notin W(X)$, then $v' = \alpha(e) \ominus \alpha[u] \oplus \alpha[v_1]$ for some $v_1 \in W(X)$, and $\varrho_v^{-1}(u) = \alpha^{-1}[(v_1 + \alpha(e)) - \alpha^{-1}[\alpha(e) \ominus \alpha[u] \oplus \alpha[v_1]]]$.

Assume $\alpha[\beta(v) + \alpha(e)] \in W(X)$. Then $\varrho_v^{-1}(u) = \alpha^{-1}(\alpha^{-1}(w) - \beta(v))$, where $w = \alpha[\beta(v) + \alpha(e)] - \alpha(e) + \alpha[u]$. From $u \neq e$ and $v \neq e \setminus e = \beta^{-1}(e - \alpha(e))$ we obtain $w = \alpha[\beta(v) + \alpha(e)] \ominus \alpha(e) \oplus \alpha[u]$, and hence $\alpha^{-1}[w] \in W(X)$.

If $d(\beta(v)) \geqslant 2$ or $d(\beta(v)) = 0$, then $d(\beta(v) + \alpha(e)) \geqslant d(\beta(v))$, and thus $d(w) \geqslant d(\beta(v))$ in all cases. Therefore $\varrho_v^{-1}(u) = \alpha^{-1}[\alpha^{-1}[w]\ominus\beta(v)]$ or $\varrho_v^{-1}(u) = \alpha^{-1}[\alpha^{-1}[w]]$, and $d(\varrho_v^{-1}(u)) \geqslant d(u) + 3$ is always true. □

Lemma 5.3. *Let $u \neq e$ be an element of $W(X)$. Then:*

(i) *$R_{e\setminus e}(u) = u\circ(e\setminus e) = \alpha(u)-\alpha(e)+e$, $d(u\circ(e\setminus e)) \geqslant d(u)-2$, and $d(u\circ(e\setminus e)) \leqslant d(u)$ if and only if $u = \alpha^{-1}[u_1]$ for some $u_1 \in W(X)$;*

(ii) *$R_{e\setminus e}^{-1}(u) = u/(e\setminus e) = \alpha^{-1}(u+\alpha(e)-e)$, $d(u/(e\setminus e)) \geqslant d(u)-2$ and $d(u/(e\setminus e)) \leqslant d(u)$ if and only if either*

   (a) *$u = u' - \alpha(e)$ for some $u' \in W(X)$, $d(u') = 0$, or*

   (b) *$u = \alpha[u_1] \ominus \alpha(e) \oplus e$ for some $u_1 \in W(X)$, $u_1 \neq e$;*

(iii) *$L_{e/e}(u) = (e/e)\circ u = \beta(u) - \beta(e) + e$, $d((e/e)\circ u) \geqslant d(u) - 2$ and $d((e/e)\circ u) \leqslant d(u)$ if and only if $u = \beta^{-1}[u_1]$ for some $u_1 \in W(X)$; and*

(iv) *$L_{e/e}^{-1}(u) = (e/e)\setminus u = \beta^{-1}(u+\beta(e)-e)$, $d((e/e)\setminus u) \geqslant d(u)-2$ and $d((e/e)\setminus u) \leqslant d(u)$ if and only if either*

   (a) *$u = u' - \beta(e)$ for some $u' \in W(X)$, $d(u') = 0$, or*

   (b) *$u = \beta[u_1] \ominus \beta(e) \oplus e$ for some $u_1 \in W(X)$, $u_1 \neq e$.*

P r o o f. It suffices to prove just (i) and (ii), since (iii) and (iv) then follow by symmetry. The expressions of $u \circ (e \setminus e)$ and $u/(e \setminus e)$ are clear. There is $u \neq e$, and hence $\alpha[u] \in W(X)$ implies $d(\alpha(u) + e - \alpha(e)) > d(u)$. If $u = \alpha^{-1}[u_1]$, then $d(u_1 + e - \alpha(e)) = d(u) - 1$ when $d(u) \geqslant 3$, and $2 \geqslant d(u)$ trivially implies $d(u_1 + e - \alpha(e)) \geqslant d(u) - 2$. The rest of (i) is clear.

Suppose now $d(\alpha^{-1}(u - e + \alpha(e))) \leqslant d(u)$. If $\alpha^{-1}[u - e + \alpha(e)] \in W(X)$, then there clearly exists $u' \in W(X)$ with $d(u') = 0$ and $u = u' - \alpha(e)$. In such a case $d(\alpha^{-1}(u - e + \alpha(e))) = d(u) = 1$.

