Mathematica Slovaca

Ján Duplák

Rot-quasigroups as isotopes of Abelian groups

Mathematica Slovaca, Vol. 26 (1976), No. 4, 287--298

Persistent URL: http://dml.cz/dmlcz/129074

Math. Slov., 26, 1976, No. 4, 287—298

ROT-QUASIGROUPS AS ISOTOPES OF ABELIAN GROUPS

JÁN DUPLAK

A quasigroup $Q(.)$ is called a rot-quasigroup if Q(.) satisfies the identity

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

In this paper we shall show that from the existence of a certain kind of Abelian groups (called tur groups) there follows the existence of rot-quasigroups, and conversely. Further we find out necessary and sufficient conditions under which an Abelian group is a tur group. Moreover, we find out sufficient conditions under which a periodic tur group is a direct sum of two isomorphic groups.

In this paper we shall need the following properties of rot-quasigroups: Let $Q(.)=Q(A)$ be a rot-quasigroup, L_x (R_x) a left (right) multiplication of $Q(.)$, $L_x^2=S_x$, $S_xS_y=V_{x,y}$, and x, y, z, t arbitrary elements of $Q(.)$. Then

(2) $xy\,.\,zt=xz\,.\,yt$ (the mediality law),
(3) $x\,.\,x=x$ (idempotency),
(4) $L_xR_x=R_xL_x$ (elasticity),
(5) $A^{-1}[x, y]=yxy$,
(6) $L_x^4=1$,
(7) $x\,.\,xy=yxy\,.\,y$,
(8) $S_xS_yS_z=S_u$ if and only if $u={}^{-1}A[xy, yzy]={}^{-1}A[x\,.\,zyz, z]$,
(9) $S_xS_yS_z=S_zS_yS_x$,
(10) L_x, R_x are automorphisms of $Q(.)$,
(11) $S_at=S_bt$ for some t if and only if $a=b$,
(12) $S_a=x$ if and only if $a=x$,
(13) $V_{a,b}=1$ if and only if $a=b$.

These properties of rot-quasigroups are proved by the author in [3].

Let $G(.)$ and $G(\circ)$ be quasigroups. An ordered triple (α, β, γ) of bijections α, β, γ of G onto G is called an isotopism of $G(.)$ onto $G(\circ)$, and $G(.)$ is said to be isotopic to or an isotope of $G(\circ)$, provided

$$x\,.\,y=\gamma^{-1}(\alpha x\circ\beta y) \tag{14}$$

for all x, y in G. We shall write (14) also in the form (see [1])

$$(.) = (\circ)^{(\alpha\ \beta,\ \gamma)},$$

or

$$(.) = (\circ)^{T}$$

if t e tr p (α β γ) i denoted by T. Every isotope of a quasigroup is a quasigroup. The otopy of quasigroups is clearly an equivalence relation. If $T-(\alpha, \alpha, \alpha)$, then an i otopism T of $Q(A)$ upon $Q(B)$ is an isomorphism and we wr te

$$A^{\alpha} = B .$$

An sotopi m $(\alpha\ \beta, 1)$ of $G(.)$ onto $G(\circ)$ is called a principal isotopism, and $G(\ )$ is called a principal isotope of $G(.)$. The principal isotope $G(\circ)$ of $G(.)$, d fi d n the fol o in way

($$(\ ) = (.)^{(R_a^{\ 1},\ L_b^{\ 1}\ 1)}$$

a t e identity element $b.a$ Thus every quasigroup is isotopic to a loop.

L α β,) an otopism of $G(.)$ on o $G(\circ)$ and $(\alpha', \beta', \gamma')$ be an isotopism of $G(\circ)$ onto $G(\ )$, then $(\alpha\alpha', \beta\beta', \gamma\gamma\ )$ is an isotopism of $G(.)$ onto $G(*)$ (see [1]).

T eo e n 1. L t $Q(\ )$ be rot-quasigroup and e be an arbitrary element of Q. T n the qua gro p $Q(B)$ defined by

6 $$B = (.)^{(R\ ,\ 1,\ L^{-}\ )}$$

is distributive quasigro p.

Pr of. *V' can write* (16) *i the form*

$$[x, y] = L_e(R_e x . y) ,$$
$$B[x, y] = e(xe . y)$$

an ac ording to (1),

$$B[x, y] = x . xy .$$

We see th t operation B is independent of the element e. Next we prove that B is a l t-distribu ive operation Since $Q(\ )$ is distributive, then

$$z[z(x .\ y)] - z[zx . (zx . zy)] ,$$

, accordi g to (17)

$$B[z, B[x, y]] = (z . zx) . (z . zx)(z . zy)$$
$$B[z, B[\ , y]] = B[B[z, x], B[z, y]] ,$$

wh e B is t d' t ib t e oper tion. Fir lly we prove the right-distributivity of B Si ce R and L_x are utomorphisms of $Q(\ )$, then

