

FREE PQ-ALGEBRAS

PIERRE ANTOINE GRILLET

By a PQ (product-quotients) algebra, we mean a non-empty set \mathcal{A} together with three single-valued and not necessarily associative operations $\cdot, /, \backslash$ that we shall treat as product, right quotient, and left quotient although we require no relation between them. The theory of binary systems provides the following examples:

A. \mathcal{A} is the set of all subsets of a groupoid G (which may be a semigroup) with the operations defined by:

$$\begin{aligned} A \cdot B &= AB = \{ab; a \in A, b \in B\}, \\ A/B &= A \cdot \cdot B = \{x \in G; Bx \cap A \neq \emptyset\}, \\ A \backslash B &= A \cdot \cdot B = \{x \in G; xA \cap B \neq \emptyset\}. \end{aligned}$$

B. \mathcal{A} is a quasigroup with the operations defined (cf. **1**) by:

$$\begin{aligned} a \cdot b &= ab, \\ a/b &= \text{unique } x \text{ such that } bx = a, \\ a \backslash b &= \text{unique } y \text{ such that } ya = b. \end{aligned}$$

A third example is any residuated groupoid, the quotient operations being then $a/b = a \cdot \cdot b$ and $a \backslash b = b \cdot \cdot a$ (e.g., the set of all ideals of a ring) (cf. **5**).

Our purpose is to study the congruences \mathcal{C} on a groupoid or semigroup or quasigroup G such that G/\mathcal{C} is a commutative and cancellative semigroup (an abelian group if G is a quasigroup). We call such congruences associative, commutative, and cancellative and want to characterize their classes and construct the smallest. The smallest cancellative congruence on a semigroup was first constructed by Lefebvre (**9**). Our construction is completely new and makes use of concepts that we first develop in any free PQ-algebra and later interpret in terms of binary relations on G .

The free PQ-algebra generated by a non-empty set \mathcal{E} is just the set of all (non-empty) words made from the elements of \mathcal{E} and the three operations with a suitable disposition of parentheses. In this algebra we define for each $X \in \mathcal{E}$ a rank function rk_X ($\text{rk}_X P$ is the number of times X appears in P) and a degree function d_X° which is completely determined by the following conditions: $d_X^\circ X = +1$, $d_X^\circ Y = 0$ if $Y \in \mathcal{E}$, $Y \neq X$, and

$$d_X^\circ(P \cdot Q) = d_X^\circ P + d_X^\circ Q, \quad d_X^\circ(P/Q) = d_X^\circ P - d_X^\circ Q = d_X^\circ(Q \backslash P).$$

Received August 23, 1966 and in revised form, December 21, 1967.

If $X \in \mathcal{E}$ and $\mathcal{F} \subseteq \mathcal{E} - \{X\}$, an element P of the algebra is an \mathcal{F} -force element in X if $\text{rk}_X P = 1, d_X^\circ P = +1, d_Y^\circ P = 0$ if $Y \in \mathcal{F}$ and $\text{rk}_Z P = 0$ if $Z \in \mathcal{E} - \mathcal{F} - \{X\}$.

If now G is a groupoid, we have a free PQ-algebra $\overline{\mathcal{A}}$ on $\mathcal{E} \cup \{X\}$, where \mathcal{E} is the set of all subsets of G and X an ‘‘indeterminate.’’ For every $P \in \overline{\mathcal{A}}$, we have a mapping f_P of \mathcal{E} into itself, whose value $f_P(A)$ at A is obtained by replacing X by A and the three operations of $\overline{\mathcal{A}}$ by the corresponding operations described in example A. We also make G a subset of \mathcal{E} by the identification of $\{x\}$ and x for all $x \in G$. Then we prove the following theorems: (1) the smallest associative and cancellative congruence \mathcal{C} on G is the set of all pairs (x, y) such that $y \in f_P(x)$ for some G -force element P in X ; (2) a non-empty subset H of G is a class of some associative, commutative, and cancellative congruence on G if and only if $f_P(H) \subseteq H$ for all P as above.

