Matematický časopis 23 (1973), No. 3

ROT-QUASIGROUPS

JÁN DUPLÁK, Prešov

Let $\mathscr{E}^2$ be an oriented Euclidean plane and let $(.)$ be a binary operation defined in $\mathscr{E}^2$ by $a \,.\, b = c$, if c is the image of b under the rotation $R[a, +90°]$. We find easily that the groupoid $\mathscr{E}^2$ $(.)$ is a medial, idempotent, elastic and transitive quasigroup. Moreover, the groupoid $\mathscr{E}^2$ $(.)$ satisfies the interesting identity $x \,.\, (x \,.\, y) = z \,.\, [(x \,.\, z) \,.\, y]$. This identity will be taken as an axiom in the description of certain quasigroups, rot-quasigroups, which we are going to study.

We remark that a groupoid with the law of composition (A) in a set $\mathscr{Q}$ is denoted by $\mathscr{Q}$ (A). Let a, b be arbitrary elements of $\mathscr{Q}$ and let there exist uniquely determined $y \in \mathscr{Q}$ such that $A[a, x] = b$, $A[y, a] = b$. Then $\mathscr{Q}(A)$ is a quasigroup. We shall denote $A^{-1}[a, b] = x$, ${}^{-1}A[b, a] = y$ if and only if $A[a, x] = b$, $b = A[y, a]$, respectively. It is clear that if $\mathscr{Q}$ (A) is a quasigroup, then $\mathscr{Q}$ (A^{-1}) and $\mathscr{Q}$ $({}^{-1}A)$ are quasigroups (see [1]).

Definition 1. *A rot-quasigroup is such a quasigroup which satisfies the identity*

$$x \,.\, xy = z(xz \,.\, y)^{(1)} \tag{1}$$

In the following the symbol $\mathscr{Q}(A) = \mathscr{Q}(.)$ or $\mathscr{Q}$ denotes a rot-guasigroup.

This paper considers elementary properties of rot-quasigroups $\mathscr{Q}(.)$ and groups of all their automorphisms, denoted by $(\mathscr{G}\,(\mathscr{Q}), \circ) = \mathscr{G}\,(\mathscr{Q})$.

Theorem 1. *For any* $x, y \in \mathscr{Q}$

$$x \,.\, x = x \quad \text{(idempotency)},$$

$$x(yx \,.\, y) = y, \tag{2}$$

$$x \,.\, yx = xy \,.\, x \quad \text{(elasticity)},$$

$$x \,.\, xy = yxy \,.\, y, \tag{3}$$

$$A^{-1}[x, y] = yxy. \tag{4}$$

---

(1) The expression $x \,.\, y$ will be usually written in the abbreviation xy. Thus $x \,.\, yz = x \,.\, (y \,.\, z)$ and $xyx = x \,.\, yx = xy \,.\, x$.

Proof. The proof is straightforward. From (1) we have the idempotency, (2) for $x = z$, $x = y$, respectively. Now we prove the elasticity. Since $\mathcal{Q}$ (.) is a quasigroup there exists $t \in \mathcal{Q}$ such that $x = yt$ for arbitrary x, $y \in \mathcal{Q}$. It follows from the idempotency and (1) that $x \,.\, yx = x(yx \,.\, yx) = t(yt \,.\, yx) = t(x \,.\, yx)$. Thus $x \,.\, yx = t(x \,.\, yx)$, which implies $t = x \,.\, yx$. Hence $x = yt = y(x \,.\, yx)$ and so $x = y(x \,.\, yx)$. From the last identity and (2) we obtain $x \,.\, yx = xy \,.\, x = xyx$. To prove (3) assume $y = z$ in (1). Then with respect to the elasticity we obtain (3). Finally, we prove (4). It follows from (2) that $A^{-1}[x, y] = yx \,.\, y$ and because of the elasticity we obtain (4).

We recall that the right (left) translation with respect to $a \in \mathcal{Q}$ is the map $R_a : \mathcal{Q} \to \mathcal{Q}$, $x \to x \,.\, a$ ($L_a : \mathcal{Q} \to \mathcal{Q}$, $x \to a \,.\, x$).