$$R_z^2L_z(x\,.\,xy)R_z^2L_zx\,.\,(R_z^2L_zx)(R_z^2L_zy)\,,$$
$$[z(x\,.\,xy)z]z=(zxz\,.\,z)\,.\,(zxz\,.\,z)(zyz\,.\,z)\,,$$

and by (7)

$$(x\,.\,xy)\,.\,(x\,.\,xy)z=(x\,.\,xz)\,.\,(x\,.\,xz)(y\,.\,yz)\,.$$

According to (17), we get

$$B[B[x,y],z]=B[x\,.\,xz,y\,.\,yz]\,,$$
$$B[B[x,y],z]=B[B[x,z],B[y,z]]\,,$$

whence B is also a right-distributive operation. This completes the proof.

By Theorem 8.2 of [1] we have the following

Corollary 1. If $Q(B)$ is defined as in Theorem 1, then the quasigroups $Q(^{-1}B)$ and $Q(B)$ (where ^{-1}B is the left-division of B) are distributive quasigroups.

Since an isotope of a transitive quasigroup is a transitive quasigroup, we have the following

Corollary 2. Let B be defined as in Theorem 1. Then the quasigroups $Q(B)$, $Q(^{-1}B)$ are transitive distributive quasigroups, i.e. $Q(B)$ and $Q(^{-1}B)$ are idempotent medial quasigroups.

Lemma 1. Let $Q(B)$ be the isotope of a rot-quasigroup $Q(.)$ defined by (16). Then

$$S_xS_aS_y=S_a \quad \text{if and only if} \quad {}^{-1}B[x,y]=a\,.$$

Proof. It follows from (8) that $S_xS_aS_y=S_a$ if and only if $^{-1}A[xa,aya]=a$, i.e. $a\,.\,aya=xa$, $(a\,.\,ay)a=xa$, using the cancellation law we have $a\,.\,ay=x$ and by (17), $B[a,y]=x$, whence $^{-1}B[x,y]=a$.

Corollary. If $Q(B)$ is an isotope of a rot-quasigroup $Q(.)$, defined by (16), then $Q(^{-1}B)$ is a commutative quasigroup.

This corollary directly follows from (9).

Lemma 2. If a quasigroup $Q(B)$ satisfies the conditions of Lemma 1, then

$$S_xS_aS_y=S_b \quad \text{if and only if} \quad {}^{-1}B[x,y]={}^{-1}B[a,b]\,.$$

Proof. First, suppose $S_xS_aS_y=S_b$. If $s={}^{-1}B[x,y]$ and $u=B[s,a]$, then by Lemma 1 we have

$$S_xS_sS_y=S_s\,,\qquad S_aS_sS_u=S_s\,.$$

Hence

$$S_xS_sS_y=S_aS_sS_u\,.$$

Since $S_x^2 = 1$ for all x, then

$$S \ = S_s S_a S_x S \, S_y \ ,$$

and according to (9) we have $S_u = S_x S_a S_y$. Since $S_b = S_x S_a S_y$, then $S_u = S_b$, and by (11) we get $u = b$. Conversely, suppose ${}^1B[x, y] = {}^1B[a, b]$. If ${}^1B[x, y] = s$, then by Lemma 1,

$$S_x S \, S_y = S_s \quad \text{and} \quad S_a S_s S_b = S_s \ .$$

Hence

$$S_x S \, S_y = S \, S \, S_b, \quad S_b = S \, S_a S_x S_s S_y, \quad S_b = S_s S_s S_x S_a S_y \ ,$$

whence $S_b = S_x S_a S_y$. This completes the proof.

Let L_e^* be a left multiplication of $Q({}^1B)$ (B is defined as in Theorem 1). The isotope $({}^1B)^{(1 \ 1, L_e)}$ of ${}^1B$ will be denoted by $(+)$, i.e.

(18) $$(+) = ({}^1B)^{(1, 1 \ L^*)}$$

Hence

(19) $$x + y = L^* \ {}^1(\ {}^1B[x, y]) \ .$$

Replacing a by e in Lemma 2, we get $b = L_e^* \ {}^1(\ {}^1B[x, y])$, and by (19) we have $b = x + y$. Thus

(20) $$S_x S_e S_y = S_{x+y}$$

Theorem 2. If a quasigroup $Q(B)$ satisfies the conditions of Theorem 1 and $(+)$ is defined by (18), then $Q(+)$ is an Abelian group with the zero e.