These results hold *verbatim* if G is a semigroup or a quasigroup. However, any congruence on a semigroup is associative; and we prove that, when G is a quasigroup, one can use the free PQ-algebra generated by $G \cup \{X\}$ (instead of $\overline{\mathcal{A}}$) in the construction of \mathcal{C} and then \mathcal{C} appears as the transitivity equivalence of a canonical group of transformations.

We are glad to express here our gratefulness to Professor Naoki Kimura for the interest he expressed in this work, and to Professor Edwin Clark for many helpful suggestions about the wording of this paper.

1. Free PQ-algebras.

1. Let \mathcal{A} be the free PQ-algebra on the non-empty set \mathcal{E} . If $X \in \mathcal{E}$ and $P \in \mathcal{A}$, $\text{rk}_X P$ denotes the number of times X appears in the word P (cf. introduction). By $\text{rk} P$ we mean $\sum_{X \in \mathcal{E}} \text{rk}_X P$; it is just the length of the word P , a positive integer since the empty word is left out.

Most of the proofs in this section are by induction on the rank, using the following

PROPOSITION 1.1. *Every $P \in \mathcal{A}$ of rank larger than 1 can be written uniquely in exactly one of the forms $Q.R, Q/R, Q \setminus R$. Then $\text{rk}_X P = \text{rk}_X Q + \text{rk}_X R$ for each $X \in \mathcal{E}$ and $\text{rk} P = \text{rk} Q + \text{rk} R$.*

Proof. The expression of P as a word gives immediately the existence of such a decomposition of P ; note that, if it were not unique, then \mathcal{A} would not be free. The assertions on the ranks are obvious.

2. For each $X \in \mathcal{E}$ and $P, Q \in \mathcal{A}$, $P \circ_X Q$ is the word obtained from P by replacing X by Q each time X appears in P . More precisely:

PROPOSITION 1.2. *For every $X \in \mathcal{E}$ and $Q \in \mathcal{A}$ there exists a unique mapping $P \rightarrow P \circ_X Q$ of \mathcal{A} into \mathcal{A} such that:*

- (i) $X \circ_X Q = Q, Y \circ_X Q = Y$ if $Y \in \mathcal{E}, Y \neq X$;

(ii) for every $R, S \in \mathcal{A}$:

$$\begin{aligned} (R.S) \circ_X Q &= (R \circ_X Q) \cdot (S \circ_X Q), \\ (R/S) \circ_X Q &= (R \circ_X Q)/(S \circ_X Q), \\ (R \setminus S) \circ_X Q &= (R \circ_X Q) \setminus (S \circ_X Q). \end{aligned}$$

Proof. By 1.1 the existence and uniqueness of this mapping, postulated when $\text{rk } P = 1$, are immediate by induction on $\text{rk } P$. Observe that (ii) simply means that our mapping is a homomorphism.

Observe also that $P \circ_X Q = P$ whenever $\text{rk}_X P = 0$.

PROPOSITION 1.3. For all $P, Q \in \mathcal{A}$ and $X, Y \in \mathcal{E}$:

$$\begin{aligned} \text{rk}_X (P \circ_X Q) &= \text{rk}_X P \cdot \text{rk}_X Q, \\ \text{rk}_Y (P \circ_X Q) &= \text{rk}_Y P + \text{rk}_X P \text{rk}_Y Q \quad \text{if } Y \neq X. \end{aligned}$$

Proof. By (i) of 1.2, these formulae hold when $\text{rk } P = 1$. If $n \geq 2$ and if they hold when $\text{rk } P < n$, then they hold when $\text{rk } P = n$. Indeed, 1.1 gives $P = R.S$ or R/S or $R \setminus S$, with $\text{rk } R < n, \text{rk } S < n$; then the formulae hold for R and S , hence for P by (ii) of 1.2.