Theorem 2. *For any x, $y \in \mathcal{Q}$*

(5) $$L_x^2 = L_y L_{xy}\,,$$

(6) $$L_x L_y = L_z^2, \text{ where } z = {}^{-1}A[y, x]\,,$$

(7) $$L_x^3 y = yxy\,,$$

(8) $$L_x^4 = 1\,,$$

(9) $$(L_x^2 L_y^2)^{-1} = L_y^2 L_x^2,$$

(10) $$L_x L_y = L_y^{-1} L_x^{-1}, \text{ i. e. } (L_x L_y)^2 = 1\,,$$

(11) $$L_x^{-1} = L_x^3 = L_y L_x L_y\,,$$

(12) $$L_{xy}^3 = L_x^2 L_y\,.$$

Proof. It is clear that (1) ⇒ (5) ⇒ (6). From (1) the identity $x(x \,.\, xy) = z(xz \,.\, xy)$ follows and so $L_x^3 y = y(xy \,.\, xy)$, if $y = z$. Hence $L_x^3 y = yxy$. Further (2) and (7) ⇒ (8) ⇒ (9); (6) and (8) ⇒ (10); 10 and (8) ⇒ (11). By (11) and (5), $L_{xy}^3 = L_y L_{xy} L_y = L_x^2 L_y$. This completes the proof.

We recall that a medial quasigroup is such a quasigroup which satisfies the identity $xy \,.\, wz = xw \,.\, yz$.

Theorem 3. *A rot-quasigroup is medial.*

Proof. Choose x, y, z, $w \in \mathcal{Q}$. By (11), (12) and (5), $L_y = L_{xz} L_y \,.\, L_{xz}^3 = L_x^2 L_z = L_y L_{xy} L_z$. Hence $L_{xz} L_y w = L_{xy} L_z w$ and so $xz \,.\, yw = xy \,.\, zw$.

Combining Th 3 (i. e. Theorem 3) with Th 2.6 and Th 8.3 from [1] we obtain the following results.

Corollary 1. *Every rot-quasigroup is transitive, i. e. each loop isotopic to a rot-quasigroup is necessarily a group.*

Corollary 2. *For any $x \in \mathcal{Q}$, L_x and R_x are automorphisms of a rot-quasigroup $\mathcal{Q}$ (.), i. e. L_x, $R_x \in \mathcal{G}$ ($\mathcal{Q}$).*

Corollary 3. *Every rot-quasigroup* $\mathcal{Q}$ (.) *is distributive, i. e.* $\mathcal{Q}$ (.) *satisfies the identities* $x \,.\, yz = xy \,.\, xz$, $xy \,.\, z = xz \,.\, yz$.

Definition 2. *For any* $x, y \in \mathcal{Q}$, *the map* $V_{x,y} = L_x^2 L_y^2$ *is called a left transfer.*

Theorem 4. *For any* $x, y \in \mathcal{Q}$

$$L_x L_y^{-1} = V_{x,\, ^{-1}A[x,\, y]}\,. \tag{13}$$

Proof. It follows from (11) that $L_y^{-1} = L_x L_y L_x$. Then $L_x L_y^{-1} = L_x L_x L_y L_x$ and with respect to (6) we have (13).

The following result is the immediate consequence of (4) and Th 4.

Corollary. *For any* $x, y \in \mathcal{Q}$

$$V_{x,y} = L_x L_{xyz}^{-1}. \tag{14}$$

Theorem 5. $L_a^2 t = L_b^2 t$ *for some* t *if and only if* $a = b$; $L_a^2 x = x$ *if and only if* $a = x$; $V_{a,b} = 1$ *if and only if* $a = b$; $V_{a,b} \neq 1$ *has no invariant points.*

Proof. It follows from (1) that $L_a^2 t = L_b^2 t \Rightarrow a \,.\, at = b \,.\, bt \Rightarrow z(az \,.\, t) = z(bz \,.\, t) \Rightarrow az \,.\, t = bz \,.\, t \Rightarrow a = b$. By (3) $L_a^2 x = x \Leftrightarrow a \,.\, ax = x \Leftrightarrow xax \,.\, x = x \Leftrightarrow a = x$. Because of the statement (8) and the first assertion of the theorem, $V_{a,b} = 1 \Leftrightarrow a = b$. Let $V_{a,b} c = c$. Since $L_a^{-2} = L_a^2$, $L_b^2 c = L_a^2 c$. Hence $a = b$ by the first assertion of this theorem. It follows that $V_{a,b} = 1$. The proof is complete.

