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[1] 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 $\bigcup_{i>0} J_i$. Then M is a commutative quasigroup (op. cit. Corollary 2).

DEFINITION. The rank, $\mathfrak{R}_x$, 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 $\mathfrak{q}_i$ be a congruence on J_i; that is, an equivalence on J_i such that if $a\ \mathfrak{q}\ a'$ and $b\ \mathfrak{q}\ b'$ and $ab\in J_i$ and $a'b'\in J_i$, then $ab\ \mathfrak{q}_i\ a'b'$. We define $\mathfrak{q}_{i+1}$ as follows: $x\ \mathfrak{q}_{i+1}\ y$ and $y\ \mathfrak{q}_{i+1}\ x$ 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) $x\ \mathfrak{q}_i\ y$,
(ii) $x=y$ ($\mathfrak{R}_x=i+1$),
(iii) $x=a\times b$ and $y=a'\times b'$, where $a\ \mathfrak{q}_i\ a'$ and $b\ \mathfrak{q}_i\ b'$,
(iv) $x=a\times b$ and $y\ \mathfrak{q}_i\ a'b'$ where $a\ \mathfrak{q}_i\ a'$ and $b\ \mathfrak{q}_i\ b'$,

or

(v) $x\ \mathfrak{q}_{i+1}\ z$ and $y\ \mathfrak{q}_{i+1}\ z'$ via (iv), and $z\ \mathfrak{q}_i\ z'$.

(i) ensures that $\mathfrak{q}_{i+1}\supseteq\mathfrak{q}_i$; (ii) ensures that $\mathfrak{q}_{i+1}$ 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 $\mathfrak{q}_{i+1}$ is transitive. In fact, $\mathfrak{q}_{i+1}$ is an equivalence on J_{i+1}, and if a and b are in J_i, then $a\ \mathfrak{q}_{i+1}\ b$ if and only if $a\ \mathfrak{q}_i\ b$.

$\mathfrak{q}_{i+1}$ is a congruence. For suppose that $a\ \mathfrak{q}_{i+1}\ a'$, $b\ \mathfrak{q}_{i+1}\ b'$, $ab\in J_{i+1}$, and $a'b'\in J_{i+1}$. If $a, a', b, b'\in J_i$, then $ab\ \mathfrak{q}_{i+1}\ a'b'$; this follows from the fact that $\mathfrak{q}_i$ 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 $ab\ \mathfrak{q}_{i+1}\ a'b'$ if any other of the elements a, a', b, b' is not in J_i.

It follows that if $\mathfrak{q}_0$ is a congruence on J_0 and q_i is defined for each $i>0$ as above and $\mathfrak{q}=\bigcup_{i>0}\mathfrak{q}_i$, then q is a congruence on M. It is in fact the least congruence on M for which $a\ \mathfrak{q}\ b$ whenever $a\ \mathfrak{q}_0\ b$. (It is a congruence for multiplication only, not for division, unless $\mathfrak{q}_0$ is equality.) Clearly $\mathfrak{q}\cap(J_i\times J_i)=\mathfrak{q}_i$.

6. An example will illustrate this definition. Let J_0 be $\{\alpha, \beta, \gamma, \delta\}$ and $\mathfrak{q}_0$ be $\alpha\beta|\gamma|\delta$. (This notation means that the $\mathfrak{q}_0$-classes are $\{\alpha, \beta\}$, $\{\gamma\}$, and $\{\delta\}$.) The columns of the table show the $\mathfrak{q}$-classes; the rows show the rank of the entry.

0	α, β	γ	δ
1			
2	$(\alpha/\beta)\alpha$, $(\beta/\alpha)\beta$, etc.	$(\gamma/\alpha)\beta$, $(\gamma/\beta)\alpha$	as γ
3	$(\alpha/\alpha\alpha)(\alpha\beta)$ etc.	$(\gamma/\alpha\alpha)(\alpha\beta)$ etc.	
	$\vdots$	$\vdots$	$\vdots$

1	$\alpha\alpha, \alpha\beta, \beta\beta$	$\alpha\gamma, \beta\gamma$	$\cdots$	α/α	$\cdots$		
2						$\alpha\alpha\cdot\alpha, \alpha\alpha\cdot\beta, \alpha\beta\cdot\alpha$, etc.	$\cdots$
3	$\frac{\alpha\alpha}{\beta}\alpha$ etc.	$\frac{\alpha\gamma}{\beta}\alpha$ etc.	$\cdots$	$\frac{\alpha/\alpha}{\alpha}\beta$ etc.	$\cdots$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

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 $\alpha\alpha$, $\alpha\beta$, and $\beta\beta$ are gathered into one class by (iii), so are $\alpha\gamma$ and $\beta\gamma$, etc. When we come to J_2, since $\alpha=(\alpha/\alpha)\alpha=(\alpha/\beta)\beta$ we get $(\alpha/\beta)\alpha$ and $(\alpha/\alpha)\beta$ in the $\mathfrak{q}$-class of α, and so on.

