CERTAIN CONGRUENCES ON QUASIGROUPS

H. A. THURSTON

1. Using the ideas of [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 $a\theta b$ will sometimes be used for this. For example, a mapping $x \to x\theta$ 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 $a\theta c\phi b$ for some $c$.
Clearly $\theta^{-1}$ and $\theta\phi$ are relations in $S$ if $\theta$ and $\phi$ are.

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

2. Given a quasigroup whose set of elements is $S$ it is possible to give definitions of two operations / and \: $a/b$ is the $x$ for which $x \cdot b = a$.
$a\backslash b$ is the $x$ for which $a \cdot x = b$.

Clearly

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

On the other hand, if we have an algebra $E$ whose set of elements is $S$, whose operations are $\cdot$, /, and \, 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 $\phi$ on a quasigroup is reversible if (i) $a\phi b$ whenever $a\phi b c \phi d c$ and (ii) $a\phi b$ whenever $a\phi c b$. Clearly a congruence on $S$ is reversible if and only if it is a congruence on $E$. Equally clearly, $S/\phi$ is a quasigroup under the Kronecker operation $\cdot$ if and only if $\phi$ 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.** \( \rho_s \) is the mapping \( x \mapsto x \cdot a \), and \( \lambda_s \) is \( x \mapsto a \cdot x \). The *translator*, \( \Sigma \), of \( S \) (or of \( E \)) is the group generated by all \( \rho_s \) and \( \lambda_s \) 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 \( x \sigma y \) whenever \( x \alpha y \) and \( \sigma \in \Sigma \); that is, if and only if \( \sigma^{-1} q \sigma \subseteq q \) 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 \( \theta q \phi \).

If \( \sigma \in \Sigma \), then \( x \sigma \rightarrow (x \sigma)q \) is a mapping, \( \delta \) say, of \( S/q \) into \( S/q \). For if \( xq = yq \), then \( x \sigma y \). Therefore \( x \sigma y \) and so \( x \sigma q = y \sigma q \). The mapping \( \sigma \rightarrow \delta \) is a homomorphism (that is, \( \sigma \rightarrow \delta \tau \)) 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 \( U \theta^{-1} \phi \) (over all \( \theta, \phi \) for which \( \theta \phi \)).

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 \( c, \ a p^t c b \). Therefore \( a \theta^{-1} \phi c \) and \( c \psi^{-1} b \), where \( \theta \phi \) and \( \psi \chi \). Then \( a \theta^{-1} \phi \chi = c = b \chi^{-1} \psi \) and so \( (a, b) \in (\theta \psi^{-1} \phi; \chi = (\theta^{-1} \phi)^{-1} \psi^{-1} \chi) \). But \( \theta \phi \psi^{-1} \phi = \psi^{-1} \psi \psi^{-1} \chi \). Therefore \( a p^t b \), and so \( (p^t)^2 \subseteq p^t \).

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

**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 \( q^t \), \( p \supseteq q^t \) if and only if (i) \( \theta^{-1} \phi \subseteq q \) whenever \( \theta \phi \). And (i) is true, by the definition of \( p^t \), if and only if \( p^t \subseteq q \). Then if \( p = q^t \) we have \( p^t \subseteq q \), that is \( q^t \subseteq q \). On the other hand, if \( a \phi b \), let \( u \) be any element of \( S \) and put \( a = u \lambda_w \), \( b = u \lambda_u \). Then \( vqw \) (because \( q \) is reversible), and so, for any \( x \) of \( S \), \( x \lambda_q x \lambda_w \). Therefore \( \lambda_q \lambda_w \subseteq q \), and so \( \lambda_q \lambda_w \subseteq q \). But \( (a, b) = (u \lambda_w, u \lambda_u) \subseteq \lambda_q \lambda_w \). Therefore \( aq^t b \). Therefore \( q^t \supseteq q \) and so \( q = q^t \).

Therefore \( \dagger \) is a one-to-one mapping of the set of all congruences on \( E \) into the set of congruences on \( \Sigma \), and \( \dagger \) is \( (\dagger)^{-1} \). 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 \( E \). Any congruence on a group is given by a normal subgroup: let the congruences \( \eta \) and \( \tau \) be given by subgroups \( \Pi \) and \( P \). Then, for every \( a \) of \( S \), \( ap = a\Pi \). For if \( b \in ap \), let \( u \), \( v \), and \( w \) be as in §7. Then \( b = a\lambda_1^{-1}\lambda_v \) where \( \lambda_1^{-1}\lambda_v \in \Pi \). Therefore \( ap \subseteq a\Pi \). On the other hand, if \( b \in a\Pi \), then \( b = a\theta \) where \( \theta \in \Pi \) and so \( \theta \eta \). Then \( ab = a\eta \); that is, \( b\eta \), and so \( b \in ap \). Therefore \( a\Pi \subseteq ap \), and so \( a\Pi = ap \). In the same way, \( a\Pi = ap \).

Now, if \( aprb \), then for some \( c \), \( a \in c\Pi \) and \( c \in b\tau \). Therefore \( a \in b\Pi \tau = b\Pi \). We may now let \( a = b\phi \) where \( \theta \subseteq \Pi \) and \( \phi \subseteq P \). Then \( a \tau b \theta \). But \( b\eta b \theta \). Therefore \( aprb \). Therefore \( \eta \tau \subseteq \eta \tau \); that is, \( \tau \) and \( \tau \) are permutable.

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 permutable 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