3. Now we define the degree functions.

PROPOSITION 1.4. For each $X \in \mathcal{E}$ there exists a unique mapping d_X° of \mathcal{A} into the set of all integers such that: $d_X^\circ X = +1, d_X^\circ Y = 0$ if $Y \in \mathcal{E} - \{X\}$ and

$$d_X^\circ(P.Q) = d_X^\circ P + d_X^\circ Q, \quad d_X^\circ(P/Q) = d_X^\circ(Q \setminus P) = d_X^\circ P - d_X^\circ Q.$$

Proof. The existence and uniqueness of $d_X^\circ P$ are postulated when $\text{rk } P = 1$, and follow, for all P , from 1.1 and the formulae above by induction on $\text{rk } P$.

PROPOSITION 1.5. $|d_X^\circ P| \leq \text{rk}_X P$ and $d_X^\circ P \equiv \text{rk}_X P \pmod{2}$.

Proof. This is clear when $\text{rk } P = 1$. Assume that it holds for all $S \in \mathcal{A}$ such that $\text{rk } S < n$ (where $n \geq 2$) and that $\text{rk } P = n$. Then $P = Q.R$ or Q/R or $R \setminus Q$ by 1.1 and

$$\begin{aligned} |d_X^\circ P| &= |d_X^\circ Q \pm d_X^\circ R| \leq |d_X^\circ Q| + |d_X^\circ R| \leq \text{rk}_X Q + \text{rk}_X R = \text{rk}_X P, \\ d_X^\circ P &\equiv d_X^\circ Q \pm d_X^\circ R \equiv d_X^\circ Q + d_X^\circ R \equiv \text{rk}_X Q + \text{rk}_X R \equiv \text{rk}_X P \pmod{2} \end{aligned} \quad (2)$$

since $\text{rk } Q < n, \text{rk } R < n$.

PROPOSITION 1.6. For all $P, Q \in \mathcal{A}$ and $X, Y \in \mathcal{E}$:

$$\begin{aligned} d_X^\circ(P \circ_X Q) &= d_X^\circ P \, d_X^\circ Q, \\ d_Y^\circ(P \circ_X Q) &= d_Y^\circ P + d_X^\circ P \, d_Y^\circ Q \quad \text{if } Y \neq X. \end{aligned}$$

Proof. If $\text{rk } P = 1$, then $P \in \mathcal{E}$. If $P \neq X$, then $d_X^\circ P = 0$ and $P \circ_X Q = P$, so that

$$\begin{aligned} d_X^\circ(P \circ_X Q) &= d_X^\circ P = 0 = d_X^\circ P d_X^\circ Q, \\ d_Y^\circ(P \circ_X Q) &= d_Y^\circ P = d_Y^\circ P + d_X^\circ P d_Y^\circ Q \quad \text{if } Y \neq X. \end{aligned}$$

If $P = X$, then $d_X^\circ P = +1$, $P \circ_X Q = Q$, and

$$\begin{aligned} d_X^\circ(P \circ_X Q) &= d_X^\circ Q = d_X^\circ P d_X^\circ Q, \\ d_Y^\circ(P \circ_X Q) &= d_Y^\circ Q = d_Y^\circ P + d_X^\circ P d_Y^\circ Q \quad \text{if } Y \neq X. \end{aligned}$$

Hence the formulae hold whenever $\text{rk } P = 1$.

Assume that they hold for all $T \in \mathcal{A}$ such that $\text{rk } T < n$ (where $n \geq 2$) and suppose $\text{rk } P = n$. Then $P = R.S$ or R/S or $R \setminus S$, where $\text{rk } R < n$, $\text{rk } S < n$. Therefore the formulae hold for R and S ; they hold also for P , by (ii) of 1.2, since they are linear in $(d_X^\circ P, d_Y^\circ P)$. This completes the proof.

4. An element P of \mathcal{A} is *simple* in $X \in \mathcal{E}$ if $\text{rk}_X P = 1$ (i.e., X appears exactly once in P).

PROPOSITION 1.7. *If P is simple in X , then $d_X^\circ P = \pm 1$.*

Proof. This follows from 1.5.

PROPOSITION 1.8. *If P is simple in X , and if X does not appear in Q ($\text{rk}_X Q = 0$), then $P.Q, Q.P, P/Q, Q/P, P \setminus Q, Q \setminus P$ are simple in X .*

Proof. If R denotes any of these six elements, then $\text{rk}_X R = \text{rk}_X P + \text{rk}_X Q = 1 + 0 = 1$, by 1.1.