Assume $\alpha^{-1}[u-e+\alpha(e)] \notin W(X)$. Then $u = \alpha[u_1] \oplus e \ominus \alpha(e)$ for some $u_1 \in W(X)$, $u_1 \neq e$. We have $d(u_1) = d(u)-1$ when $d(u) \geqslant 3$, and $d(u_1) \geqslant d(u)-2$ when $d(u) \leqslant 2$. □

Lemma 5.4. *Assume $\varphi, \psi \in \{L_{e/e}^{\pm 1}, R_{e\setminus e}^{\pm 1}\}$, and suppose that $d(\varphi(u)) \leqslant d(u)$ and $d(\psi(u)) \leqslant d(u)$ for some $u \in W(X)$, $u \neq e$. Then $\varphi = \psi$.*

P r o o f. Consider cases (i)–(iv) of Lemma 5.3. Case (i) does not match any of cases (ii)–(iv), and a similar fact holds for case (iii), too. Cases (ii) and (iv) cannot hold imultaneously as well, and the element u' (or u_1) can be derived from u in each of the cases in a unique way. □

Lemma 5.5. *Suppose that $u \in W(X)$, $u \neq e$, $\varphi \in \{L_{e/e}^{\pm 1}, R_{e\setminus e}^{\pm 1}\}$ and $\psi \in \{\lambda_v^{\pm 1}, \varrho_v^{\pm 1};\ v \in W(X)\} \setminus \{L_{e/e}^{\pm 1}, R_{e\setminus e}^{\pm 1}\}$ are such that $d(\varphi(u)) \leqslant d(u)$ and $d(\psi(u)) \leqslant d(u)$. Then there exists $u_1 \in W(X)$ such that either*
(a) *$u = \alpha^{-1}[u_1]$, $\varphi = R_{e\setminus e}$ and $\psi = \varrho_v^{\pm 1}$, $v \in W(X) \setminus \{e \setminus e\}$; or*
(b) *$u = \beta^{-1}[u_1]$, $\varphi = L_{e/e}$ and $\psi = \lambda_v^{\pm 1}$, $v \in W(X) \setminus \{e/e\}$.*

P r o o f. If $\psi = \varrho_v^{\pm 1}$, $v \neq e \setminus e$, then $u = \alpha^{-1}[u_1]$ for some $u_1 \in W(X)$, by Corollaries 4.3 and 4.5. For the rest apply Lemma 5.3 and use the symmetry. □

Lemma 5.6. *For $u, v, w \in W(X)$ assume that $u \neq e$, $v \neq e \setminus e$, $\psi = \varrho_v^{\pm 1}$, and that either $\varphi = \lambda_w^{\pm 1}$, $w \neq e/e$, or $\varphi = \varrho_w^{\pm 1}$, $w \neq e \setminus e$. If*

$$d(u) \geqslant \max\{d(\psi(u)), d(u \circ (e \setminus e)), d(\varphi(u \circ (e \setminus e)))\},$$

then $\varphi = R_{e\setminus e}^{\pm 1}$ or $\varphi = L_{e/e}^{\pm 1}$.

P r o o f. First note that $u = \alpha^{-1}[u_1]$ for some $u_1 \in W(X)$, by Lemma 5.3 (i), and that $u \circ (e \setminus e) = u_1 - \alpha(e) + e$. Part (i) of Lemma 5.3 also yields $d(u_1 - \alpha(e) + e) \geqslant d(u_1) - 1$, and we shall observe that it will be enough to show $\alpha[u_1 - \alpha(e) + e] \in W(X)$ and $\beta[u_1 - \alpha(e) + e] \in W(X)$. Indeed, the former incidence covers the case $\varphi = \varrho_w^{\pm 1}$, $w \in W(X)$, as Lemmas 5.1 and 5.2 imply $d(\varphi(u \circ (e \setminus e))) \geqslant 3 + d(u_1) - 1 = d(u) + 1$, while the case $\varphi = \lambda_w^{\pm 1}$, $w \in W(X) \setminus \{e\}$, follows in a similar way from statements that are symmetric to these two lemmas.

To prove $\alpha[u_1 - \alpha(e) + e] \in W(X)$ and $\beta[u_1 - \alpha(e) + e] \in W(X)$ we need to investigate just the cases when $u_1 - \alpha(e) + e$ has exactly one base factor. We can use, furthermore, the assumption $d(\psi(u)) \leqslant u$ to restrict our investigation of the structure of $u_1 = \alpha[u]$ just to the cases described in Lemmas 4.2 and 4.4.