Proof. First we prove the identity

(21) $$(+) = B^{(1, \tilde{L}_e \ {}^1R_e, \tilde{R}_e)}$$

where $\tilde{L}_e$, $\tilde{R}_e$ are a left and a right multiplication of $Q(B)$, respectively. It i obvious that if

$$t = \tilde{R}_e \ {}^1(B[x, \tilde{L}_e \ {}^1R_e y]), \quad R_e y - u, \quad L_e \ {}^1u = r \quad \text{and} \quad B[x, r] = s \ ,$$

then $t = R_e \ {}^1s$. From these equations we have

$${}^1B[u, e] = y, \quad {}^1B[u, r] = e, \quad {}^1B[s, r] = x, \quad {}^1B[s, e] = t \ .$$

Since $Q(\ {}^1B)$ is a medial quasigroup,

$${}^1B[\ {}^1B[r, u] \quad B[s \quad]] = {}^1B[\ {}^1B[r, s], \ {}^1B[u, e]]$$

and according to th above ti n we g t ${}^1B[e, t] - {}^1B[x, y]$, whence $t = L^* \ {}^1(\ {}^1B[x, y]$, a l y) t y Thus

$$x+y=\tilde R_e^{-1}(B[x, \tilde L_e^{-1}\tilde R_e y])=B[x,y]^{(1, \tilde L_e^{-1}R_e, \tilde R_e)}.$$

Since $B[x, e]=x.xe=exe.e$, then

$$B[x, e]=exe.e,\ B[e, x]=e.ex,$$
$$\tilde R_e x=L_eR_e^2x, \quad \tilde L_e x=S_e x,$$

whence

(22)
$$\tilde R_e=L_eR_e^2, \quad \tilde L_e=L_e^2.$$

The equations (21) and (16) imply

$$(+)=(.)^{(R_e,\,1,\,L_e^{-1})(1,\,\tilde L_e^{-1}\tilde R_e,\,\tilde R_e)}$$

and by (22),

$$(+)=(.)^{(R_e,\,1,\,L_e^{-1})(1,\,L_e^2L_eR_e^2,\,L_eR_e^2)}=(.)^{(R_e,\,L_e^3R_e^2,\,R_e^2)}$$

Since R_e is an automorphism of $Q(.)$,

$$(.)=(.)^{(R_e^{-2},\,R_e^{-2},\,R_e^{-2})}$$

Therefore

$$(.)^{(R_e,\,L_e^3R_e^2,\,R_e^2)}=(.)^{(R_e^{-2},\,R_e^{-2},\,R_e^{-2})(R_e,\,L_e^{-1}R_e^2,\,R_e^2)}$$
$$=(.)^{(R_e^{-1},\,R_e^{-2}L_e^{-1}R_e^2,\,R_e^{-2}R_e^2)}=(.)^{(R_e^{-1},\,L_e^{-1},\,1)}$$

Thus

(23)
$$(+)=(.)^{(R_e^{-1},\,L_e^{-1},\,1)}$$

i.e. $Q(+)$ is a principal isotope of $Q(.)$. By Corollary 1 of Theorem 2 of [1], $Q(+)$ is a group, and by Theorems 1.2 and 2.9 of [1], e is the zero of $Q(+)$. From (20) and (9) it directly follows that $Q(+)$ is an Abelian group.

Lemma 3. Let $Q(.)$, B, $(+)$ be the same as in Theorem 2. Then the multiplications L_e, R_e of $Q(.)$ are automorphisms of $Q(B)$, $Q(^{-1}B)$ and $Q(+)$.

Proof. Since L_e is an automorphism of $Q(.)$ and $R_eL_e=L_eR_e$,

$$B^{L_e}=B^{(L_e,\,L_e,\,L_e)}=(.)^{(R_e,\,1,\,L_e^{-1})(L_eL_e,\,L_e)}=$$
$$=(.)^{(L_e,\,L_e,\,L_e)(R_e,\,1,\,L_e^{-1})}=(.)^{(R_e,\,1,\,L_e^{-1})}=B.$$

This proves that L_e is an automorphism of $Q(B)$. Next we prove that L_e is an automorphism of $Q(+)$. By (23) we have

$$(+)^{L_e}=(.)^{(R_e^{-1},\,L_e^{-1},\,1)L_e}=(.)^{L_e(R_e^{-1},\,L_e^{-1},\,1)}=$$
$$=(:)^{L_e(R_e^{-1},\,L_e^{-1},\,1)}=(.)^{(R_e^{-1},\,L_e^{-1},\,1)}=(+).$$

Similarly we prove additional assertions.

Theorem 3. Let G be the group of all maps $V_{a,b} = S_a S_b$ of a rot-quasigroup $Q(.)$ (see [3]). If $(+)$ is the isotope of a rot-quasigroup $Q(.)$ defined by (23), then the group $Q(+)$ is isomorphic to the group G.

Proof. Let ψ be the map $Q \to G, x \mapsto V_{e,x}$. By (20) we have $\psi x \psi y = V_{e,x} V_{e,y} = S_e S_x S_e S_y = S_e S_{x+y} = V_{e,x+y} = \psi(x+y)$, whence ψ is a homomorphism. If $V_{e,x} = V_{e,y}$, then $S_x = S_y$ and by (11), $x = y$. Hence ψ is an injective map. Let $V_{u,v}$ in G be an arbitrary element. By (8), there exists an x in Q such that $S_x = S_e S_u S_v$, i.e. $S_e S_x = S_u S_v$, whence $V_{e,x} = V_{u,v}$, $\psi x = V_{u,v}$, and so ψ is a surjective map.

