NONCOMMUTING QUASIGROUP CONGRUENCES

H. A. THURSTON

1. The purpose of this paper is to exhibit a quasigroup with two noncommuting congruences on it. The quasigroup is in fact the free equationally-defined commutative quasigroup generated by four elements, and I shall use the construction devised by G. E. Bates and F. Kiokemeister, Bull. Amer. Math. Soc. vol. 54 (1948) p. 1180.

2. Definition. A set $S$ of elements such that to each of certain pairs $a, b$ of elements there corresponds a uniquely-defined product $ab$ in $S$ and such that if $ab$ is defined then so is $ba$ and is equal to it is a partial commutative groupoid. The identity $xy = yx$ will be implicitly assumed; e.g. if I define $pq$, then $qp$ is to be defined as the same element, even if this is not explicitly mentioned.

3. Definition. $T$ is the extension of a partial commutative groupoid $S$ if $T$ consists of the elements of $S$, together with an element $a \times b$ for each pair $a, b$ for which $ab$ is not defined in $S$ and an element $a/b$ for each ordered pair $a, b$ for which $bx = a$ is not solvable in $S$, $a \times b$ being equal to $b \times a$, but all other elements being distinct. Multiplication is defined in $T$ as follows: if $ab$ is defined in $S$, then it is defined in $T$ to be the same element; if $ab$ is not defined in $S$, then $ab$ is defined in $T$ to be $a \times b$; and for each $a/b$ defined as above $(a/b)b = a$. All other products in $T$ are undefined.

4. Let $J_0$ be a commutative partial groupoid in which no products are defined. For each $i$, let $J_{i+1}$ be the extension of $J_i$, and let $M$ be $\bigcup_{i \geq 0} J_i$. Then $M$ is a commutative quasigroup (op. cit. Corollary 2).

Definition. The rank, $R_x$, of an element $x$ of $M$ is the suffix of the first $J_i$ to which $x$ belongs.

(We could complete the definition of division as an operation on $M$ by putting $(xy)/y$ equal to $x$. If we do this we see that the algebra we have defined is in fact the free equationally-defined quasigroup generated by the elements of $J_0$.)

5. Let $q_i$ be a congruence on $J_i$; that is, an equivalence on $J_i$ such that if $a q a'$ and $b q b'$ and $ab \in J_i$ and $a'b' \in J_i$, then $ab q_i a'b'$. We define $q_{i+1}$ as follows: $x q_{i+1} y$ and $y q_{i+1} x$ if and only if

Received by the editors March 26, 1951 and, in revised form, September 19, 1951.

1 The congruences are quasigroup congruences, not equationally-defined-quasigroup congruences (it is known that any two of the latter commute). (See the last sentence but one of §5.)
(i) $x \equiv y$, 
(ii) $x = y$ ($R_x = i + 1$), 
(iii) $x = a \times b$ and $y = a' \times b'$, where $a \equiv a'$ and $b \equiv b'$, 
(iv) $x = a \times b$ and $y \equiv a' b'$ where $a \equiv a'$ and $b \equiv b'$, 
or
(v) $x \equiv_{i+1} z$ and $y \equiv_{i+1} z'$ via (iv), and $z \equiv q$.

(i) ensures that $\equiv_{i+1} \supseteq \equiv_i$; (ii) ensures that $\equiv_{i+1}$ is on $J_{i+1}$; (iv) gives the conditions under which an element of rank $i + 1$ is equivalent to one of lower rank; and (v) says that two elements of rank $i + 1$ which are equivalent to two equivalent elements in $J_i$ are equivalent to one another, and so ensures that $\equiv_{i+1}$ is transitive. In fact, $\equiv_{i+1}$ is an equivalence on $J_{i+1}$, and if $a$ and $b$ are in $J_i$, then $a \equiv_{i+1} b$ if and only if $a \equiv_i b$.