If $\psi = \varrho_v$, then Lemma 4.2 applies, and we see that $u_1 - \alpha(e) + e$ is equal to (1) $-u' + e$, (2) $\alpha^{-1}[u'] - v' + e$, (3) $-\alpha^{-1}[v'] + u' + e$, (4) $\alpha^{-1}[u'] - \beta(v) + \alpha(e) + e$, (5) $-\alpha^{-1}[v'] + u' - \alpha(e) + e$, and (6) $\alpha^{-1}[u'] \ominus \alpha^{-1}[v'] \oplus e$, respectively. Case (6) is clear, and the facts (1) $d(-u' + e) = 0$, (2) $v' \neq e$ and $d(\alpha^{-1}[u']) > d(v' + e)$, (3) $d(-\alpha^{-1}[v']) > d(u' + e)$, (4) $d(\alpha^{-1}[u']) > d(\beta(v))$, and (5) $d(-\alpha^{-1}[v']) > d(u')$ can be used, respectively, to see that both $\alpha[u_1 - \alpha(e) + e]$ and $\beta[u_1 - \alpha(e) + e]$ belong to $W(X)$.

Suppose now $\psi = \varrho_v^{-1}$ and consider Lemma 4.4. Then $u_1 - \alpha(e) + e$ equals (1) $u' + e$, (2) $-\alpha[v'] + u' - e$, (3) $\alpha[u'] - v' + e$, (4) $u' - \alpha[\alpha(e) + \beta(v)] - \alpha(e) + e$, (5) $\alpha[u'] + v' + e$, and (6) $\alpha[u'] \ominus \alpha[\alpha(e) + \beta(v)] \oplus e$, respectively. Case (6) is clear again, and the other cases follow from (1) $d(u' + e) = 0$, (2) $d(-\alpha^{-1}[v']) > d(u' - e)$, (3) $d(\alpha[u']) > d(e - v')$, (4) $d(-\alpha[\alpha(e) + \beta(v)]) > d(u')$, and (5) $d(\alpha[u']) > d(e - v')$, respectively. □

Lemma 5.7. *Consider $u \in W(X)$, $u \neq e$, $\varphi \in \{L_{e/e}^{-1}, L_{e/e}, R_{e\setminus e}\}$ and $\varphi', \varphi'' \in \{\varrho_t^{\pm 1}, \lambda_t^{\pm 1};\ t \in W(X)\}$. Let $\psi = \varrho_v^{\pm 1}$, $v \in W(X) \setminus \{e \setminus e\}$, be such that $d(u) \geqslant \max\{d(\psi(u)), d(u \circ (e \setminus e)), d(\varphi(u \circ (e \setminus e))), d(\varphi'\varphi(u \circ (e \setminus e))), d(\varphi''\varphi'\varphi(u \circ (e \setminus e)))\}$. Suppose also $\varphi' \neq \varphi^{-1}$ and $\varphi'' \neq (\varphi')^{-1}$. Then $\varphi = L_{e/e}^{-1}$ and there exists $w \in W(X)$ such that $d(w + \alpha(e)) = d(w + \beta(e))$, $u = \alpha^{-1}[w + \alpha(e)]$ and $(e/e) \setminus (u \circ (e/e)) = \beta^{-1}[w + \beta(e)]$.*

P r o f. From $d(\psi(u)) \leqslant d(u)$ we get the existence of such $u_1 \in W(X)$ that $u = \alpha^{-1}[u_1]$, by Corollaries 4.3 and 4.5. Hence $u \circ (e/e) = u_1 - \alpha(e) + e$.

Let us start with the cases $\varphi = R_{e\setminus e}$ and $\varphi = L_{e/e}$. Put $\gamma = \alpha$ if $\varphi = R_{e\setminus e}$, and $\gamma = \beta$ if $\varphi = L_{e/e}$. Then $\varphi(u \circ (e/e)) = \gamma(u_1 - \alpha(e) + e) - \gamma(e) + e$. Suppose first $\gamma[u_1 - \alpha(e) + e] \in W(X)$. This means $\varphi(u \circ (e/e)) = \gamma[u_1 - \alpha(e) + e] \ominus \gamma(e) \oplus e$, as $u_1 \neq \alpha(e)$. If $d(u_1 - \alpha(e) + e) \geqslant d(u_1)$, then $d(\varphi(u \circ (e/e))) = d(u)$ and $d(u \circ (e/e)) \geqslant \max\{d(\varphi^{-1}(\varphi(u \circ (e/e)))), d(\varphi'(\varphi(u \circ (e/e))))\}$. However, this is not possible if $\varphi' \notin \{L_{e/e}^{\pm 1}, R_{e\setminus e}^{\pm 1}\}$, as $\varphi(u \circ (e/e))$ is not of the form $\alpha^{-1}[u_2]$ or $\beta^{-1}[u_2]$, $u_2 \in W(X)$, by Corollaries 4.3 and 4.5 and by their corresponding left-right symmetric versions. But there cannot be $\varphi' \in \{L_{e/e}^{\pm 1}, R_{e\setminus e}^{\pm 1}\}$ either, by Lemma 5.4. Hence $d(u_1 - \alpha(e) + e) < d(u_1)$, which implies $u_1 = u' + \alpha(e)$, where $u' \in W(X)$, $d(u') = 0$ and $u' \neq 0$. Then $d(u) = 2$, $\varphi(u \circ (e/e)) = \gamma[u' + e] \ominus \gamma(e) \oplus e$, $d(\varphi(u \circ (e/e))) = 1$, and Lemmas 5.1

and 5.2 (together with their left-right symmetric versions) yield $\varphi' \in \{L_{e/e}^{\pm 1}, R_{e\setminus e}^{\pm 1}\}$, as otherwise we would get $d(\varphi'\varphi(u \circ (e/e))) \geqslant 4$.