Theorem 4. Let the operations B, $(+)$ satisfy the conditions of Theorem 2. If $-y$ is the element inverse to y with respect to $(+)$, then $B[x, y] = x + x - y = 2x - y$.

Proof. First we prove that a left multiplication L_e^* of $Q(^{-1}B)$ is an automorphism of $Q(+)$. Since $L_e^* = R_e^*$, $L_e^* x = {}^{1}B[x, e]$, i.e. $B[L_e^* x, e] = x$, then $\tilde{R}_e L_e^* x = x$, and by (22),

$$L_e^* = R_e^{-2} L_e^{-1} . \tag{24}$$

Since L_e, R_e are automorphisms of $Q(+)$, L_e^* is an automorphism of $Q(+)$. If $x = y$ in (21), then $(L_e^*)^{-1} x = x + x = 2x$ and thus the map

$$L_e^* : Q(+) \to Q(+), \quad x \mapsto \frac{x}{2}$$

is an automorphism of $Q(+)$. Since $L_e^*(z+y) = {}^{-1}B[x, y]$,

$$^{-1}B[z, y] = \frac{z+y}{2} . \tag{25}$$

If $^{-1}B[z, y] = x$ (i.e. $z = B[x, y]$), then from (25) we have $2x = B[x, y] + y$, whence

$$B[x, y] = 2x - y . \tag{26}$$

this completes the proof.

Theorem 5. Let $Q(.)$ be a quasigroup and $Q(+)$ be the group defined by (23) (or by (18)). Then

$$x . y = x + L_e^{-1} x + L_e y \tag{27}$$

for all x, y in Q.

Proof. If the operation B is defined by (16), then $x . y = L_e^{-1}(B[R_e^{-1} x, y])$. Using (26), we have

$$x . y = L_e^{-1}(2R_e^{-1} x - y) = L_e^{-1} R_e^{-1}(2x) - L_e^{-1} y .$$

Since ${}^{1}B[e, B[y, e]] = y$ for all y in Q,

$$^{-1}B[e, y . ye] = y . \tag{28}$$

The operation B is independent of the element e, therefore

$$B=(.)^{(R_e,1,L_e^{-1})}=(.)^{(R_y,1,L_y^{-1})}$$

for all y in Q. Since L_e is an automorphism of $Q(^{-1}B)$ and $Q(B)$, then L_y is also an automorphism of $Q(^{-1}B)$ and $Q(B)$. According to (28),

$$L_y(^{-1}B[e, y.ye])=L_y y, \quad ^{-1}B[L_y e, L_y^3 e]=y\ ,$$
$$^{-1}B[ye, L_y^{-1}e]=y\ .$$

By (5), we have $L_y^{-1}e=A^{-1}[y, e]=y, e]=eye$, therefore

$$^{-1}B[ye, eye]=y, \quad L_e^{-1}(^{-1}B[ye, eye])=L_e^{*-1}y=L_e^{*-1}(^{-1}B[y, y])\ .$$

According to (19), $ye+eye=y+y$. If $y=R_e^{-1}x$, then $x+L_e x=R_e^{-1}x+R_e^{-1}x$, $L_e^{-1}x+x=L_e^{-1}(2R_e^{-1}x)=L_e^{-1}R_e^{-1}(2x)$. Thus $x.y=x+L_e^{-1}x+L_e y$. This completes the proof.

If L_e is a multiplication of a rot-quasigroup $Q(.)$, then by (22) and (26), $L_e^2 x=\tilde{L}_e x=B[e, x]=e+e-x=-x$. Thus we have the following important property of an automorphism L_e of the group $Q(+)$:

(29) $$L_e^2 x=-x$$

for all x in Q. If $x+x=e$ in $Q(+)$, i.e. $V_{e,x}^2=1$, then by (8), $V_{-1A[e.exe,e],x}=1$ and by (13), $^{-1}A[e\ .\ exe, e]=x$, i.e. $xe=e\ .\ exe$, whence $x=e$. This proves the following property of the group $Q(+)$:

$$x=e \quad \text{if and only if} \quad x+x=e\ ,$$

where e is the zero of $Q(+)$. Since $x+L_e^{-1}x=L_e^{-1}R_e^{-1}(2x)$ and $L_e^{*-1}x=2x$, then $x+L_e^{-1}x=L_e^{-1}R_e^{-1}L_e^{*-1}x=R_e x$. Consequently, $x+L_e^{-1}x$ is an automorphism of $Q(+)$.

