

CONGRUENCES AND FINITE QUASIGROUPS

Proposition 1 *Let Q be a quasigroup. An equivalence \sim on Q is a congruence if and only if for all $x, y, z \in Q$*

$$x \sim y \Rightarrow xz \sim yz, zx \sim zy, x/z \sim y/z \text{ and } z \setminus x = z \setminus y.$$

Proof. If $*$ is a binary operation on Q , then \sim is compatible with $*$ if and only if $x \sim y \Rightarrow x * z \sim y * z$ and $z * x \sim z * y$ holds for all $x, y, z \in Q$. To see that this is true consider $a, b, c, d \in Q$ such that $a \sim b$ and $c \sim d$. If the implication holds for all $x, y, z \in Q$, then $a * c \sim b * c \sim b * d$.

Due to this fact the proof may be restricted to verifying implications $x \sim y \Rightarrow z/x \sim z/y$ and $x \sim y \Rightarrow x \setminus z \sim y \setminus z$. It is enough to prove the latter implication because of mirror symmetry. Before doing so let us observe that all implications assumed may be considered as equivalences. E.g., we have $x \sim y \Leftrightarrow xz \sim yz$. To prove the converse direction suppose that $xz \sim yz$. By the assumptions of the statement $(xz)/z \sim (yz)/z$. However $(xz)/z = x$ and $(yz)/z = y$. Similarly in the other cases.

Thus $x \setminus z \sim y \setminus z \Leftrightarrow z \sim x(y \setminus z) \Leftrightarrow z/(y \setminus z) \sim (x(y \setminus z))/(y \setminus z)$. Now, $z/(y \setminus z) = y$ and $x(y \setminus z)/(y \setminus z) = x$. □

Proposition 2. *If Q is a finite quasigroup, then a subset closed under multiplication is a subquasigroup and an equivalence compatible with \cdot is a congruence of the quasigroup.*

Proof. Let $S \subseteq Q$ be closed under multiplication. This means that if $i \geq 1$ and $s, t \in S$, then $L_s^i(t) \in S$ and $R_s^i(t) \in S$. To see that S is a subquasigroup we have to show that $L_s^{-1}(t) = s \setminus t$ and $R_s^{-1}(t) = t/s$ belong to S too. Since L_s and R_s are of finite order there exist $i, j \geq 1$ such that $L_s^i = L_s^{-1}$ and $R_s^j = R_s^{-1}$.

Let now \sim be an equivalence compatible with multiplication. If $x \sim y$ then $L_z^i(x) \sim L_z^i(y)$ and $R_z^i(x) \sim R_z^i(y)$ for all $z \in Q$ and $i \geq 1$. In view of Proposition 1 we may proceed like in the first part of this proof.

Another option how to show that an equivalence compatible with \cdot is a congruence, is to use the fact an equivalence is a congruence if and only if the equivalence is a subalgebra if considered as a subset of the square. □