If $\varphi' \in \{L_{e/e}, R_{e\setminus e}\}$, then set $\gamma' = \beta$ when $\varphi' = L_{e/e}$ and $\gamma' = \alpha$ when $\varphi' = R_{e\setminus e}$. We obtain $\varphi'\varphi(u \circ (e/e)) = \gamma'[\gamma[u_1 + e] \ominus \gamma(e) \oplus e] \ominus \gamma'(e) \oplus e$, and hence $d(\varphi'\varphi(u \circ (e/e))) = 2 = d(u)$. There is either $\varphi'' \notin \{L_{e/e}^{\pm 1}, R_{e\setminus e}^{\pm 1}\}$, or $\varphi'' \in \{L_{e/e}^{\pm 1}, R_{e\setminus e}^{\pm 1}\}$, but both cases can be excluded by the same argument as in the preceding paragraph.

If $\varphi' \in \{L_{e/e}^{-1}, R_{e\setminus e}^{-1}\}$, then choose $\gamma' \in \{\alpha, \beta\}$ in such a way that $\gamma' \neq \gamma$. There is $\varphi' \neq \varphi^{-1}$, and hence $\varphi'\varphi(u \circ (e/e)) = (\gamma')^{-1}[\gamma[u' + e] \ominus \gamma(e) \oplus \gamma'(e)]$ and $d(\varphi'(u \circ (e/e))) = 2 = d(u)$. The case $\varphi'' \in \{L_{e/e}^{\pm 1}, R_{e\setminus e}^{\pm 1}\}$ is again blocked by Lemma 5.4. Assume $\varphi'' \notin \{L_{e/e}^{\pm 1}, R_{e\setminus e}^{\pm}\}$ and from the two symmetric situations choose the one with $\gamma' = \alpha$ and $\gamma = \beta$. Then $\varphi = \varrho_w^{\pm 1}$ for some $w \in W(X)$, $w \neq e \setminus e$, by the symmetric versions of Corollaries 4.3 and 4.5. These corollaries describe the structure of the α-leading part of cases (1)–(5), respectively, and we see that $\varphi'\varphi(u \circ (e/e))$ fits none of the corresponding descriptions. Since it does not correspond to the case (6) of Lemmas 4.2 or 4.4 as well, we can conclude by observing that we never have $\gamma[u_1 - \alpha(e) + e] \in W(X)$.

Hence $u_1 = \gamma^{-1}[u'] \oplus \alpha(e) \ominus e$ for some $u' \in W(X)$, and the α-leading part of u equals $\gamma^{-1}[u']$ or $\gamma^{-1}[u'] \oplus \alpha(e)$. Therefore $\gamma = \alpha$, by Corollaries 4.3 and 4.5. Suppose first $\psi = \varrho_v$, $v = W(X) \setminus \{e \setminus e\}$. The possible forms of the α-leading part point to cases (2), (4) and (6) of Lemma 4.2. By inspecting these cases we immediately see that cases (2) and (6) do not match our situation. If fact, this is also true for case (4), as $\beta(v) = -\alpha(e) + e$ just when $v = e \setminus e$.

If $\psi = \varrho_v^{-1}$, $v \in W(X) \setminus \{e \setminus e\}$, then Corollary 4.5 excludes all cases of Lemma 4.4, but case (6). Since that case does not match our situation as well, we see that we can turn to the case $\varphi = L_{e/e}^{-1}$.

We have $L_{e/e}^{-1} R_{e\setminus e}(u) = L_{e/e}^{-1} R_{e\setminus e}(\alpha^{-1}[u_1]) = \beta^{-1}(u_1 - \alpha(e) + \beta(e))$. Assume first $\beta^{-1}[u_1 - \alpha(e) + \beta(e)] \notin W(X)$. Then $u_1 = \beta[u'] \oplus \alpha(e) \ominus \beta(e)$, which clearly does not match any of the situations in Lemmas 4.2 and 4.4. Since some matching is necessary, as $\psi = R_v^{\pm 1}$, we see that $\beta^{-1}[u_1 - \alpha(e) + \beta(e)] \in W(X)$. There cannot be $d(u_1) = 0$, as in such a case there would be $2 = d((e/e) \setminus (u \circ (e \setminus e))) > d(u) = 1$. If $d(u_1 - \alpha(e) + \beta(e)) = 0$, then $u_1 = u' \oplus \alpha(e) \ominus \beta(e)$ for some $u' \in W(X)$, $d(u') = 0$, and this again causes a mismatch with every case of Lemmas 4.2 and 4.4. Therefore the depths of both u_1 and $u_1 - \alpha(e) + \beta(e)$ are positive, and they equal each other. Conclude by setting $w = u_1 - \alpha(e)$. □