Now we shall describe necessary and sufficient conditions under which an Abelian group is isotopic to a rot-quasigroup. Therefore we give the following

Definition 1. Let $H(+)$ be an Abelian group with the following properties

(I) there exists an automorphism φ of $H(+)$ such that $\varphi^2 x=-x$ for all x in H,

(II) $H(+)$ has no element of the order 2,

(III) the map $\varrho: H\to H$, $x\mapsto x+\varphi^{-1}x$ is a surjective map, provided that φ has the property (I) of the definition.

Then $H(+)$ is said to be a tur group and φ is a tur automorphism of $H(+)$.

We may easily verify that the conditions of the definition are independent.

By the above-presented discussion, the principal isotope $(.)^{(R_e^{-1},L_e^{-1},1)}$ of a rot-quasigroup $Q(.)$ is a tur group. The following theorem shows that any tur group is isotopic to a rot-quasigroup.

Theorem 6. If $H(+)$ is a tur group and φ a tur automorphism of $H(+)$, then the groupoid $H(.)$ defined by

$$x\,.\,y = x + \varphi^{-1}x + \varphi y \tag{30}$$

is a rot-quasigroup.

Proof. Denote by ϱ the map $H \to H$, $x \mapsto x + \varphi^{-1}x$. By (30), we have $(.) = (+)^{(\varrho,\varphi,1)}$. In order to prove that $H(.)$ is a quasigroup, we must show that ϱ is a bijection. Moreover, ϱ is a homomorphism. Indeed, $\varrho(x+y) = x + y + \varphi^{-1}(x+y) = x + \varphi^{-1}x + y + \varphi^{-1}y = \varrho x + \varrho y$. Next we prove that $Ker\varrho = \{e\}$. If $\varrho x = e$, i.e. $x + \varphi^{-1}x = e$, then $\varphi x + x = \varphi\varrho x = \varphi e = e$. Thus $\varrho x + \varphi\varrho x = e$, i.e. $(x + \varphi^{-1}x) + (\varphi x + x) = e + e = e$, hence $2x = e$ and by (II), $x = e$. Thus Ker $\varrho = \{e\}$. According to (II), ϱ is an automorphism of $H(+)$. Finally we show the identity (1). Clearly, the left-hand side of (1) is

$$x\,.\,xy = x + \varphi^{-1}x + \varphi(xy) = x + \varphi^{-1}x + (x + \varphi^{-1}x + \varphi y) =$$
$$= x + \varphi^{-1}x + \varphi x + x + \varphi^2 y = 2x - y\ .$$

Using $\varphi^{-1}x = \varphi^3 x = \varphi^2(\varphi x) = -\varphi x$, i.e.

$$\varphi^{-1}x = -\varphi x\ , \tag{31}$$

the right-hand side of (1) is

$$z(xz\,.\,y) = z + \varphi^{-1}z + \varphi(xz\,.\,y) = z + \varphi^{-1}z + \varphi(xz + \varphi^{-1}xz +$$
$$+ \varphi y) = z + \varphi^{-1}z + \varphi x + x - z + x + \varphi^{-1}x + \varphi z - y = 2x - y\ .$$

Thus the sides of (1) are equal. This completes the proof.

According to (31), we can write (30) in the form

$$x\,.\,y = x - \varphi x + y\ .$$

If φ is a tur automorphism of a tur group $H(+)$, then $(\varphi^{-1})^2 x = \varphi^{-2}x = \varphi^2 x = -x$, so φ^{-1} is also a tur automorphism of $H(+)$. According to (30), a groupoid $H(\circ)$ defined by

$$x \circ y = x + \varphi x - \varphi y$$

is a rot-quasigroup (isotopic to $H(.)$, which is defined by (32)).

Theorem 7. An Abelian group $Q(+)$, which has the properties (I) and (II) of Definition 1, is a tur group if and only if

(IV) for every y in Q, there exists x in Q such that

$$2x = y\ .$$

Proof. Let $Q(+)$ be a tur group with the zero e and φ be a tur automorphism of $Q(+)$. Then $\varphi = L_e$ is a multiplication of a rot-quasigroup $Q(.)$ defined by (30).

Since L_e^{*-1}: $Q \to Q$, $x \mapsto 2x$ is an automorphism of $Q(+)$, there exists an x in Q such that $2x = y$. Conversely, let (IV) hold. We must show that the map ϱ: $x \mapsto x - \varphi x$ is a surjective map. Clearly, ϱ is a homomorphism of $Q(+)$. Let $\varrho x = a$, where a is an element of Q. Then $\varphi\varrho x = \varrho a$, i.e. $x + \varphi x = \varphi a$ and also $(x + \varphi x) + (x - \varphi x) = \varphi a + a$, whence $2x = a + \varphi a$. By (IV), there exists b in H such that $2b = a + \varphi a$. Now we show that $\varrho b = a$. Let $\varrho b = c$. Then

$$2c = \varrho b + \varrho b = \varrho(2b) = \varrho(a + \varphi a) = a + \varphi a - \\ - \varphi(a + \varphi a) = a + \varphi a - \varphi a + a = 2a \ .$$

Hence $2(a - c) = e$, and by (II), $a - c = e$, i.e. $a = c$. This completes the proof.