Theorem 6. *For any* $x, y, z \in \mathcal{Q}$ *there exists a unique point* $u \in \mathcal{Q}$ *such that* $L_x^2 L_y^2 L_z^2 = L_u^2$. *The point* u *is given by*

$$u = {}^{-1}A[x(zv \,.\, y \,.\, zv), v], \tag{15}$$

where $v \in \mathcal{Q}$ *is an arbitrary element.*

Proof. It follows from (5) that for any $t, v \in \mathcal{Q}$

$$L_x^2 L_y^2 L_z^2 = L_t L_{xt} L_t L_{yt} L_v L_{zv}$$

and according to (10)

$$L_x^2 L_y^2 L_z^2 = L_{xt}^{-1} L_{yt} L_{zv}^{-1} L_v^{-1}.$$

If $L_{yt} = L_{zv}$ (i. e. $yt = zv$, $t = A^{-1}[y, zv] = zv \,.\, y \,.\, zv$], then

$$L_x^2 L_y^2 L_z^2 = L_{xt}^{-1} L_v^{-1} = L_v L_{xt}$$

and by (6), $L_x^2 L_y^2 L_z^2 = L_u^2$, where $u = {}^{-1}A[xt, v] = {}^{-1}A[x(zv \,.\, y \,.\, zv), v]$. The unicity of u follows directly from Th 5.

There are two interesting simplifications of (15), namely

(16) $$u = {}^{-1}A[x\,.\,zyz,z] \qquad \text{for } v = z,$$

(17) $$u = {}^{-1}A[xy,yzy] \qquad \text{for } v = yzy.$$

Since $L_u^{-2} = L_u^2$, $L_x^2L_y^2L_z^2 = (L_x^2L_y^2L_z^2)^{-1} = L_z^2L_y^2L_x^2$. Hence for any $x, y, z \in \mathcal{Q}$

(18) $$L_x^2L_y^2L_z^2 = L_z^2L_y^2L_x^2.$$

Combining (18) with (16) we obtain the identity

(19) $${}^{-1}A[x\,.\,zyz,z] = {}^{-1}A[z\,.\,xyx,x].$$

Definition 3. *For any a, $b \in \mathcal{Q}$ a map $P_{a,b} = R_aR_b^{-1}$ is called a right transfer.*

Theorem 7. *For any a, b, $c \in \mathcal{Q}$*

(20) $$P_{a,b} = V_{R_b^{-2}a,b}\,,$$

(21) $$V_{c,b} = P_{R_b^2c,b}\,.$$

Proof. It is clear that for any a. $b \in \mathcal{Q}$ there exists a unique element $d \in \mathcal{Q}$ such that $bd = R_b^{-2}a$, i. e. $bdb\,.\,b = a$, $a = d\,.\,db$. Similarly, for any b, $d \in \mathcal{Q}$ there exists a unique element $a \in \mathcal{Q}$ such that $bd = R_b^{-2}a$. To complete the proof it suffices to show

