Commentationes Mathematicae Universitatis Carolinae

Jaroslav Ježek

Normal subsets of quasigroups

Commentationes Mathematicae Universitatis Carolinae, Vol. 16 (1975), No. 1, 77--85

Persistent URL: http://dml.cz/dmlcz/105606

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE

16,1 (1975)

NORMAL SUBSETS OF QUASIGROUPS

Jaroslav JEŽEK, Praha

Abstract: A characterization of normal subsets (i.e. blocks of normal congruences) in quasigroups is given.

Key words: Quasigroup, loop, normal subset, congruence.

AMS: 20N05 Ref. Ž.: 2.721.7

---

1. A connection between quasigroups and loops. The reader is supposed to be acquainted with Section 1 of [4]. Terminology can be found in [1] and [2].

Quasigroups will be considered as algebras with three binary operations. The class $\mathcal{K}$ of all quasigroups is a variety. $\mathcal{K}^*$ denotes the variety of all algebras $Q(\cdot, /, \backslash, e)$ such that $Q(\cdot, /, \backslash)$ is a quasigroup and $e \in Q$.

We denote by $\mathcal{M}$ the variety of all algebras $Q(*, /\!/, \backslash\!\backslash, f, \alpha, \beta, \gamma, \delta)$ satisfying the following four conditions:

(i) $Q(*, /\!/, \backslash\!\backslash, f)$ is a loop with the unit f;

(ii) $\alpha, \beta, \gamma, \delta$ are permuations of Q (and thus unary operations in Q);

(iii) $\gamma = \alpha^{-1}$ and $\delta = \beta^{-1}$;

(iv) $\beta(f) = f$.

Further, we define a translation φ of the type $\{ \cdot , / , \backslash , e \}$ into the type $\{ * , /\!/ , \backslash\!\backslash , f, \alpha , \beta , \gamma , \delta \}$ and a translation ψ of $\{ * , /\!/ , \backslash\!\backslash , f, \alpha , \beta , \gamma , \delta \}$ into $\{ \cdot , / , \backslash , e \}$ as follows:

$$\varphi (\cdot) = \alpha (x) * \beta (y) ,$$
$$\varphi (/) = \gamma (x /\!/ \beta (y)) ,$$
$$\varphi (\backslash) = \delta (\alpha (x) \backslash\!\backslash y) ,$$
$$\varphi (e) = f ,$$
$$\psi (*) = (x/e) ((e/e) \backslash y) ,$$
$$\psi (/\!/) = (x /((e / e) \backslash y)) e ,$$
$$\psi (\backslash\!\backslash) = (e / e) ((x / e) \backslash y) ,$$
$$\psi (f) = e ,$$
$$\psi (\alpha) = xe ,$$
$$\psi (\beta) = (e / e) x ,$$
$$\psi (\gamma) = x / e ,$$
$$\psi (\delta) = (e / e) \backslash x .$$

Corresponding to these translations, there are mappings T_φ of $\mathfrak{M}$ into $\mathcal{K}^*$ and T_ψ of $\mathcal{K}^*$ into $\mathfrak{M}$.

1.1. <u>Theorem</u>. The varieties $\mathcal{K}^*$ and $\mathfrak{M}$ are rationally equivalent under φ, ψ .

<u>Proof</u> is a matter of counting.

2. <u>Normal subsets</u>. By a normal congruence of a quasigroup $Q(\cdot , / , \backslash)$ we mean any congruence of the algebra $Q(\cdot , / , \backslash)$. In other words: $\sim$ is a normal congruence iff it is a congruence of $Q(\cdot)$ and the factor $Q/\sim$ is a quasigroup. A subset H of Q is called

normal if it is a block of a normal congruence of Q .

In [3] normal subsets of finite and in [1] normal subquasigroups of arbitrary quasigroups are characterized. Belousov's proof is complicated. We shall find a more simple proof which can be, moreover, applied to arbitrary normal subsets. The idea is the following: Theorem 1.1 enables us to restrict ourselves to the case of normal subloops and the proof for normal subloops is easy.