We first turn to situations when $\varphi, \psi \in \{\varrho_v^{\pm 1};\ v \in W(X),\ v \neq e \setminus e\}$, $d(\varphi(u)) \leqslant d(u)$ and $d(\psi(u)) \leqslant d(u)$. We shall observe that then nearly always $\varphi = \psi$.

Lemma 6.1. *Suppose that $\varphi = \varrho_v$ and $\psi = \varrho_w$ for some $v, w \in W(X) \setminus \{e/e\}$. Suppose, furthermore, that there exists $u \in W(X)$ such that $d(\varphi(u)) \leqslant d(u)$ and $d(\psi(u)) \leqslant d(u)$. If $\varphi \neq \psi$ then there exist $u', v', w' \in W(X)$ of depth 0 such that $u' \neq 0$, $u = \alpha^{-1}(\alpha(e) + u')$, $v = \beta^{-1}(v' - \alpha(e))$ and $w = \beta^{-1}(w' - \alpha(e))$.*

P r o o f. Lemma 4.2 gives six situations under which $d(\varphi(u)) \leqslant d(u)$ can hold. The number (1)–(6) of the situation will be referred to as the cause of depression of φ at u. The structure of the α-leading part of u, as exhibited in Corollary 4.3, makes it clear that if the cause of depression of φ at u differs from that of ψ at u, then one of them has to equal (6). Let it be the case of ψ. Hence $u = \alpha^{-1}[\alpha^{-1}[u_1] \ominus \alpha^{-1}[w'] \oplus \alpha(e)]$ and $w = \beta^{-1}[\alpha^{-1}[w'] \ominus \alpha(e)]$, for some $u_1, w' \in W(X)$. The structure of u, as implied by (6), makes it impossible for φ to have causes (1)–(3). If (4) is the cause, then $u' = u_1$ and $\beta(v) = \alpha^{-1}[w'] \ominus \alpha(e)$, which yields $\alpha[\alpha(e) + \beta(v)] \notin W(X)$, a contradiction with one of the assumptions of (4). If (5) is the cause, then there must be $v' = w'$, which implies $\beta(v) = \beta(w)$ and $\alpha[\alpha(u) + \beta(v)] \notin W(X)$, a contradiction with one of the assumptions of (5).

Therefore we know that there is the same cause of depression at u for both φ and ψ. If the cause equals (6), then $\varphi = \psi$ follows immediately from the expression of u in Lemma 4.2. In cases (3) and (5) we can read v and w from the α-leading part of u, which leads to $v = w$ and $\varphi = \psi$ as well. Cases (2) and (4) are similar, since they allow a unique determination of $v = w$ from $\alpha(u) - u_0$, where u_0 is the α-leading part of u.

This finishes the proof, since case (1) corresponds to the situation described in this lemma. □

Lemma 6.2. *Suppose that $\varphi = \varrho_v^{-1}$ and $\psi = \varrho_w^{-1}$ for some $v, w \in W(X) \setminus \{e/e\}$. Suppose, furthermore, that there exists $u \in W(X)$ such that $d(\varphi(u)) \leqslant d(u)$ and $d(\psi(u)) \leqslant d(u)$. If $\varphi \neq \psi$ then there exist $u', v', w' \in W(X)$ of depth 0 such that $u' \neq 0$, $u = \alpha^{-1}(\alpha(e) + u')$, $v = \beta^{-1}(v' - \alpha(e))$ and $w = \beta^{-1}(w' - \alpha(e))$.*

P r o o f. Let us speak again about the cause of depression of φ (or ψ) at u (but this time with respect to Lemma 4.4). Proceeding similarly as in Lemma 6.1, first verify that if (6) is the cause with respect to φ, then it also has to be the cause with respect to ψ. Corollary 4.5 then shows, by considering the structure of the α-leading part of u, that there is only one common cause of the depression at u for both φ

and ψ. This is straightforward, and the last step, namely showing that v is uniquely determined by each of the causes (2)–(6), is straightforward as well, like in the proof of Lemma 6.1. The rest is clear. $\square$