(22) $$P_{d.db.b} = V_{bd,b}.$$

From (2) there follows the identity $b = x\,.\,bxb$. Since $L_b \in \mathcal{G}\ (\mathcal{Q})$, $L_b^3b = L_b^3(x\,.\,bxb) = L_b^3x\,.\,L_b^3(bxb) = L_b^3x\,.\,L_b^4(xb) = L_b^3x\,.\,xb$. Hence $b = L_b^3x\,.\,xb$ and by (11), $b = L_dL_bL_dx\,.\,xb = d(b\,.\,dx)\,.\,xb$. According to (2) and Corollary 3 of Th 3, $b = (b\,.\,dbd)(b\,.\,dx)\,.\,xb = [b\,.\,d(bd\,.\,x)]\,.\,xb$. If $u = bd\,.\,x$ and $z = du$, then $b = bz\,.\,xb$, $zb = z(bz\,.\,xb)$, $du\,.\,b = z(bz\,.\,xb)$. By (1) we have $du\,.\,b = b(b\,.\,xb) = b\,.\,bxb$ and so $u(du\,.\,b) = u(b\,.\,bxb)$, $u(du\,.\,b) = (bd\,.\,x)(b\,.\,bxb)$, $d\,.\,db = (bd\,.\,x)\,(b\,.\,bxb)$, $x(d\,.\,db) = x\,.\,(bd\,.\,x)\,(b\,.\,bxb)$, i. e. $R_{d.db}x = x\,.\,(bd\,.\,x)(b\,.\,bxb)$. By (1) have $R_{d.db}x = bd\,.\,[bd\,.\,(b\,.\,bxb)]$ and so $R_{d.bd}x = L_{bd}^2L_b^2R_bx$, hence $R_{d.db} = L_{bd}^2L_b^2R_b$, $R_{d.db}R_b^{-1} = L_{bd}^2L_b^2$, which is the identity (20). If $c = R_b^{-2}a$, then from (20) we obtain (21).

Corollary. *Each left transfer is a right transfer and each right transfer is a left transfer.*

With respect to the last result, we shall speak about a transfer. To express a transfer more precisely we have to use either a right or a left transfer notation.

Next we shall consider the structure of the group $\mathcal{G}\ (\mathcal{Q})$ and of its subgroups. We list five of them:

$\mathcal{G}$ — the group generated by all left and right translations of $\mathcal{Q}\ (.)$,
$\mathcal{G}_L$ — the group generated by all left translations,
$\mathcal{G}_R$ — the group generated by all right translations,

$\mathscr{G}_T$ — the group generated by all transfers,
$\mathscr{G}_S$ — the group generated by all involutions L_x^2.

Theorem 8. *The set of all transfers forms an Abelian group which is identical with the group* $\mathscr{G}_T$.

Proof. By Th 6 there exists $u \in \mathscr{Q}$ such that $V_{x,y}V_{z,t} = V_{u,t}$ for any $x, y, z, t \in \mathscr{Q}$. It follows from (9) that $V_{y,x} = V_{x,y}^{-1}$. Hence the set of all transfers forms the group $\mathscr{G}_T$. By (18) we have $V_{x,y}V_{z,t} = V_{z,y}\ V_{x,y,t} = V_{z,t}$ $V_{x,y}$. Hence $\mathscr{G}_T$ is an Abelian group.

We recall that $\mathscr{H}$ is a normal subgroup of a group $\mathscr{G}$, denoted by $\mathscr{H} \lhd \mathscr{G}$, if $f\mathscr{H}f^{-1} = \mathscr{H}$ for each element f of some set generators of $\mathscr{G}$.

Theorem 9. $\mathscr{G}_T \lhd \mathscr{G}_S \lhd \mathscr{G}_L$; $\mathscr{G}_T \lhd \mathscr{G}_L$.

Proof. It is clear that for any $a, x, y \in \mathscr{Q}$.

$$L_a^2 V_{x,y} L_a^{-2} = L_a^2 L_x^2 L_y^2 L_a^2 = L_y^2 L_x^2 L_a^2 L_a^2 = L_y^2 L_x^2 = V_{y,x}.$$

Hence $\mathscr{G}_T \lhd \mathscr{G}_S$. Further, from (6), (13) and Th 6 it follows that

$$L_a L_x^2 L_a^{-1} = L_a L_x L_x L_a^{-1} = L^2_{-1_{A[x,a]}} L_x^2 L^2_{-1_{A[x,a]}} = L_u^2$$

where u is given by (15), therefore $\mathscr{G}_S \lhd \mathscr{G}_L$. Similarly for any $a, x, y \in \mathscr{Q}$

$$L_a V_{x,y} L_a^{-1} = L_a L_x^2 L_y^2 L_a^{-1} = L_a L_x \,.\, L_x L_y \,.\, L_y L_a^{-1}$$
$$L^2_{-1_{A[x,a]}} L^2_{-1_{A[x,a]}} L_y^2 L^2_{-1_{A[y,a]}} = V_{u}, -1_{A[y,a]},$$

where u is given by (15). This completes the proof.