2.1. Proposition. Let $\sim$ be a normal congruence of a quasigroup Q ; let H be a block of $\sim$ and e an element of H . Then

(i) $a \sim b \Longleftrightarrow aH = bH \Longleftrightarrow Ha = Hb \Longleftrightarrow ea / b \in H \Longleftrightarrow$
$\Longleftrightarrow (a / e) \backslash b \in H \Longleftrightarrow b \in (a / e) H$;

(ii) $(a / e) H = H(e \backslash a)$ for all $a \in Q$; the set $(a / e) H$ is just the block of $\sim$ containing a .

Proof is easy.

Let Q be a quasigroup and e an arbitrary element of Q . By an e-inner permutation of Q we mean a permutation p belonging to the associated group of Q and satisfying $p(e) = e$. If e is given, then the set of all e-inner permutations of Q is evidently a subgroup of Q .

2.2. Proposition. Let Q be a quasigroup and e an element of Q . For any $a, b \in Q$ put

$$R_{a,b} = R^{-1}_{e\backslash(ea.b)} \circ R_b \circ R_a ,$$

$$L_{a,b} = L^{-1}_{(a.be)/e} \circ L_a \circ L_b ,$$

$$T_a = L^{-1}_{ea/e} \circ R_a .$$

The group of all e-inner permutations of Q is just the subgroup of the permutation group of Q generated by all these permutations $R_{a,b}$, $L_{a,b}$ and T_a (where a and b range over Q).

Proof is contained in [1].

If Q is a loop with the unit 1 , then 1-inner permutations of Q are called its inner permutations.

2.3. Lemma. A subloop H of a loop Q is normal iff any inner permutation of Q maps H into H .

Proof. Suppose first that H is normal, so that H is a block of a normal congruence $\sim$ of Q . If p is an inner permutation and $h \in H$, then $h \sim 1$ and thus $p(h) \sim p(1) = 1 \in H$.

Suppose now that H is a sublopp and any inner permutation of Q maps H into H . Taking inverse permutations into account we see that any inner permutation maps H onto H . Define an equivalence $\sim$ on Q by

$$a \sim b \text{ if } aH = bH .$$

Evidently, H is a block of $\sim$. We shall show that $\sim$ is a normal congruence of Q .

We have $a \cdot bH = ab \cdot H$ for all $a, b \in Q$. Indeed, $a \cdot bH = L_a \circ L_b(H) = L_{ab} \circ L_{a,b}(H) = L_{ab}(H)$.

We have $a \sim b \Longleftrightarrow b \in aH \Longleftrightarrow a \backslash b \in H$. Indeed, $aH = bH$ implies $b = b \cdot 1 \in bH = aH$ and $b \in aH$ implies

$a \setminus b \in H$ evidently; if $a \setminus b \in H$, then $aH = a \cdot (a \setminus b)H = a(a \setminus b) \cdot H = bH$.

We have $a \sim b \Longleftrightarrow ac \sim bc$ and $a \sim b \Longleftrightarrow ca \sim cb$. Indeed, the inner permutation $L_{ac}^{-1} \circ R_c \circ L_a$ transforms $a \setminus b$ into $ac \setminus bc$ and the inner permutation $L_{ca}^{-1} \circ L_c \circ L_a$ transforms $a \setminus b$ into $ca \setminus cb$.

This shows that $\sim$ is a normal congruence, so that H is normal.

2.4. Theorem. Let a quasigroup Q, a subset H of Q and an element $e \in H$ be given. H is a normal subset of Q iff the following two conditions are satisfied:

(i) any e-inner permutation of Q maps H into H;

(ii) if $(a / e)b = c$ and two of the elements a, b, c belong to H, then the third belongs to H, too.

Proof. Suppose first that H is normal, so that H is a block of a normal congruence $\sim$ of Q. If p is an e-inner permutation and $h \in H$, then $h \sim e$ and thus $p(h) \sim p(e) = e \in H$. Let $(a / e)b = c$. If $a, b \in H$, then $c = (a / e)b \sim (e/e)e = e \in H$. If $a, c \in H$, then $b = (a / e) \setminus c \sim (e / e) \setminus e = e \in H$. If $b, c \in H$, then $a = (c / b)e \sim (e / e)e = e \in H$.