Lemma 6.3. *Suppose that $\varphi = \varrho_v^{-1}$ and $\psi = \varrho_w$ for some $v, w \in W(X) \setminus \{e/e\}$. Suppose, furthermore, that there exists $u \in W(X)$ such that $d(\varphi(u)) \leqslant d(u)$ and $d(\psi(u)) \leqslant d(u)$. If $\varphi \neq \psi$ then there exist $u', v', w' \in W(X)$ of depth 0 such that $u' \neq 0$, $u = \alpha^{-1}(\alpha(e) + u')$, $v = \beta^{-1}(\alpha^{-1}(v') - \alpha(e))$ and $w = \beta^{-1}(w' - \alpha(e))$.*

Proof. From the proofs of Lemmas 6.1 and 6.2 we know that the causes of depression are determined uniquely. Suppose first that the cause with respect to φ differs from (1). From Corollary 4.3 and Lemma 4.2 we observe that then the α-leading part of u contains a base factor of the form $\pm\alpha^{-1}[w]$, $w \in W(X)$. By looking at Corollary 4.5 and Lemma 4.4, we see that the α-leading part of u cannot have such a base factor. Hence (1) is the cause with respect to φ, $\alpha(e)$ is the α-leading part of u, and the rest is clear. $\square$

Lemma 6.4. *Suppose that $\varphi \in \{\lambda_v^{\pm 1}, \varrho_v^{\pm 1};\ v \in W(X)\}$ is expressed as γ_v^{ε} and δ_w^{η}, where γ and δ stand for λ or ϱ, and where $\varepsilon, \eta \in \{-1, 1\}$ and $v, w \in W(X)$. Then $\gamma = \delta$, $\varepsilon = \eta$ and $v = w$.*

Proof. It suffices to observe that one can always choose such a $u \in W(X)$ that the types γ^{ε} and δ^{η} can be determined from $\varphi(u)$ uniquely and that then $v \neq w$ leads to a contradiction.

Select u in such a way that it contains at least two base factors and that its depth exceeds the depths of v and w at least by two. Recall that $\beta(e) \neq \beta(\alpha(v) + \beta(e))$ for $v \neq e/e$ and $\alpha(\beta(v) + \alpha(e)) \neq \alpha(e)$ when $v \neq e \setminus e$. From Lemmas 5.3 and 4.1 we see that then $\varphi \in \{L_{e/e}, R_{e\setminus e}\}$ if and only if $\varphi(u)$ has more that one base factor, which equals $\alpha[u]$ when $\varphi = R_{e\setminus e}$, and it equals $\beta[u]$ when $\varphi = L_{e/e}$. Assume that $\varphi(u)$ has just one base factor. Then $\varphi \in \{L_{e/e}^{-1}, R_{e\setminus e}^{-1}\}$ if and only if $d(\varphi(u)) = d(u) + 1$, and $\varphi(u)$ is of the form $\beta^{-1}[w]$ in the case of a left translation, while for a right translation it has the form $\alpha^{-1}[w]$. This is similar in the remaining cases where the β-leading part of $\lambda_v(u)$ and $\lambda_v^{-1}(u)$ equals $\beta[\beta[u] \oplus \alpha(v)]$ and $\beta^{-1}[\beta[u] \oplus (\beta(\alpha(v) + \beta(e)) - \beta(e))]$, respectively, and the α-leading part of $\varrho_v(u)$ and $\varrho_v^{-1}(u)$ equals $\alpha[\alpha[u] \oplus \beta(v)]$ and $\alpha^{-1}[\alpha[u] \oplus (\alpha(\beta(v) + \alpha(e)) - \alpha(e))]$, respectively. The rest is clear. $\square$

The results of Lemma 6.4 are not surprising, and they will be assumed in the following text implicitly. They were necessary in order to be sure that no identity of the form like $\varrho_v^{-1} = \lambda_w$ can take place.

Proposition 6.5. *Let X be a non-empty set with an element e, and let u be an element of $W(X)$, $u \neq e$. Assume $k \geqslant 1$ and consider the sequences $v_1, \dots, v_k \in W(X)$ and $\varphi_1, \dots, \varphi_k$, where $\varphi_i \in \{\lambda_{v_i}^{\pm 1}, \varrho_{v_i}^{\pm 1}\}$, $1 \leqslant i \leqslant k$. If $\varphi_i \neq \varphi_{i+1}^{-1}$ for every i, $1 \leqslant i < k$, then $\varphi_k \dots \varphi_1(u) \neq u$.*

Proof. Assume $\varphi_k \dots \varphi_1(u) = u$, $u \in W(X)$ and $u \neq e$. If $\varphi_1 = \varphi_k^{-1}$, then $k \geqslant 3$ and $(\varphi_{k-1} \dots \varphi_2)(\varphi_1(u)) = \varphi_1(u)$. Hence we can be concerned just with the case $\varphi_k \neq \varphi_1^{-1}$. Put $u_0 = u$, $u_1 = \varphi_1(u)$, $\dots$, $u_k = \varphi_k \dots \varphi_1(u)$. Then $u_k = u_0$ and $\varphi_i \dots \varphi_1 \varphi_k \dots \varphi_{i+1}(u_i) = u_1$ for each i, $1 \leqslant i < k$. The sequence $\varphi_1, \dots, \varphi_k$ can be thus replaced by its rotation, and so we can assume that the depth of u_1 attains the maximum of the depths of $u_1, \dots, u_k$. The indices of u_i and φ_i will be interpreted modulo k (such an approach makes the size of k unimportant—it can even equal 1).