PROPOSITION 1.9. *If P and Q are both simple in X , so is $P \circ_X Q$.*

Proof. Then $\text{rk}_X (P \circ_X Q) = \text{rk}_X P \text{rk}_X Q = 1$, by 1.3.

5. In this subsection $X \in \mathcal{E}$ is fixed. We define an involution on the set of all elements of \mathcal{A} which are simple in X . (This involution will later correspond to the inversion of bijective mappings, and to the involution for binary relations which sends a binary relation \mathcal{R} onto \mathcal{R}^* defined by: $x \mathcal{R}^* y$ if and only if $y \mathcal{R} x$).

THEOREM 1.10. *There exists a unique mapping $*$ which sends each $P \in \mathcal{A}$ which is simple in X onto some $P^* \in \mathcal{A}$ which is also simple in X , and is such that $X^* = X$ and that, whenever Q is simple in X and X does not appear in R :*

$$\begin{aligned} (Q.R)^* &= Q^* \circ_X (R \setminus X), \\ (R.Q)^* &= Q^* \circ_X (X/R), \\ (Q/R)^* &= Q^* \circ_X (R.X), \\ (R/Q)^* &= Q^* \circ_X (X \setminus R), \\ (Q \setminus R)^* &= Q^* \circ_X (R/X), \\ (R \setminus Q)^* &= Q^* \circ_X (X.R). \end{aligned}$$

Proof. The existence and uniqueness of P^* are postulated when $\text{rk } P = 1$ (whence $P = X$). If they are proved for all $S \in \mathcal{A}$ such that $\text{rk } S < n$ (where $n \geq 2$), which are simple in X , and if $\text{rk } P = n$, then by 1.1 P falls in exactly one of the six cases above, so that P^* is uniquely determined by one of the six formulae; observe that these formulae make P^* simple in X by 1.9, as $R \setminus X, X/R, \dots$ are simple in X by 1.8 and Q^* is simple in X by the induction hypothesis.

PROPOSITION 1.11. *If P and Q are simple in X , then $(P \circ_X Q)^* = Q^* \circ_X P^*$.*

Proof. First note that $P \circ_X Q$ and $Q^* \circ_X P^*$ are both simple in X by 1.9. The proof is now by induction on $\text{rk } P$. If $\text{rk } P = 1$, then $P = X$ and $(P \circ_X Q)^* = Q^* = Q^* \circ_X X$. If the equation holds whenever P is simple in X and $\text{rk } P < n$ (where $n \geq 2$), and if $\text{rk } P = n$, then by 1.1 P falls in exactly one of the six cases of Theorem 1.10. In the first case ($P = R.S, \text{rk}_X S = 0$):

$$\begin{aligned} (P \circ_X Q)^* &= ((R \circ_X Q) \cdot (S \circ_X Q))^* = ((R \circ_X Q) \cdot S)^* \\ &= (R \circ_X Q)^* \circ_X (S \setminus X) = (Q^* \circ_X R^*) \circ_X (S \setminus X) \\ &= Q^* \circ_X (R^* \circ_X (S \setminus X)) = Q^* \circ_X P^*. \end{aligned}$$

The proof is analogous in the other cases.

PROPOSITION 1.12. *If P is simple in $X, P^{**} = P$.*

Proof. This is clear if $\text{rk } P = 1$. If it holds whenever $\text{rk } P < n$ (where $n \geq 2$), and if $\text{rk } P = n$, then P falls in exactly one of the six cases of Theorem 1.10; in the first case ($P = Q.R, \text{rk}_X R = 0$):

$$\begin{aligned} (Q.R)^{**} &= (Q^* \circ_X (R \setminus X))^* = (R \setminus X)^* \circ_X Q^{**} \\ &= (X \circ_X (X.R)) \circ_X Q = (X.R) \circ_X Q = Q.R, \end{aligned}$$

using the induction hypothesis and 1.11. The proof is similar in the other cases.

