CERTAIN CONGRUENCES ON QUASIGROUPS

H. A. THURSTON

1. Using the ideas of [1],1 we define a lattice-isomorphism between the reversible congruences on a quasigroup and certain congruences on its group of translations. This may be used to get certain properties of the quasigroup congruences from those of the translation-group congruences; for example, it gives a new proof that reversible congruences on a quasigroup are permutable (a proof of this has been given in [3]).

NOTATION. A relation $\theta$ in a set $S$ is a set of ordered 2-sets of elements of $S$. If $(a, b) \in \theta$, we say “$a$ is in the relation $\theta$ to $b$”; the shorter notation $ab\theta$ will sometimes be used for this. For example, a mapping $x \rightarrow x\theta$ may be taken to be the set of all $(x, x\theta)$ and is then a relation in this sense.

$\theta^{-1}$ is the set of all $(a, b)$ for which $b\theta a$.

$\theta\phi$ is the set of all $(a, b)$ for which $ab\phi b$ for some $c$.

Clearly $\theta^{-1}$ and $\theta\phi$ are relations in $S$ if $\theta$ and $\phi$ are.

If $q$ is an equivalence (that is, if $q^{-1} = qq = q$), then $aq$ is the set of all elements in the relation $q$ to $a$.

2. Given a quasigroup whose set of elements is $S$ it is possible to give definitions2 of two operations / and \:

$a/b$ is the $x$ for which $x \cdot b = a$.

$a\backslash b$ is the $x$ for which $ax = b$.

Clearly

(1) $$(a/b) \cdot b = a, \quad a \cdot (a\backslash b) = b, \quad (a/b)/b = a, \quad a\backslash (a \cdot b) = b.$$ 

On the other hand, if we have an algebra $E$ whose set of elements is $S$, whose operations are $\cdot$, $/$, and $\backslash$, and for which (1) is true, then the algebra $S$ with the operation $\cdot$ and elements $S$ is a quasigroup. $E$ is equationally defined: it might possibly be named an equasigroup.

3. DEFINITION. A congruence $q$ on a quasigroup is reversible if (i) $aqb$ whenever $acqbc$ and (ii) $aq\phi$ whenever $caqcb$. Clearly a congruence on $S$ is reversible if and only if it is a congruence on $E$. Equally clearly, $S/q$ is a quasigroup under the Kronecker operation $\cdot$ if and only if $q$ is reversible. (The reversible property is needed for cancellation to be possible.)

Received by the editors November 6, 1950 and, in revised form, February 27, 1951.

1 Numbers in brackets refer to the bibliography at the end of the paper.

2 The notation is from [2].
4. Definitions. $\rho_a$ is the mapping $x \to x \cdot a$, and $\lambda_a$ is $x \to a \cdot x$. The translator, $\Sigma$, of $S$ (or of $E$) is the group generated by all $\rho_a$ and $\lambda_a$ for all $a$ of $S$, and is a permutation group on $S$.

5. Now we give a relation between congruences on $E$ and congruences on $\Sigma$. Clearly an equivalence $q$ on $S$ is a congruence on $E$ if and only if $x\sigma y \equiv q$ whenever $x\gamma y$ and $\sigma \in \Sigma$; that is, if and only if $\sigma^{-1}q\sigma \leq q$ for every $\sigma$ of $\Sigma$. From now on the letter $q$ will be used only for congruences on $E$.

Definition. $q^t$ is the relation in $\Sigma$ for which $\theta q^t \phi$ if and only if $\theta^{-1}q\sigma < q$. If $\sigma \in \Sigma$, then $x\gamma (x\sigma)y$ is a mapping, $\xi$, say, of $S/\gamma$ into $S/\gamma$. For if $x\gamma y$, then $x\gamma y$. Therefore $x\sigma y \equiv q$ and so $x\sigma y \equiv y\sigma q$. The mapping $\sigma \to \xi$ is a homomorphism (that is, $\sigma \tau \to \xi \tau$) and $q^t$ is its kernel. Therefore $q^t$ is a congruence on $\Sigma$.

Note. Clearly $q^t \supseteq p^t$ if $q \supseteq p$.

6. From now on the letter $p$ will be used only for congruences on $\Sigma$.

Definition. $p^t$ is $\cup \theta^{-1}\phi$ (over all $\theta$, $\phi$ for which $6p$).