There is either $\varphi_2 \notin \{L_{e/e}^{\pm 1}, R_{e\backslash e}^{\pm 1}\}$, or $\varphi_1 \notin \{L_{e/e}^{\pm 1}, R_{e\backslash e}^{\pm 1}\}$, by Lemma 5.4. One could consider $\varphi_k^{-1}, \dots, \varphi_1^{-1}$ in place of $\varphi_1, \dots, \varphi_k$, and hence we can assume $\varphi_1 \notin \{L_{e/e}^{\pm 1}, R_{e\backslash e}^{\pm 1}\}$. Left-right symmetry then makes possible the assumption $\varphi_1 = \varrho_{v_1}^{\pm 1}$, where $v_1 \neq e\backslash e$. We shall show that $u_1 = \alpha^{-1}(\alpha(e) + u_1')$ for some $u_1' \in W(X)$, $u_1' \neq 0$ and $d(u_1') = 0$. This follows from Lemmas 6.1, 6.2 and 6.3 when $\varphi_2 \notin \{L_{e/e}^{\pm 1}, R_{e\backslash e}^{\pm 1}\}$.

The case of $\varphi_2 \in \{L_{e/e}^{\pm 1}, R_{e\backslash e}^{\pm 1}\}$ needs somewhat more attention. There is $\varphi_2 = R_{e\backslash e}$, by Lemma 5.5, and Lemma 5.6 implies $\varphi_3 \in \{L_{e/e}^{\pm 1}, R_{e\backslash e}^{\pm 1}\}$. There is $\varphi_3 \neq R_{e\backslash e}^{-1}$, by $\varphi_3 \neq \varphi_2^{-1}$, and from Lemma 5.7 we get $\varphi_3 = L_{e/e}^{-1}$. Lemma 5.7 also yields the existence of such a $w \in W(X)$ that $u_1 = \alpha^{-1}[w + \alpha(e)]$, $u_3 = \beta^{-1}[w + \beta(e)]$ and $d(w + \alpha(e)) = d(w + \beta(e)) \geqslant 1$.

We have $\varphi_4 \notin \{L_{e/e}^{\pm 1}, R_{e\backslash e}^{\pm 1}\}$, by Lemma 5.4. Let us now consider Corollaries 4.3 and 4.5 (and Lemmas 4.2 and 4.4, when referring to the case (6)) together with their left-right symmetric versions. Firstly we see that $\varphi_4 = \lambda_{v_4}^{\pm 1}$, where $v_4 \neq e/e$. Secondly, there must be $d(w) = 0$, as $d(w) > 0$ stipulates that $w + \beta(e)$ has in its leading part a base factor of the form $\pm\beta[w']$, which is also a base factor of w. This base factor would be retained in the leading part of $w + \alpha(e)$, but there it cannot occur, as $\varphi_1 = \varrho_{v_1}^{\pm 1}$. The structure of u_1 is therefore of the required form in this case as well.

The maximum depth is hence equal to two, and Lemmas 4.2 and 4.4 imply that u_0 equals $\alpha^{-1}(\alpha(v_1' + u_1') - v_1' + \alpha(e))$ when $\varphi_1 = \varrho_{v_1}^{-1}$, and $\alpha^{-1}(\alpha^{-1}(v_1' + u_1') - \alpha^{-1}(v_1') + \alpha(e))$ when $\varphi_1 = \varrho_{v_1}$, respectively, where $v_1' \in W(X)$, $d(v_1') = 0$. The α-leading part of u_0 thus necessarily contains at least two base factors. However, u_0 attains the maximum depth, and hence it can be subjected to the same treatment as u_1. This treatment establishes the existence of exactly one base factor. We have obtained a contradiction. □

From Proposition 1.9 we see that Proposition 6.5 can be restated as

Theorem 6.6. *Define on $W(X)$, X a set, operations $\circ$, $/$, $\backslash$, by $u \circ v = \alpha(u) + \beta(v)$, $u/v = \alpha^{-1}(u - \beta(v))$ and $v \backslash u = \beta^{-1}(u - \alpha(v))$. Then $W(X)(\circ, /, \backslash)$ is a quasigroup isotopic to the Abelian group $W(X)(+, -, 0)$, and its multiplication group is a Frobenius group. Every inner mapping group $(\mathrm{Mlt}\, W(X))_u$, $u \in W(X)$, is a free group with a free base $\{L^{-1}_{(u\circ(v\circ u))/u} L_u L_v;\ v \in W(X)\} \cup \{R^{-1}_{u\backslash((u\circ v)\circ u)} R_u R_v;\ v \in W(X)\}$.*

In Section 3 we defined the quasigroup $Q(X)$ as the subquasigroup of $W(X)$ that is generated by X. We have proved (cf. Corollary 3.5) that $Q(X)$ is free in the variety of all quasigroups isotopic to Abelian groups.