Let $H(+)$ be an Abelian group with the properties (II) and (IV). Then the product group $H \times H$ is a tur group. Indeed the map

$$\varphi: H \times H \to H \times H, \quad (x, y) \mapsto (-y, x)$$

is a tur automorphism of $H \times H$, and so by Theorem 7, $H \times H$ is a tur group. A tur group need not be a direct sum of two isomorphic groups. In what follows we shall find sufficient conditions under which a periodic tur group is a direct sum of two isomorphic groups.

Theorem 8. Let Z_r be the cyclic group of order r and let Z_r be the direct sum of cyclic p-groups $F_1, F_2, \ldots, F_s$, whose orders are $r_1^{n_1}, \ldots, r_s^{n_s}$, respectively. Then Z_r is a tur group if and only if every r_i is a prime of the form $4m_i + 1$, where m_i is a positive integer, $i = 1, 2, \ldots, s$.

Proof. Let Z_r be a tur group and φ be a tur automorphism of Z_r. Evidently, $\varphi(F_i) = \{\varphi t\colon t \in F_i\}$ is a group of order $r_i^{n_i}$. Since $r_i \neq r_j$ for $i \neq j$, $\varphi(F_i) = F_i$, so F_i is a tur group for all i. Thus Z_r is a direct sum of cyclic p-groups which are tur groups. Let $C_i = \{0, 1, 2, \ldots, r_i^{n_i} - 1\}$ and let $\varphi 1 = k$. Then $\varphi^2 1 = \varphi k = k\varphi 1 = k^2$. Since $\varphi^2 1 = -1$, $k^2 \equiv -1 \pmod{r_i^{n_i}}$. According to § 4b and § 3a of Chapter V of [2], $r_i = 4m_i + 1$. Conversely, suppose $r = r_i^{n_i} \ldots r_s^{n_s}$, where $r_i = 4m_i + 1$ is a prime for all $i = 1, 2, 3, \ldots, s$. According to Exercise 3a and § 4b of Chapter V of [2], there exists k_i such that $k_i^2 \equiv -1 \pmod{r_i^{n_i}}$ for all i. Let us define φ_i, $F_i \to F_i$ by $\varphi_i t = tk_i$. It follows from Exercise 6 of Chapter V of [2] that k_i and r_i are relatively prime, therefore φ_i is a bijection. It may be easily verified that φ_i is a tur automorphism of the cyclic p-group F_i, which has the order $r_i^{n_i}$, whence F_i is a tur group for all i. Since a direct sum of tur groups is a tur group, Z_r is a tur group.

Corollary 1. If Z_r is a cyclic tur group, then Z_r is a direct sum of cyclic p-groups which are tur groups.

Corollary 2. If φ is a tur automorphism of a cyclic tur group Z_r, and if Z_r is a direct sum of p-groups $F_1, F_2, \ldots, F_s$, then $\varphi(F_i) = F_i$ for every $i = 1, 2, \ldots, s$.

Example 1. Let $Z(p^\infty)$ be a group of the type p^∞. Then $Z(p^\infty)$ is a tur group if and only if there exists a positive integer m such that $p = 4m + 1$.

Proof. Let C_n be such a subgroup of $Z(p^\infty)$ whose order is p^n and let $p=4m+1$. By Theorem 8, C_n is a tur group for all $n=1, 2, 3, \ldots$. It follows from Exercise 6 of Chapter V of [2] that the congruence $x^2 \equiv -1 \pmod{p^n}$ has exactly two solutions, therefore C_n has exactly two tur automorphisms. Let φ_1 be a tur automorphism of C_1. We shall define a tur automorphism φ of $Z(p^\infty)$ by induction on n. Let φ_n be a tur automorphism of C_n and let ψ_1, ψ_2 be distinct tur automorphisms of C_{n+1}. Since C_n is a subgroup of C_{n+1}, $\psi_1(C_n)$ and $\psi_2(C_n)$ are subgroups of C_{n+1}. Every group C_{n+1} has a unique subgroup of the order p^n, therefore the restrictions of ψ_1 and ψ_2 to C_n are tur automorphisms of C_n. Consequently, either ψ_1 or ψ_2 is an extension of γ_n. If ψ_i ($i=1$ or $i=2$) is an extension of φ_n, then set $\varphi_{n+1}=\psi_i$. Now we define φ: $Z(p^\infty)\to Z(p^\infty)$, by $\varphi x=\varphi_n x$ for x in C_n. It can be easily shown that φ is a tur automorphism of $Z(p^\infty)$. The converse follows from Theorem 8.