Theorem 10. $\mathscr{G}_T \lhd \mathscr{G}_R$.

Proof. From the mediality there follows the identity $R_x t \,.\, L_y s = R_y t \,.\, L_x s$. If $u = R_y t$, $z = L_y s$ (i. e. $t = R_y^{-1} u$, $s = L_y^{-1} z$), then $R_x R_y^{-1} u \,.\, z = u \,.\, L_x L_y^{-1} z$. Hence $R_z R_x R_y^{-1} u = R_{L_x L_y{}^{-1}z}\, u$. It is obvious that $L_x L_y^{-1} z = x \,.\, A^{-1}[y, z] =$ $= x \,.\, zyz$, therefore

$$R_z R_x R_y^{-1} = R_{x \cdot zyz}. \tag{23}$$

If $y = z$, then from (23) we have

$$R_x R_y^{-1} = R_y^{-1} R_{xy}. \tag{24}$$

Further, by (24) we have $R_a P_{x,y} R_a^{-1} = R_a R_x R_y^{-1} R_a^{-1} = R_a R_y^{-1} R_{xy} R_a^{-1} =$ $= P_{a,y} P_{xy,a}$. Hence $\mathscr{G}_T \lhd \mathscr{G}_R$. This completes the proof.

Theorems 9 and 10 lead to the question: What do the factor-groups $\mathscr{G}_S/\mathscr{G}_T$, $\mathscr{G}_L/\mathscr{G}_S$, $\mathscr{G}_L/\mathscr{G}_T$ and $\mathscr{G}_R/\mathscr{G}_T$ look like? The following theorems show it.

Theorem 11. $\mathscr{G}_S/\mathscr{G}_T \approx \mathscr{Z}_2$ (*i. e. the group* $\mathscr{G}_S/\mathscr{G}_T$ *is isomorphic to the group of remainders* modulo *2*).

Proof. It follows from Th 6 that each element $f \in \mathscr{G}_S$ can be written in the form $f = L_x^2$ or $f = L_x^2 L_y^2$. If $f = L_x^2 L_y^2$, then $f \in \mathscr{G}_T$. If $f = L_x^2$, then $f = L_a^2 L_a^2 L_x^2 = L_a^2 V_{a,x} \in L_a^2 G_T$. Clearly $(\mathscr{G}_T \cup L_a^2 \mathscr{G}_T) \subset \mathscr{G}_S$. Hence $\mathscr{G}_T \cup \cup L_a^2 \mathscr{G}_T = \mathscr{G}_S$. According to Th 5, $f \in \mathscr{G}_T$, $f \neq 1$ has no invariant point and $f \in L_a^2 \mathscr{G}_T$ has exactly one invariant point. This implies $\mathscr{G}_T \cap L_a^2 \mathscr{G}_T = \emptyset$ and the proof is completed.

Theorem 12. $\mathscr{G}_L / \mathscr{G}_S \approx \mathscr{Z}_2$.

Proof. Similarly to the proof of Th 11 we shall show that $\mathscr{G}_S \cup L_a \mathscr{G}_S$ is a disjoint decomposition of the group $\mathscr{G}_L$. It follows from (6), (11) and Th 6 that each element $f = L_{a_1}^{n_1} \ldots L_{a_k}^{n_k} \in \mathscr{G}_L$ can be rewritten in the form

$$f = L_a^2 \text{ or } f = L_a^2 L_b^2 \text{ or } f = L_a \text{ or } f = L_a L_b^2.$$

If $f = L_a^2$ or $f = L_a^2 L_b^2$, then $f \in \mathscr{G}_S$. If $f = L_a$ or $f = L_a L_b^2$, then $f \in L_a \mathscr{G}_S$. Hence $\mathscr{G}_L \subset (\mathscr{G}_S \cup L_a \mathscr{G}_S)$. Since $(\mathscr{G}_S \cup L_a \mathscr{G}_S) \subset \mathscr{G}_S$, we have $\mathscr{G}_L = \mathscr{G}_S \cup L_a \mathscr{G}_S$, which is a disjoint decomposition of $\mathscr{G}_L$, because $L_a \notin \mathscr{G}_S$.