$\equiv_{i+1}$ is a congruence. For suppose that $a \equiv_{i+1} a'$, $b \equiv_{i+1} b'$, $ab \in J_{i+1}$, and $a'b' \in J_{i+1}$. If $a, a', b, b' \in J_i$, then $ab \equiv_{i+1} a'b'$; this follows from the fact that $\equiv_i$ is a congruence if $ab$ and $a'b'$ are in $J_i$, from (iii) if neither is in $J_i$, and from (iv) if just one is. Now suppose that $a$ is not in $J_i$. Since $ab$ is in $J_{i+1}$, $a$ must be of the form $c/b$, where $c \in J_i$. $c/b$ is equivalent only to itself, for, of (i) to (v), only (ii) applies to elements of this form. Therefore $a' = c/b$. But $a'b'$ is in $J_{i+1}$. Therefore $b' = b$. Then $ab = c = a'b'$. Similarly we see that $ab \equiv_{i+1} a'b'$ if any other of the elements $a, a', b, b'$ is not in $J_i$.

It follows that if $\equiv_0$ is a congruence on $J_0$ and $\equiv_i$ is defined for each $i > 0$ as above and $q = \bigcup_{i>0} \equiv_i$, then $q$ is a congruence on $M$. It is in fact the least congruence on $M$ for which $a \equiv b$ whenever $a \equiv_0 b$. (It is a congruence for multiplication only, not for division, unless $\equiv_0$ is equality.) Clearly $q \cap (J_i \times J_i) = \equiv_i$.

6. An example will illustrate this definition. Let $J_0$ be $\{\alpha, \beta, \gamma, \delta\}$ and $q_0$ be $\alpha\beta|\gamma\delta$. (This notation means that the $q_0$-classes are $\{\alpha, \beta\}$, $\{\gamma\}$, and $\{\delta\}$.) The columns of the table show the $q$-classes; the rows show the rank of the entry.

<table>
<thead>
<tr>
<th>0</th>
<th>$\alpha, \beta$</th>
<th>$\gamma$</th>
<th>$\delta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>|</td>
<td>|</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$\alpha/\beta$, $\beta/\alpha$, etc.</td>
<td>$(\gamma/\alpha)\beta$, $(\gamma/\beta)\alpha$</td>
<td>|</td>
</tr>
<tr>
<td>3</td>
<td>$\alpha/\alpha\alpha$ etc.</td>
<td>$(\gamma/\alpha\alpha)(\alpha\beta)$ etc.</td>
<td>|</td>
</tr>
<tr>
<td>|</td>
<td>|</td>
<td>|</td>
<td></td>
</tr>
</tbody>
</table>
The process of constructing the table is roughly this: the first row is given. In the second row, no element can go into one of the existing classes, for an element can be equivalent to an element of a previous $J_i$ only via (iv): this requires that the previous element factorizes; but no element of $J_0$ factorizes in $J_0$. The elements $aa$, $a\beta$, and $\beta\beta$ are gathered into one class by (iii), so are $a\gamma$ and $\beta\gamma$, etc. When we come to $J_2$, since $a = (a/\beta)\beta$ we get $(a/\beta)a$ and $(a/\beta)\beta$ in the $q$-class of $a$, and so on.

7. Theorem. Let $a$ etc. be as above, and let $r$ be defined similarly by putting $r_0 = a|\beta|\gamma$. If $a q c r b$ there is a $d$ of rank less than or equal to max $\{R_a, R_b\}$ such that $a q d r b$.

Proof. Let $P_n$ be the statement "If $a$, $b$, and $c$ are in $J_n$ and if $a q c r b$, then $a q d r b$ where $R_d \leq$ max $\{R_a, R_b\}$." $P_n$ may be proved by induction. $P_0$ is clearly true, and so is $P_1$. Let $n > 1$ and suppose $P_m$ true whenever $m < n$. Of all the elements $x$ for which $a q x r b$, let $c$ be one of least rank. If max $\{k_R, k_s, k_e\} < n$, then $P_n$ is true by the induction hypothesis. If $\max \{R_a, R_b\} = n$, then $P_n$ is clearly true. We are left with the case $R_c = n$, $R_a < n$, $R_b < n$.