PROPOSITION 1.13. *If P is simple in X and if $Y \in \mathcal{E}$, then $\text{rk}_Y P^* = \text{rk}_Y P$.*

Proof. If $Y = X$, both ranks are equal to 1. If $Y \neq X$, one proceeds as above, using 1.3. In the first case, for instance:

$$\begin{aligned} \text{rk}_Y (Q.R)^* &= \text{rk}_Y (Q^* \circ_X (R \setminus X)) = \text{rk}_Y Q^* + \text{rk}_X Q^* \text{rk}_Y (R \setminus X) \\ &= \text{rk}_Y Q + \text{rk}_Y R = \text{rk}_Y (Q.R). \end{aligned}$$

PROPOSITION 1.14. *If P is simple in X , then $d_X^\circ P^* = d_X^\circ P$ and $d_Y^\circ P^* = -d_X^\circ P d_Y^\circ P$ whenever $Y \in \mathcal{E}, Y \neq X$.*

Proof. It is again similar to the previous. There is nothing to prove when $\text{rk } P = 1$. And in the first case of Theorem 1.10, for instance ($P = Q.R, \text{rk}_X R = 0$), then $d_X^\circ R = 0$ by 1.5 and, using 1.6:

$$\begin{aligned} d_X^\circ (Q.R)^* &= d_X^\circ (Q^* \circ_X (R \setminus X)) = d_X^\circ Q d_X^\circ (R \setminus X) = d_X^\circ Q = d_X^\circ (Q.R), \\ d_Y^\circ (Q.R) &= d_Y^\circ (Q \circ_X (R \setminus X)) = d_Y^\circ Q + d_X^\circ Q d_Y^\circ (R \setminus X) \\ &= -d_X^\circ Q (d_Y^\circ Q + d_Y^\circ R) = -d_X^\circ P d_Y^\circ P. \end{aligned}$$

6. If finally $\mathcal{F} \subseteq \mathcal{E} - \{X\}$, we say that $P \in \mathcal{A}$ is an \mathcal{F} -force element in X if P is simple in X with $d_X^\circ P = +1$, $d_Y^\circ P = 0$ for all $Y \in \mathcal{F}$, $\text{rk}_Z P = 0$ for all $Z \in \mathcal{E} - \mathcal{F} - \{X\}$.

PROPOSITION 1.15. *If P and Q are both \mathcal{F} -force elements in X , so is $P \circ_X Q$.*

Proof. This follows from 1.3 and 1.6.

PROPOSITION 1.16. *If P is an \mathcal{F} -force element in X , so is P^* .*

Proof. This follows from 1.13 and 1.14.

2. The PQ-algebra of subsets of a groupoid.

1. The PQ-algebra of subsets of a groupoid G is the set \mathcal{E} of all subsets of G together with the operations described in the introduction (example A). For each $x \in G$, we identify $\{x\}$ and x , so that $G \subseteq \mathcal{E}$.

The set \mathcal{E} generates a free PQ-algebra \mathcal{A} . We shall denote by ϕ the canonical homomorphism of \mathcal{A} onto \mathcal{E} . Since we are interested in mappings of \mathcal{E} into \mathcal{E} , we shall also consider the over-algebra $\overline{\mathcal{A}}$ of \mathcal{A} freely generated by $\mathcal{E} \cup \{X\}$, where X is an ‘‘indeterminate’’ ($X \notin \mathcal{E}$). Then, for each $P \in \overline{\mathcal{A}}$, we have a mapping f_P of \mathcal{E} into \mathcal{E} defined by

$$f_P(A) = \phi(P \circ_X A) \quad \text{for all } A \in \mathcal{E}.$$

A mapping f of \mathcal{E} into \mathcal{E} which has the form f_P for some $P \in \overline{\mathcal{A}}$ is called *rational*; if $f = f_P$ for some $P \in \overline{\mathcal{A}}$ which is simple in X , it is called *simple*.