Theorem 6.6 therefore also yields

Theorem 6.7. *Suppose that the quasigroup $Q = Q(\cdot, /, \backslash)$ is free in the class of all quasigroups that are isotopic to an Abelian group. Then $\mathrm{Mlt}\, Q$ is a Frobenius group and $(\mathrm{Mlt}\, Q)_u$ is a free group with a free base $\{L^{-1}_{(u\cdot vu)/u} L_u L_v;\ v \in Q(X)\} \cup \{R^{-1}_{u\backslash(uv\cdot u)} R_u R_v;\ v \in Q(X)\}$, for every $u \in Q$.*

A loop that is not an Abelian group cannot have an inner mapping group which acts regularly and faithfully on at least one of its orbits [11, Proposition 1.6]. Quasigroups of this kind can exist, but they are isotopic to Abelian groups. Theorem 6.7 shows that such quasigroups cannot be described equationally. On the other hand, Proposition 2.9 can be taken as an indication that there is some hope that there can be a structural description in the finite case.

Let us finish by pointing out two problems that are naturally related to investigations done in this paper.

(1) Describe an algorithm that decides if $t \in W(X)$ is an element of $Q(X)$.
(2) Find an abstract description of the groups $\mathrm{Mlt}\, Q(X)$ and $\mathrm{Mlt}\, W(X)$. Are they free?

Acknowledgments. I thank J. D. H. Smith for discussing with me the concept of centrality and to V. A. Shcherbacov for informing me about the relevant results of the Chisinau quasigroup school.

References

[1] *A. Albert*: Quasigroups I. Trans. Amer. Math. Soc. *54* (1943), 507–519.
[2] *V. D. Belousov*: Balanced identities in quasigroups. Matem. sbornik (N.S.) *70* (1966), 55–97. (In Russian.)
[3] *V. D. Belousov*: Osnovy teorii kvazigrupp i lup. Nauka, Moskva, 1967.
[4] *G. B. Belyavskaya*: T-quasigroups and the centre of a quasigroup. Matem. Issled. *111* (1989), 24–43. (In Russian.)
[5] *G. B. Belyavskaya*: Abelian quasigroups and T-quasigroups. Quasigroups and related systems *1* (1994), 1–7.

[6] *R. H. Bruck*: A Survey of Binary Systems. Springer-Verlag, 1971.
[7] *O. Chein, H. O. Pflugfelder and J. D. H. Smith*: Quasigroups and Loops: Theory and Applications. Heldermann, Berlin, 1990.
[8] *A. Drápal*: Multiplication groups of free loops I. Czechoslovak Math. J. *46* (1996), 121–131.
[9] *A. Drápal*: Multiplication groups of free loops II. Czechoslovak Math. J. *46* (1996), 201–220.
[10] *A. Drápal*: Multiplication groups of finite free loops that fix at most two points. J. Algebra *235* (2001), 154–175.
[11] *A. Drápal*: Orbits of inner mapping groups. Monatsh. Math. *134* (2002), 191–206.
[12] *G. Grätzer*: Universal Algebra. Van Nostrand, Princeton, 1968.
[13] *J. Ježek and T. Kepka*: Quasigroups isotopic to a group. Comment. Math. Univ. Carolin. *16* (1975), 59–76.
[14] *J. Ježek*: Normal subsets of quasigroups. Comment. Math. Univ. Carolin. *16* (1975), 77–85.
[15] *J. Ježek*: Univerzální algebra a teorie modelů. SNTL, Praha, 1976.
[16] *T. Kepka and P. Němec*: T-quasigroups I. Acta Univ. Carolin. Math. Phys. *12* (1971), 39–49.
[17] *T. Kepka and P. Němec*: T-quasigroups II. Acta Univ. Carolin. Math. Phys. *12* (1971), 31–49.
[18] *J. D. H. Smith*: Mal'cev Varieties. Springer, Berlin, 1976.

Author's address: Katedra algebry, MFF UK, Sokolovská 83, 186 75 Praha 8, Czech Republic, e-mail: `drapal@karlin.mff.cuni.cz`.