Suppose now that the conditions (i) and (ii) are satisfied. Taking inverse permutations into account we see that any e-inner permutation maps H onto H. Put $Q(*, /\!/, \setminus\!\setminus, 1, \alpha, \beta, \gamma, \delta) = T_\psi(Q(\cdot, /, \setminus, e))$.

If $b \in Q$, then $(e / e) \setminus b \in H$ iff $b \in H$. Indeed,

$(e / e) \backslash b = L_{e/e}^{-1}(b)$ and $L_{e/e}^{-1}$ is evidently an e-inner permutation.

This, together with (ii), proves the following: if $(a / e)((e / e) \backslash b) = c$ and if two of the elements a, b, c belong to H, then the third belongs to H, too. As $a * b = (a / e)((e / e) \backslash b)$, this means that H is a subloop of $Q(*, /\!\!/, \backslash\!\!\backslash)$.

The associated group of the loop $Q(*, /\!\!/, \backslash\!\!\backslash)$ is contained in the associated group of $Q(\cdot, /, \backslash)$. Indeed, the left translation $x \mapsto a * x$ of $Q(*, /\!\!/, \backslash\!\!\backslash)$ can be expressed as $L_{a/e} \circ L_{e/e}^{-1}$ and the right translation $x \mapsto x * a$ as $R_{(e/e)a} \circ R_e^{-1}$.

Consequently, any inner permutation of $Q(*, /\!\!/, \backslash\!\!\backslash)$ is an e-inner permutation of $Q(\cdot, /, \backslash)$. From 2.3 it follows that H is a normal subloop of $Q(*, /\!\!/, \backslash\!\!\backslash)$. Denote by $\sim$ the corresponding normal congruence of $Q(*, /\!\!/, \backslash\!\!\backslash)$. We have

$a \sim b \Longleftrightarrow a \backslash\!\!\backslash b \in H \Longleftrightarrow (e / e)((a / e) \backslash b) \in H$.

If $x \in Q$, then $(e / e)x \in H \Longleftrightarrow x \in H$, since $(e / e)x = L_{e/e}(x)$ and $L_{e/e}$ is an e-inner permutation. Consequently,

$$a \sim b \Longleftrightarrow (a / e) \backslash b \in H .$$

Since the e-inner permutation $L_a^{-1} \circ R_e \circ L_{a/e}$ transforms $(a / e) \backslash b$ into $a \backslash be$, we get $a \sim b \Longleftrightarrow a \backslash be \in H$ and consequently $a \sim b \Longleftrightarrow (e / e)(a \backslash be) \in H$. However, $(e / e)(a \backslash be) = ae \backslash\!\!\backslash be = \alpha(a) \backslash\!\!\backslash \alpha(b)$, so that

$$a \sim b \Longleftrightarrow \alpha(a) \sim \alpha(b) .$$

Further, we have

$$a \sim b \Longleftrightarrow a /\!\!/ b \in H \Longleftrightarrow (a / ((e / e) \backslash b))\, e \in H .$$

The e-inner permutation $R_e \circ R_b^{-1} \circ L_{e/e} \circ R_{(e/e)\backslash b} \circ R_e^{-1}$ transforms $(a / ((e / e) \backslash b))e$ into

$$(((e / e)\, a) / b)e = ((e / e)\, a) /\!\!/ ((e / e)\, b) =$$
$$= \beta(a) /\!\!/ \beta(b) \text{ , so that}$$

$$a \sim b \Longleftrightarrow \beta(a) /\!\!/ \beta(b) \in H \Longleftrightarrow \beta(a) \sim \beta(b) .$$

This shows that $\sim$ is a congruence of the algebra $Q(*, /\!\!/, \backslash\!\!\backslash, 1, \alpha, \beta, \gamma, \delta)$. Consequently, the rational equivalence of $\mathcal{K}^*$ and $\mathfrak{M}$ guarantees that $\sim$ is a congruence of the algebra $Q(\,.\,, /, \backslash, e)$ and thus a normal congruence of the quasigroup Q.