Theorem 13. $\mathscr{G}_L / \mathscr{G}_T \approx \mathscr{Z}_4$.

Proof. It is easy to show that $\mathscr{G}_T \cup L_a \mathscr{G}_T \cup L_a^2 \mathscr{G}_T \cup L_a^3 \mathscr{G}_T$ is the disjoint decomposition of $\mathscr{G}_L$.

Lemma 1. *Let n be a positive integer. If $R_a^n = 1$ for some element $a \in \mathscr{Q}$, then $R_z^n = 1$ for all $z \in \mathscr{Q}$.*

Proof. From (24) we have $R_x = R_y^{-1} R_{xy} R_y$. If $xy = z$ (i. e. $y = A^{-1}[x, z] = = zxz$), then

$$R_x = R_{A^{-1}[x,z]}^{-1} R_z R_{A^{-1}[x,z]} = R_{zxz}^{-1} R_z R_{zxz}.$$

Thus

$$R_a^n = (R_{zaz}^{-1} R_z R_{zaz})^n = R_{zaz}^{-1} R_z^n R_{zaz}.$$

Since $R_a^n = 1$, $R_{zaz} = R_z^n R_{zaz}$. Hence $R_z^n = 1$.

Lemma 2. *Each element $f \in \mathscr{G}_R$ can be written in the form*

$$R_{a_1} R_{a_2} \ldots R_{a_n} \text{ or } R_{a_1}^{-1} R_{a_2}^{-1} \ldots R_{a_n}^{-1} \text{ or } P_{a_1, a_2},$$

where $a_1, a_2, \ldots, a_n$ are suitable elements of $\mathscr{Q}$ and n is a positive integer.

Proof. Let $\mathscr{L} = \{R_x : x \in \mathscr{Q}\} \cup \{R_x^{-1} : x \in \mathscr{Q}\}$ be the base to the group $\mathscr{G}_R$. We proceed by induction on the length of a word $f \in \mathscr{G}_R$. Clearly, the assertion is valid for $n = 1$ and $n = 2$ (see (24). Assume that $g \in \mathscr{G}_R$ is of the length $n + 1 > 2$. If $g = R_a f$, where

$$f = R_{a_1}^{-1} \ldots R_{a_n}^{-1} = R_{a_1}^{-1} R_{a_2}^{-1} \circ h,\ h = R_{a_3}^{-1} \ldots R_{a_n}^{-1},$$

then by (23),

$$g = R_a R_{a_1}^{-1} R_{a_2}^{-1} \circ h = R^{-1}_{a_1 \cdot a_2 a a_2} \circ h\,,$$

which is the required form of g. Similarly we do the rest of the proof.

Theorem 14. *Let $a \in \mathcal{Q}$ be a fixed element and let $\langle R_a \rangle$ be the subroup of $\mathcal{G}(\mathcal{Q})$ generated by $R_a \in \mathcal{G}_R$. Then $\mathcal{G}_R / \mathcal{G}_T \approx \langle R_a \rangle$.*

Proof. It follows from (23) and (24) that

$$R_{x \cdot zyz} = R_z R_x R_y^{-1} = R_z R_y^{-1} R_{xy} = R_y^{-1} R_{zy} R_{xy}\,.$$

If $zy = t$, $xy = u$ (i. e. $z = {}^{-1}A[t, y]$, $x = {}^{-1}A[u, y]$), then $R_y^{-1} R_t R_u = R_d$, where $d = {}^{-1}A[u, y]. {}^{-1}A[t, y] y {}^{-1}A[t, y]$. Thus for arbitrary elements $a_1, \ldots, a_n$, $b_1, \ldots, b_n$, a, b there exist $e, f \in \mathcal{Q}$ such that

$$P_{e,f} = R_{a_n}^{-1} \ldots R_{a_1}^{-1} R_{b_1} \ldots R_{b_n} P_{a,b}\,,$$

i. e.