PROPOSITION 2.1. *If $(A_i)_{i \in I} \subseteq \mathcal{E}$ and if f is a simple mapping of \mathcal{E} , then $f(\cup_{i \in I} A_i) = \cup_{i \in I} (f(A_i))$.*

Proof. This follows from the \cup -distributivity of the three operations of \mathcal{E} .

It follows from 2.1 that a *simple* mapping $f = f_P$ of \mathcal{E} is completely determined by the binary relation \mathcal{R}_P on G defined by: $x \mathcal{R}_P y$ if and only if $x \in f_P(y)$. Such a binary relation is called *simple*.

2. The operations of $\overline{\mathcal{A}}$ induce operations on rational mappings and simple binary relations.

PROPOSITION 2.2. *For any $P, Q \in \overline{\mathcal{A}}$ and $A \in \mathcal{E}$:*

$$\begin{aligned} f_{P \cdot Q}(A) &= f_P(A) f_Q(A), \\ f_{P/Q}(A) &= f_P(A) \cdot \cdot f_Q(A), \\ f_{P \setminus Q}(A) &= f_P(A) \cdot \cdot \cdot f_Q(A). \end{aligned}$$

Proof. Both ϕ and $P \rightarrow P \circ_X A$ are homomorphisms.

PROPOSITION 2.3. *If $P, Q \in \overline{\mathcal{A}}$, $f_{P \circ_X Q} = f_P \circ f_Q$.*

Proof. If $\text{rk } P = 1$, either $P = X$ and then f_P is the identity mapping and $f_{P \circ_X Q} = f_Q = f_P \circ f_Q$; or $P \neq X$, $P \in \mathcal{E}$, and then f_P is a constant mapping and $f_{P \circ_X Q} = f_P = f_P \circ f_Q$.

If the formula is true whenever $\text{rk } P < n$ (where $n \geq 2$) and if we take $\text{rk } P = n$, then, by 1.1, $P = R.S$ or R/S or $R \setminus S$ and, using 2.2:

$$\begin{aligned} f_{P \circ_X Q}(A) &= f_{R \circ_X Q}(A) f_{S \circ_X Q}(A) \\ &= f_R(f_Q(A)) f_S(f_Q(A)) = f_P(f_Q(A)) \end{aligned}$$

for all $A \in \mathcal{E}$, $Q \in \overline{\mathcal{A}}$, since $\text{rk } R < n$, $\text{rk } S < n$. One completes the induction similarly in the two other cases.

Binary relations on G have also a composition, defined by: $x \mathcal{R} \circ \mathcal{S} z$ if and only if $x \mathcal{R} y$ and $y \mathcal{S} z$ for some $y \in G$.

PROPOSITION 2.4. *If P and Q are both simple in X , then $\mathcal{R}_{P \circ_X Q} = \mathcal{R}_P \circ \mathcal{R}_Q$.*

Proof. This follows from 2.3.

PROPOSITION 2.5. *If P is simple in X , then $\mathcal{R}_{P^*} = \mathcal{R}_P^*$.*

Proof. If $\text{rk } P = 1$, then $P = X = P^*$ and both \mathcal{R}_P and \mathcal{R}_{P^*} are the equality relation on G ; the formula follows.

If the formula holds whenever $\text{rk } P < n$ (where $n \geq 2$) and if we take $\text{rk } P = n$, then P falls in exactly one of the six cases of Theorem 1.10. In the first case ($P = Q.R$, $\text{rk}_X R = 0$), f_R is a constant mapping since X does not appear in R , so that $f_R(A) = B$, say, for all $A \in \mathcal{E}$. Then $y \in f_P(x)$ is successively equivalent to

$$\begin{aligned} y \in f_Q(x) f_R(x) &= f_Q(x) B \quad \text{by 2.2;} \\ (\exists z \in G) y \in zB, z \in f_Q(x); \\ (\exists z \in G) x \in f_{Q^*}(z), z \in B \cdot \cdot y &\quad \text{since } \text{rk } Q < n; \\ x \in f_{Q^*}(B \cdot \cdot y) &\quad \text{by 2.1;} \\ x \in f_{Q^*}(f_R(y) \cdot \cdot f_X(y)) &= f_{Q^*}(f_{R \setminus X}(y)) \quad \text{by 2.2;} \\ x \in f_{P^*}(y) &= f_{Q^* \circ_X (R \setminus X)}(y) \quad \text{by 2.3.} \end{aligned}$$

The other cases are analogous.