7. THEOREM. *Let* $\mathfrak{q}$ *etc. be as above, and let* $\mathfrak{r}$ *be defined similarly by putting* $\mathfrak{r}_0=\alpha|\beta|\gamma\delta$. *If* $a\ \mathfrak{q}\ c\ \mathfrak{r}\ b$ *there is a* d *of rank less than or equal to* $\max\{\mathcal{R}_a, \mathcal{R}_b\}$ *such that* $a\ \mathfrak{q}\ d\ \mathfrak{r}\ b$.

PROOF. Let $\mathcal{P}_n$ be the statement "If a, b, and c are in J_n and if $a\ \mathfrak{q}\ c\ \mathfrak{r}\ b$, then $a\ \mathfrak{q}\ d\ \mathfrak{r}\ b$ where $\mathcal{R}_d\leqq\max\{\mathcal{R}_a, \mathcal{R}_b\}$." $\mathcal{P}_n$ may be proved by induction. $\mathcal{P}_0$ is clearly true, and so is $\mathcal{P}_1$. Let $n>1$ and suppose $\mathcal{P}_m$ true whenever $m<n$. Of all the elements x for which $a\ \mathfrak{q}\ x\ \mathfrak{r}\ b$, let c be one of least rank. If $\max\{\mathcal{R}_a, \mathcal{R}_b, \mathcal{R}_c\}<n$, then $\mathcal{P}_n$ is true by the induction hypothesis. If $\max\{\mathcal{R}_a, \mathcal{R}_b\}=n$, then $\mathcal{P}_n$ is clearly true. We are left with the case $\mathcal{R}_c=n$, $\mathcal{R}_a<n$, $\mathcal{R}_b<n$.

Then c is equivalent to an element a of lower rank. Therefore, by §5(iii), $c=de$ and $a=d'e'$, where $d\ \mathfrak{q}_{n-1}\ d'$ and $e\ \mathfrak{q}_{n-1}\ e'$. Also $\max\{\mathcal{R}_d, \mathcal{R}_e\}=n-1$, otherwise we would not have $\mathcal{R}_c=n$. Similarly $b=d''e''$, where $d\ \mathfrak{r}_{n-1}\ d''$ and $e\ \mathfrak{r}_{n-1}\ e''$.

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

$$d'\ \mathfrak{q}\ d'''\ \mathfrak{r}\ d'' \text{ and } \mathcal{R}_{d'''}\leqq\max\{\mathcal{R}_{d'}, \mathcal{R}_{d''}\}. \tag{1}$$

Similarly,

$$e'\ \mathfrak{q}\ e'''\ \mathfrak{r}\ e'' \text{ and } \mathcal{R}_{e'''}\leqq\max\{\mathcal{R}_{e'}, \mathcal{R}_{e''}\}.$$

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

$$n-1 = \mathfrak{R}_{d'''} \leqq \max\{\mathfrak{R}_{d'}, \mathfrak{R}_{d''}\} \qquad \text{(by (1))}$$
$$\leqq n-1 \qquad \text{(because } d' \text{ and } d'' \text{ are in } J_{n-1}\text{)}.$$

Therefore one of d', d'' is of rank $n-1$; suppose it is d'. We have now that $d'e' \in J_{n-1}$ 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 $\mathfrak{R}_f < n-1$. Now $(f/e')e'' = d''e'' \in J_{n-1}$. Therefore $e' = e''$. Therefore $d'e' = d''e'' = f$. Therefore $a \; \mathfrak{q} \; f \; \mathfrak{r} \; b$ and $\mathfrak{R}_f < n-1$. This contradicts the definition of c.

8. In the theorem of §7, put $a = \delta$ and $b = (\gamma/\alpha)\beta$. Then $\max\{\mathfrak{R}_a, \mathfrak{R}_b\} = 2$. Therefore if there is a c such that $a \; \mathfrak{q} \; c \; \mathfrak{r} \; b$, there will be one whose rank is at most 2. Clearly there is no such c.

On the other hand, $a = \delta \; \mathfrak{r} \; \gamma \; \mathfrak{q} \; (\gamma/\alpha)\beta = b$. Therefore $\mathfrak{q}$ and $\mathfrak{r}$ 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 $\mathfrak{q}$ and $\mathfrak{r}$ 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 $\mathfrak{q}$ and $\mathfrak{r}$ both fail to have this doubly infinite character, then they commute.

UNIVERSITY OF BRISTOL