$$R_{a_1} \ldots R_{a_n} P_{e,f} = R_{b_1} \ldots R_{b_n} P_{a,b}\,.$$

Hence the decompositions $R_{a_1} \ldots R_{a_n} \mathcal{G}_T$, $R_{b_1} \ldots R_{b_n} \mathcal{G}_T$ are not disjoint and so they are equal. Analogously

$$R_{a_1}^{-1} \ldots R_{a_n}^{-1} \mathcal{G}_T = R_{b_1}^{-1} \ldots R_{b_n}^{-1} \mathcal{G}_T\,.$$

Thus

$$\mathcal{G}_R / \mathcal{G}_T = \bigcup_{i \in \mathcal{N}} R_a^i \mathcal{G}_T\,,$$

where $\mathcal{N}$ is the set of all integers. Therefore $\mathcal{G}_R / \mathcal{G}_T \approx \langle R_a \rangle$. Clearly, the map $R_a^i \mathcal{G}_T \to R_a^i$ is an isomorphism.

The results are summarized in the diagram

$$\begin{tikzcd}
 & \mathcal{G} \arrow[dl] \arrow[dr] & & \mathcal{G}(\mathcal{Q}) \arrow[ll] \\
\mathcal{G}_L \arrow[d, "2"] \arrow[drr, "4"] & & \mathcal{G}_R \arrow[d, "{n,\infty}"] & \\
\mathcal{G}_S \arrow[rr, "2"] & & \mathcal{G}_T &
\end{tikzcd}$$

in which $\mathcal{A} \xrightarrow{n} \mathcal{B}$ denotes that $\mathcal{B}$ is a normal subgroup of $\mathcal{A}$ of the index n and $\mathcal{A} \to \mathcal{B}$ denotes that $\mathcal{B}$ is a subgroup of $\mathcal{A}$.

Now we shall consider the finite rot-quasigroups.

Theorem 15. *If* $\mathcal{Q}$ (.) *is a finite rot-quasigroup, then* card $\mathcal{Q} = 4p - 3$, *where* p *is a positive integer.*

Proof. Let $\mathcal{Q} = \{a_1, \ldots, a_n\}$. It is obvious that $\mathcal{H} = \{L^4_{a_1}, L_{a_1}, L^2_{n_1}, L^3_{a_1}\}$ is a subgroup of $\mathcal{G}_L$ which acts on the set $\mathcal{Q}$ by

$$\mathcal{Q} \times \mathcal{H} \to \mathcal{Q},\ (x, L^i_{a_1}) \to L^i_{a_1} x .$$

This action leads to the orbit decomposition $\mathcal{Q}/\mathcal{H}$ of $\mathcal{Q}$:

$$\mathcal{Q} = \mathcal{H}(a_1) \cup \mathcal{H}(a_2) \cup \ldots \cup \mathcal{H}(a_n) .$$

Clearly, card $\mathcal{H}$ $(a_i) = 4$ for $i = 2, 3, \ldots, n$ and $\mathcal{H}(a_1) = \{a_1\}$. Therefore, card $\mathcal{Q} = 4$ (card $\mathcal{Q}/\mathcal{H} - 1) + 1 = 4p - 3$, where $p =$ card $\mathcal{Q}/\mathcal{H}$.

Example. Let $(\mathcal{Z}_p, +)$ be an Abelian group of remainders modulo p and $\mathcal{Q} = \mathcal{Z}_p \times \mathcal{Z}_p$. Define the binary operation by

$$\mathcal{Q} \times \mathcal{Q} \to \mathcal{Q},\ (a, b) \,.\, (c, d) = (a + b - d, -a + c + b) .$$

If p is odd, then $\mathcal{Q}$ (.) is a rot-quasigroup. It can be easily shown that the last assertion is true.

Acknowledgement

I would like to express my thanks to M. Hejný, for his valuable advice by which he helped me to solve problems concerning the subject.

REFERENCES

[1] БЕЛОУСОВ, В. Д.: Основы теории квазигрупп и луп. Издательство «Наука» 1967.

Received June 2, 1971

Katedra matematiky
Pedagogickej fakulty
Univerzity P. J. Šafárika
Prešov