3. If $H \in \mathcal{E}$, an H -force element P of $\overline{\mathcal{A}}$ is an \mathcal{F} -force element as defined in §1, with $\mathcal{F} = G \cup \{H\}$. The set of all H -force elements will be denoted by \mathcal{H} . An H -force mapping is a mapping f of the form f_P for some $P \in \mathcal{H}$; an H -force relation is a binary relation of the form \mathcal{R}_P for some $P \in \mathcal{H}$. The sets of all H -force mappings and relations will be denoted by \mathcal{H}^f and \mathcal{H}^r , respectively. Any H -force mapping or relation is simple.

PROPOSITION 2.6. *If f and f' (\mathcal{R} and \mathcal{R}') are H -force mappings (relations), so is $f \circ f'$ ($\mathcal{R} \circ \mathcal{R}'$).*

Proof. This follows from 1.15 and 2.3 (2.4).

PROPOSITION 2.7. *If \mathcal{R} is an H -force relation, so is \mathcal{R}^* .*

Proof. This follows from 1.16 and 2.5.

Observe finally that the identity mapping of G is an H -force mapping (which we shall denote by I), and the equality relation on G is an H -force relation.

4. Now we can state our main theorem.

THEOREM 2.8. *The smallest associative, commutative, and cancellative congruence on G in a class of which a given subset H of G is contained is the binary relation \mathcal{C} on G defined by:*

$$x \mathcal{C} y \Leftrightarrow x, y \in \bigcup_{f \in \mathcal{H}^f} f(H) \text{ or } (\exists \mathcal{R} \in \mathcal{H}^r) x \mathcal{R} y.$$

The proof is given in the two next subsections. We have to prove that \mathcal{C} is an associative, commutative, and cancellative congruence on G and that H is contained in one class of \mathcal{C} ; and conversely that \mathcal{C} is the smallest such congruence.

5. To prove the direct part of the theorem, we use the properties of H -force mappings and relations. First we consider $\bar{H} = \bigcup_{f \in \mathcal{H}^f} f(H)$. Since $I \in \mathcal{H}^f$, $H \subseteq \bar{H}$.

LEMMA 2.9. *For any $f \in \mathcal{H}^f$, $f(\bar{H}) \subseteq \bar{H}$.*

Proof. By 2.1 and 2.6:

$$f(\bar{H}) = f(\bigcup_{g \in \mathcal{H}^f} g(H)) = \bigcup_{g \in \mathcal{H}^f} f(g(H)) \subseteq \bigcup_{h \in \mathcal{H}^f} h(H) = \bar{H}.$$

LEMMA 2.10. *For every $\mathcal{R} \in \mathcal{H}^r$, $x \in \bar{H}$ and $x \mathcal{R} y$ implies $y \in \bar{H}$.*

Proof. Since $\mathcal{R}^* \in \mathcal{H}^r$ by 2.7, $y \in f(x)$ for some $f \in \mathcal{H}^f$ and $y \in \bar{H}$ follows from 2.9.

Now we can prove that \mathcal{C} is an equivalence relation.

LEMMA 2.11. *\mathcal{C} is an equivalence relation on G and H is contained in a class of \mathcal{C} (namely, \bar{H}).*