If H is a subquasigroup of Q, then clearly (ii) can be omitted. We shall give one more characterization of normal subquasigroups; another proof can be found in [1], too.

2.5. <u>Theorem</u>. Let a quasigroup Q, its subquasigroup H and an element $e \in H$ be given. H is a normal subquasigroup of Q iff $aH \,.\, bH = ((ae \,.\, be) / e)H$ for all $a, b \in Q$.

<u>Proof</u>. Suppose first that H is a block of a normal congruence $\sim$. If $h_1, h_2 \in H$, then

$$ah_1 \,.\, bh_2 \sim ae \,.\, be = ((ae \,.\, be) / e)\, e \in ((ae \,.\, be) / e)\, H .$$

If $h \in H$, then

$$((ae \cdot be) / e)h \sim ((ae \cdot be) / e)e = ae \cdot be \in aH \cdot bH .$$

Suppose now $aH \cdot bH = ((ae \cdot be) / e)H$ for all $a, b \in Q$. As H is a subquasigroup, the condition (ii) of 2.4 is evidently satisfied, so that it is sufficient to verify the condition (i).

We have $Ha = (ea / e)H$. Indeed, if $h \in H$, then $(e / e) \backslash h \in H$, too, so that

$$ha = ((e / e) ((e / e) \backslash h)) ((a / e) e) \in (e / e)H \cdot$$
$$\cdot (a / e)H = (ea / e)H ;$$

conversely, if $h \in H$, then there exists an $h' \in H$ with $((((e / e) e) ((a / e) e)) / e)h = (e / e)h' \cdot (a / e)e$, so that

$$(ea / e)h = (e / e)h' \cdot (a / e)e = (e /e)h' \cdot a \in Ha .$$

This proves $T_a(H) = H$.

We have $a \cdot bH = (a / e)e \cdot bH \subseteq (a / e)H \cdot bH = ((a \cdot be) / e)H$; conversely, if $h \in H$, then there exists an $h' \in H$ with $(((a / e)e \cdot be) / e)h = (a /e)e \cdot bh'$, so that

$$((a \cdot be) / e)h = (a /e)e \cdot bh' = a \cdot bh' \in a \cdot bH .$$

This proves $a \cdot bH = ((a \cdot be) / e)H$, i.e. $L_{a,b}(H) = H$.

We have $Ha \cdot b = (ea / e)H \cdot (b / e)e \subseteq (ea / e)H \cdot (b / e)H = ((ea. b) / e)H = ((e (e \backslash ea. b)) / e)H = H(e \backslash ea \cdot b)$; conversely, if $h \in H$, then there exists

an $h' \in H$ with $((ea \cdot b) / e)h = (ea / e)h' \cdot (b / e)e$,
so that

$$H(e \setminus ea \cdot b) = ((ea \cdot b) / e)H \subseteq (ea / e)H \cdot b = Ha \cdot b .$$

This proves $Ha \cdot b = H(e \setminus ea \cdot b)$, i.e. $R_{a,b}(H) = H$.

This shows that any permutation T_a , T_a^{-1} , $L_{a,b}$, $L_{a,b}^{-1}$, $R_{a,b}$, $R_{a,b}^{-1}$ maps H into H . The same must hold for any composition of these permutations, i.e. (by 2.2) for aby e-inner permutation of Q .

References:

[1] V.D. BELOUSOV: Osnovy teorii kvazigrupp i lup, Moskva, Nauka 1967.

[2] R.H. BRUCK: A survey of binary systems, Springer-Verlag 1966.

[3] G.N. GARRISON: Note on invariant complexes of a quasigroup, Ann.of Math.47(1946),50-55.

[4] J. JEŽEK and T. KEPKA: Quasigroups, isotopic to a group, Comment.Math.Univ. Carolinae 16(1975),59-76.

Matematicko-fyzikální fakulta
Karlova universita
Sokolovská 83, 18600 Praha 8
Československo

(Oblatum 17.12.1974)