Then $c$ is equivalent to an element $a$ of lower rank. Therefore, by $\S 5(\text{iii})$, $c = de$ and $a = d' e'$, where $d q_{n-1} d'$ and $e q_{n-1} e'$. Also max $\{R_d, R_e\} = n - 1$, otherwise we would not have $R_c = n$. Similarly $b = d'' e''$, where $d q_{n-1} d''$ and $e q_{n-1} e''$.

Now we apply $P_{n-1}$ to $d'$, $d$, and $d''$. There exists then a $d'''$ in $J_{n-1}$ such that

\[(1) \quad d' q d''' r d'' \quad \text{and} \quad R_{d'''} \leq \max \{R_{d''}, R_{d'''}\}.
\]

Similarly,
\[e' q e''' r e'' \quad \text{and} \quad R_{e'''} \leq \max \{R_{e''}, R_{e'''}\}.
\]

Now $a q d''' e''' r b$. Since $c$ is an element of least rank for which $a q c r b$, we have $R_{d'''}e''' \geq n$, whence clearly $R_{d'''}e''' = n$. Then max $\{R_{d'''}, R_{e'''}\} = n - 1$. Suppose it is $d'''$ which is of rank $n - 1$. Then

<table>
<thead>
<tr>
<th>1</th>
<th>$aa, a\beta, \beta\beta$</th>
<th>$a\gamma, \beta\gamma$</th>
<th>$\ldots$</th>
<th>$a/\alpha$</th>
<th>$\ldots$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
<td>$aa \cdot \alpha, aa \cdot \beta, a\beta \cdot \alpha, \ldots$</td>
<td>$\ldots$</td>
</tr>
<tr>
<td>3</td>
<td>$\frac{aa}{\beta}$ etc.</td>
<td>$\frac{a\gamma}{\beta}$ etc.</td>
<td>$\ldots$</td>
<td>$\frac{a/\alpha}{\beta}$ etc.</td>
<td>$\ldots$</td>
</tr>
</tbody>
</table>

\[\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots\]
\[ n - 1 = R_{d'''} \leq \max \{ R_{d'}, R_{d''} \} \quad \text{(by (1))} \]
\[ \leq n - 1 \quad \text{(because } d' \text{ and } d'' \text{ are in } J_{n-1}). \]

Therefore one of \( d' \), \( d''' \) is of rank \( n - 1 \); suppose it is \( d' \). We have now that \( d'e' \subseteq J_{n-1} \) and \( d' \) is of rank \( n - 1 \). Then we must have \( d' = f/e' \).

We saw in §4 that an element of this form of rank \( n - 1 \) is not equivalent to any other element of \( J_{n-1} \). Therefore \( d' = d'' = d''' = f/e' \), where \( R_f < n - 1 \). Now \( (f/e')e'' = d''e'' \subseteq J_{n-1} \). Therefore \( e' = e'' \). Therefore \( d'e' = d''e'' = f \). Therefore \( a \equiv b \) and \( R_f < n - 1 \). This contradicts the definition of \( c \).

8. In the theorem of §7, put \( a = \delta \) and \( b = (\gamma/\alpha)\beta \). Then \( \max \{ R_a, R_b \} = 2 \). Therefore if there is a \( c \) such that \( a \equiv c \equiv b \), there will be one whose rank is at most 2. Clearly there is no such \( c \).

On the other hand, \( a = \delta \equiv \gamma \equiv q \equiv (\gamma/\alpha)\beta \equiv b \). Therefore \( q \) and \( r \) do not commute.

The theorem of §7 is the application to this problem of a theorem (as yet unpublished) of J. C. Shepherdson.

The reader will notice that \( q \) and \( r \) have an infinite number of infinite congruence classes. This is important. I have just received a proof from S. Abhyankar, Harvard University, of the fact that if \( q \) and \( r \) both fail to have this doubly infinite character, then they commute.

University of Bristol