Theorem 9. If a tur group H is finite, then the order r of H has the form

$$r=r_1^{n_1}\ldots r_s^{n_s}.q^2\,,$$

where $r_i=4m_i+1$ is a prime for all $i=1, 2, 3, \ldots, s$, q is odd, and $n_1, n_2, \ldots, n_s$ are positive integers.

Proof. Since H is finite, H is a direct sum of cyclic p-groups $C_1, C_2, \ldots, C_s$, whose orders are $r_1^{n_1}, r_2^{n_2}, \ldots, r_s^{n_s}$, respectively. Let φ be a tur automorphism of H and let C_i^1 be a subgroup of C_i such that C_i^1 has the order r_i. Clearly $\varphi(C_i^1)$ is such a cyclic subgroup of H which is isomorphic to C_i^1. Let 0 be the zero of H. Then either $\varphi(C_i^1)\cap C_i^1\neq 0$, or $\varphi(C_i^1)\cap C_i^1=0$. If $\varphi(C_i^1)\cap C_i^1\neq 0$, then obviously $\varphi(C_i^1)\cap C_i^1=C_i^1$, thus C_i^1 is a tur group and by Theorem 8, $p_i=4m_i+1$. Now, let $\varphi(C_i^1)\cap(C_i^1)=\{0\}$. Then $\varphi(C_i)\cap C_i=\{0\}$. To prove this suppose $\varphi(C_i)\cap C_i= =C\neq\{0\}$. Then according to the property (I) of a tur automorphism φ we have

$$\varphi(C)=\varphi[\varphi(C_i)\cap C_i]=\varphi^2(C_i)\cap\varphi(C_i)=C_i\cap\varphi(C_i)=C\,,$$

whence C is a tur group of the order $r_i^{m_i}$, $m_i\leqslant n_i$. Since C, C_i^1 are subgroups of C_i, C_i^1 is a subgroup of C. C_i has a unique subgroup of the order r_i, therefore $\varphi(C_i^1)\cap C_i=\{0\}$. Since $C_i^1\subset C$ and $\varphi(C_i^1)\subset(C)=C\subset C_i$, $\varphi(C_i^1)\subset C_i$. Consequently, $\varphi(C_i^1)\cap C_i=\varphi(C_i^1)\neq\{0\}$ and this is in contradiction with the above mentioned assertion. Hence $\varphi(C_i)\cap C_i=\{0\}$. Since $\varphi(C_i)$ is a cyclic p-group, there exists $j\neq i$ such that $\varphi(C_i)\subset C_j$. Hence $\varphi^2(C_i)\subset\varphi(C_j)$, i.e. $C_i\subset\varphi(C_j)$. Since C_i is not a subgroup of any cyclic p-subgroup of H expect C_i, $C_i=\varphi(C_j)$ and also $\varphi(C_i)=C_j$. Thus for each C_i, there are two alternatives, either $r_i=4m_i+1$ or there exists $j\neq i$ such that C_i is isomorphic to C_j, more preciselv, $\varphi(C_i)=C_j$. If $\varphi(C_i)=C_j$, $r\neq i, j$, then obviously $\varphi(C_r)\cap C_i=\varphi(C_r)\cap C_j=\{0\}$. This completes the proof.

Since there exist more than two solutions of the congruence $x^2\equiv -1$ (mod $r_1^{n_1}\ldots r_s^{n_s}$), there are tur groups which have more than two tur automorphisms.

If φ_1 and φ_2 are two tur automorphisms of a tur group $H(+)$, then the quasigroups $H(C)$, $H(D)$ defined by

$$C=(+)^{(\varrho_1,\varphi_1,1)}, \qquad D=(+)^{(\varrho_2,\varphi_2,1)},$$

where $\varrho_i = x-\varphi_i x$, $i=1, 2$, are isotopic. Clearly

$$C=D^{(\varrho_2^{-1}\varphi_1,\varrho_2^{-1}\varphi_1,1)}$$

Theorem 10. Let $H(+)$ be a periodic tur group with the zero O. If there exists a tur automorphism ξ of $H(+)$ such that for every cyclic p-subgroup C of $H(+)$ with respect to a prime $p=4m+1$, there holds $\xi(C)\cap C=\{0\}$, then $H(+)$ is a direct sum of two isomorphic subgroups.