It is not hard to see that $p^t$ is a congruence on $E$. For (i) clearly $p^t = (p^t)^{-1}$. (ii) Let $(a, b) \in (p^t)^2$. Then, for some $c$, $a \rho_t c \rho b$. Therefore $a\theta^{-1}\phi c$ and $c \psi^{-1}b$, where $\theta \rho b$ and $\psi \rho c$. Then $a\theta^{-1} \phi = c = b\chi^{-1} \psi$ and so $(a, b) \in \theta^{-1}\phi \psi^{-1} \chi = (\theta^{-1}\Phi)(\psi^{-1} \chi)$. But $\phi^{-1} \psi \rho \phi^{-1} = 1 = \psi^{-1} \rho \rho \psi^{-1} \chi$. Therefore $a\rho b$ and so $(p^t)^2 \subseteq p^t$. (iii) Let $(a, b) \in \sigma^{-1}p^t \sigma$ where $\sigma \in \Sigma$. Then

\[(a, b) \in \sigma^{-1}p^t \sigma \quad (\text{where } \theta \rho \phi) \]
\[= (\sigma \theta)^{-1}(\phi \sigma) \quad (\text{where } (\theta \rho \phi)(\phi \sigma)) \]
\[\subseteq p^t. \]

Note. Clearly $p^t \supseteq q^t$ if $p \supseteq q$.

7. $p \supseteq q^t$ if and only if $p^t \subseteq q$. For, by the definition of $q^t$, $p \subseteq q^t$ if and only if (i) $\theta^{-1}q \subseteq q$ whenever $\theta \rho b$. And (i) is true, by the definition of $p^t$, if and only if $p^t \subseteq q$. Then if $p = q$ we have $p^t \subseteq q$, that is $q^t \subseteq q$. On the other hand, if $a \in b$, let $u$ be any element of $S$ and put $a = u\lambda_a$, $b = u\lambda_a$. Then $v \in w$ (because $q$ is reversible), and so, for any $x$ of $S$, $x\lambda_a \rho x\lambda_a$. Therefore $\lambda_a^{-1} \lambda_a \subseteq q$, and so $\lambda_a \rho \lambda_a$. But $(a, b) = (u\lambda_a, u\lambda_a) \rho \lambda_a \subseteq \lambda_a^{-1} \lambda_a$. Therefore $a \in b$. Therefore $q^t \supseteq q$ and so $q = q^t$. Therefore $\tau$ is a one-to-one mapping of the set of all congruences on $E$ into the set of congruences on $\Sigma$, and $\tau = (\tau)^{-1}$. By notes 5 and 6, this mapping is an isomorphism between the lattice of congruences on $E$ and a sublattice of the lattice of congruences on $\Sigma$.

8. Any two congruences on $E$ are permutable. Let $p$ and $r$ be any
two congruences on $\mathcal{E}$. Any congruence on a group is given by a normal subgroup: let the congruences $\mathbf{p}$ and $\mathbf{r}$ be given by subgroups $\Pi$ and $\Phi$. Then, for every $a$ of $S$, $a\mathbf{p} = a\Pi$. For if $b \in a\mathbf{p}$, let $u, v,$ and $w$ be as in §7. Then $b = a\lambda_v^{-1}\lambda_u$ where $\lambda_v^{-1}\lambda_u \in \Pi$. Therefore $a\mathbf{p} \subseteq a\Pi$. On the other hand, if $b \in a\Pi$, then $b = a\theta$ where $\theta \in \Pi$ and so $\theta \mathbf{p}^\dagger$. Then $a\theta \mathbf{p}a$; that is, $b\mathbf{p}a$, and so $b \in a\mathbf{p}$. Therefore $a\Pi \subseteq a\mathbf{p}$, and so $a\Pi = a\mathbf{p}$. In the same way, $a\mathbf{r} = a\mathbf{r}$.

Now, if $a\mathbf{p}b$, then for some $c$, $a \in c\mathbf{p} = c\Pi$ and $c \in b\mathbf{r} = b\Phi$. Therefore $a \in b\Pi = b\Phi$. We may now let $a = b\theta \phi$ where $\theta \in \Pi$ and $\phi \in \Phi$. Then $a \mathbf{r} b\theta$. But $b\mathbf{p} b\theta$. Therefore $a \mathbf{r} b$. Therefore $a \mathbf{p} b$. Therefore $a \mathbf{p} \subseteq a \mathbf{r}$; that is, $\mathbf{p}$ and $\mathbf{r}$ are permutative.

9. An important point about this is that proofs have been given (for example, in [4, pp. 87–89]) of the Schreier-Zassenhaus theorem for algebras all of whose congruences are permutative and which have a one-element subalgebra. An equasigroup has not, in general, a one-element subalgebra, but the theorem is true in this form:

If $E, A_1, \ldots, A_m$ and $E, B_1, \ldots, B_n$ are normal series of an equasigroup $E$, and if $A_m \cap B_n \neq \emptyset$, then the series have isomorphic refinements.

**BIBLIOGRAPHY**


**UNIVERSITY OF BRISTOL**