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 θ 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 θ to b"; the shorter notation $a\theta b$ 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.

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

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

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

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

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

Clearly

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

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

3. DEFINITION. A congruence $\mathfrak{q}$ on a quasigroup is *reversible* if (i) $a\mathfrak{q}b$ whenever $ac\mathfrak{q}bc$ and (ii) $a\mathfrak{q}b$ whenever $ca\mathfrak{q}cb$. Clearly a congruence on $\mathfrak{S}$ is reversible if and only if it is a congruence on $\mathcal{E}$. Equally clearly, $S/\mathfrak{q}$ is a quasigroup under the Kronecker operation $\cdot$ if and only if $\mathfrak{q}$ 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. ρ_a is the mapping $x \to x \cdot a$, and λ_a is $x \to a \cdot x$. The *translator*, Σ, of $\mathfrak{S}$ (or of $\mathcal{E}$) is the group generated by all ρ_a and λ_a for all a of S, and is a permutation group on S.

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

DEFINITION. $\mathfrak{q}^\dagger$ is the relation in Σ for which $\theta\mathfrak{q}^\dagger\phi$ if and only if $\theta^{-1}\phi \subseteq \mathfrak{q}$.

If $\sigma \in \Sigma$, then $x\mathfrak{q} \to (x\sigma)\mathfrak{q}$ is a mapping, $\bar{\sigma}$ say, of $S/\mathfrak{q}$ into $S/\mathfrak{q}$. For if $x\mathfrak{q} = y\mathfrak{q}$, then $x\mathfrak{q}y$. Therefore $x\sigma\mathfrak{q}y\sigma$ and so $x\sigma\mathfrak{q} = y\sigma\mathfrak{q}$. The mapping $\sigma \to \bar{\sigma}$ is a homomorphism (that is, $\sigma\tau \to \bar{\sigma}\bar{\tau}$) and $\mathfrak{q}^\dagger$ is its kernel. Therefore $\mathfrak{q}^\dagger$ *is a congruence on* Σ.

NOTE. Clearly $\mathfrak{q}^\dagger \supseteq \mathfrak{p}^\dagger$ if $\mathfrak{q} \supseteq \mathfrak{p}$.

6. From now on the letter $\boldsymbol{p}$ will be used only for congruences on Σ.

DEFINITION. $\boldsymbol{p}^\downarrow$ is $\bigcup \theta^{-1}\phi$ (over all θ, ϕ for which $\theta\boldsymbol{p}\phi$).

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

(iii) Let $(a, b) \in \sigma^{-1}\boldsymbol{p}^\downarrow\sigma$ where $\sigma \in \Sigma$. Then

$$\begin{aligned} (a, b) &\in \sigma^{-1}\theta^{-1}\phi\sigma && \text{(where } \theta\boldsymbol{p}\phi) \\ &= (\theta\sigma)^{-1}(\phi\sigma) && \text{(where } (\theta\sigma)\boldsymbol{p}(\phi\sigma)) \\ &\subseteq \boldsymbol{p}^\downarrow. \end{aligned}$$

NOTE. Clearly $\boldsymbol{p}^\downarrow \supseteq \boldsymbol{q}^\downarrow$ if $\boldsymbol{p} \supset \boldsymbol{q}$.

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

8. *Any two congruences on* $\mathcal{E}$ *are permutable.* Let $\mathfrak{p}$ and $\mathfrak{r}$ be any

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

Now, if $a\mathfrak{p}\mathfrak{r}b$, then for some c, $a\in qc\mathfrak{p}=c\Pi$ and $c\in b\mathfrak{r}=b\mathrm{P}$. Therefore $a\in b\mathrm{P}\Pi=b\Pi\mathrm{P}$. We may now let $a=b\theta\phi$ where $\theta\in\Pi$ and $\phi\in\mathrm{P}$. Then $a\mathfrak{r}b\theta$. But $b\mathfrak{p}b\theta$. Therefore $a\mathfrak{r}\mathfrak{p}b$. Therefore $\mathfrak{p}\mathfrak{r}\subseteq\mathfrak{r}\mathfrak{p}$; that is, $\mathfrak{p}$ and $\mathfrak{r}$ 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 $E, A_1, \cdots, A_m$ and $E, B_1, \cdots, B_n$ are normal series of an equasigroup E, and if $A_m \cap B_n \neq \varnothing$, then the series have isomorphic refinements.

Bibliography

1. A. A. Albert, *Quasigroups*. I, Trans. Amer. Math. Soc. vol. 54 (1943) p. 507.

2. T. Evans, *Homomorphisms of non-associative systems*, J. London Math. Soc. vol. 24 (1949) p. 254.

3. G. Trevisan, *A proposito delle relazioni di congruenza sui quasi-gruppi*, Rendiconti del Seminario Matematico della Università di Padova vol. 19 (1950) pp. 367–370.

4. G. Birkhoff, *Lattice theory*, Amer. Math. Soc. Colloquium Publications, vol. 25, rev. ed., 1948.

University of Bristol