Proof. If G is a cyclic subgroup of $H(+)$, then $\xi(G)\cap G=\{0\}$. Indeed, if $G\cap\xi(G)=P\neq\{0\}$, then P is a cyclic tur group. By Corollary 1 of Theorem 8, P is a direct sum of the cyclic p-groups P_1, P_2, ..., P_s, which are tur groups. By Corollary 2 of Theorem 8, $\xi(P_i)=P_i$, which is in contradiction with the assumption of this theorem. To prove the theorem, we proceed by transfinite induction on elements of H. Let $x\in H$, $x\neq 0$ be an element. (If $H=\{0\}$, then the theorem is trivial). Denote by C_x the cyclic subgroup of $H(+)$ generated by x. Then $\xi(C_x)\cap C_x=\{0\}$. Let H_1 be the direct sum of groups C_x, $\xi(C_x)$. Let H_2 be a subgroup of $H(+)$ such that H_2 is a direct sum of the groups K, $\xi(K)$ and $H_1\subset H_2$. Denote by C_y a cyclic p-subgroup of $H(+)$ generated by an element y in $H\setminus H_2$. Then either $C_y\cap K=C_u=\{0\}$ or $C_y\cap\xi(K)=\{0\}$. To prove this, suppose $C_y\cap k=C_u\neq\{0\}$ and $C_y\cap\xi(K)=C_v\neq\{0\}$. Since C_u, C_v are cyclic subgroups of the p-group C_y, we have $C_u\cap C_v\neq\{0\}$. This implies $K\cap\xi(K)\neq\{0\}$, and this is in contradiction with the induction assumption. Without loss of generality suppose $\xi C_y\cap K\neq\{0\}$. Then $\xi(C_y)\cap\xi(K)=\{0\}$ and also $[\xi(K)+C_y]\cap[K+\xi(C_y)]=\{0\}$. Hence we can define the following direct sum

$$H_3=\xi[K+\xi(C_y)]+[K+\xi(C_y)] .$$

If $C_y\cap[(K+\xi(K))\setminus(K\cup\xi(K))]=C_z\neq\{0\}$ then exist elements t, w such that $t\in K$, $C_t+\xi C_t=C_z+\xi C_z$, $C_t\subset C_w$, $C_w+\xi C_w=C_y+\xi C_y$. Hence we can define

$$H_3=\xi(K+C_w)+(K+C_w) .$$

This completes the proof.

Corollary 1. Every periodic tur group which does not contain elements of order p^k, $k=1, 2, 3, \ldots$, where p is a prime of the form $4m+1$, is a direct sum of two isomorphic groups.

Example 2. Let $Z_{13}(+)$ be the cyclic group of the order 13 and let $Z_{13}=\{0, 1, 2, \ldots, 9, a, b, c\}$. By Theorem 8, the cyclic group $Z_{13}(+)$ is a tur group. We may easily verify that the map φ: $Z_{13}\to Z_{13}$, $r\mapsto 5r$ is a tur automorphism of $U_{13}(+)$. By Theorem 6, the groupoid $Z_{13}(.)$ defined by $x.y=x-\varphi x+\varphi y$ is a rot-quasigroup which is given by the multiplication table

·	0	1	2	3	4	5	6	7	8	9	a	b	c
0	0	5	a	2	7	c	4	9	1	6	b	3	8
1	9	1	6	b	3	8	0	5	a	2	7	c	4
2	5	a	2	7	c	4	9	1	6	b	3	8	0
3	1	6	b	3	8	0	5	a	2	7	c	4	9
4	a	2	7	c	4	9	1	6	b	3	8	0	5
5	6	b	3	8	0	5	a	2	7	c	4	9	1
6	2	7	c	4	9	1	6	b	3	8	0	5a	
7	b	3	8	0	5	a	2	7	c	4	9	1	6
8	7	c	4	9	1	6	c	3	8	0	5	a	2
9	3	8	0	5	a	2	7	c	4	9	1	6	b
a	c	4	9	1	6	b	3	8	0	5	a	2	7
b	8	0	5	a	2	7	c	4	9	1	6	b	3
c	4	9	1	6	b	3	8	0	5	a	2	7	c

Example 3. Let $R(.)$ be the multiplicative group of all positive real numbers and let $Q = R \times R$. Define a binary operation $(\circ)$ on the set Q by

$$(a, b) \circ (c, d) = \left(\frac{a.b}{d}, \frac{b.c}{a}\right).$$

It can be easily shown that $Q(\circ)$ is a rot-quasigroup.

REFERENCES

[1] БЕЛОУСОВ, В. Д.: Основы теории квазгрупп и луп. 1-е изд. Москва 1967.
[2] ВИНОГРАДОВ, И. М.: Основы теории чисел. 1-е изд. Москва 1965.
[3] DUPLÁK, J.: Rot-quasigroups. Mat. Čas., 23, 1972, 223—230.

Received November 11, 1972

Katedra matematiky
Pedagogickej fakulty UPJS
Leninovo nam 6
080 01 Presov

РОТ-КВАЗИГРУППЫ КАК ИЗОТОПЫ АБЕЛЕВЫХ ГРУПП

Ян Дуплак

Резюме

Квазигруппа $Q(.)$ называется рот-квазигруппой, если в ней выполняется тождество $x.xy = z(xz.y)$. В этой работе показано, что существование рот-квазигруппы эквивалентно существованию некоторых абелевых групп (названных тур группы). Далее найдены достаточные и необходимые условия, при которых абелева группа является тур группой, и достаточные условия, при которых тур группа разложима в прямую сумму двух изоморфных групп.