Proof. Since the equality relation on G is in \mathcal{H}^r , \mathcal{C} is reflexive. It is symmetric by 2.7. Assume that $x \mathcal{C} y$ and $y \mathcal{C} z$. If $x, y, z \in \bar{H}$, then $x \mathcal{C} z$. If $x, y \in \bar{H}$ and $y \mathcal{R} z$ for some $\mathcal{R} \in \mathcal{H}^r$, then $z \in \bar{H}$ by 2.10 and $x \mathcal{C} z$. Since \mathcal{C} is symmetric, $x \mathcal{C} z$ holds also when $x \mathcal{R} y$ for some $\mathcal{R} \in \mathcal{H}^r$ and $y, z \in \bar{H}$. If finally $x \mathcal{R} y$ and $y \mathcal{R}' z$ for some $\mathcal{R}, \mathcal{R}' \in \mathcal{H}^r$, then $x \mathcal{R} \circ \mathcal{R}' z$ and $x \mathcal{C} z$ by 2.6. Therefore \mathcal{C} is an equivalence relation. The definition of \mathcal{C} and 2.10 imply that \bar{H} is a class of \mathcal{C} , which completes the proof.

LEMMA 2.12. *\mathcal{C} is a congruence on G .*

Proof. To show that \mathcal{C} is a left congruence, let $a, x, y \in G$ be such that $x \mathcal{C} y$, and set $u = ax, v = ay$.

Suppose first that $x \in f_P(y)$ for some $P \in \mathcal{H}$. Since $a \in y \cdot v$, then $u \in (y \cdot v)f_P(y) = f_Q(v)$, where $Q = (y \setminus X) \cdot (P \circ_X y)$. By 1.3 and 1.6, $\text{rk}_X Q = 1$, $d_X^\circ Q = +1$, $d_Y^\circ Q = -1 + d_Y^\circ P + d_X^\circ P d_Y^\circ y = 0$, $d_Z^\circ Q = d_Z^\circ P = 0$ for all $z \in G$, $z \neq y$ and for $z = H$, and $\text{rk}_A Q = \text{rk}_A P = 0$ for all $A \in \mathcal{E}$, $A \notin G$, $A \neq H$. Therefore $Q \in \mathcal{H}$ and $u \mathcal{C} v$.

If $x \notin f_P(y)$ for all $P \in \mathcal{H}$, then $x, y \in \bar{H}$, so that $x \in f_P(H)$, $y \in f_Q(H)$ for some $P, Q \in \mathcal{H}$. Again $u \in (y \cdot v)x$, whence $u \in (f_Q(H) \cdot v)f_P(H) = f_R(v)$, where $R = ((Q \circ_X H) \setminus X) \cdot (P \circ_X H)$. Using again 1.3, 1.6, $\text{rk}_X R = 1$, $d_X^\circ R = +1$, $d_H^\circ R = -1 + 1 = 0$, $d_Z^\circ R = 0$ for all $z \in G$ and $\text{rk}_A R = 0$ for all $A \in \mathcal{E}$, $A \notin G$, $A \neq H$. Therefore $R \in \mathcal{H}$ and $u \mathcal{C} v$.

This shows that \mathcal{C} is a left congruence. Dually, \mathcal{C} is a right congruence, which completes the proof.

LEMMA 2.13. *\mathcal{C} is cancellative.*

Proof. Let $a, x, y, u, v \in S$ be such that $x \mathcal{C} y$, $x = ua$, $y = va$. We shall prove, as before, that $u \mathcal{C} v$.

If $x \in f_P(y)$ for some $P \in \mathcal{H}$, then $a \in y \cdot v$, $u \in a \cdot x$ and $u \in (y \cdot v) \cdot f_P(y) = f_Q(v)$, where $Q = (y/X) \setminus (P \circ_X y)$. Again $Q \in \mathcal{H}$, for $\text{rk}_X Q = 1$, $d_X^\circ Q = -(-1) = +1$, $d_H^\circ Q = d_H^\circ P = 0$, $d_Y^\circ Q = -1 + 1 = 0$, $d_Z^\circ Q = 0$ for all $z \in G$, $z \neq y$ and $\text{rk}_A Q = 0$ for all $A \in \mathcal{E}$, $A \notin G$, $A \neq H$. Thus $u \mathcal{C} v$.

If $x \in f_P(H)$, $y \in f_Q(H)$ for some $P, Q \in \mathcal{H}$, then $u \in (f_Q(H) \cdot v) \cdot f_P(H) = f_R(v)$, where $R = ((Q \circ_X H)/X) \setminus (P \circ_X H)$. Again $R \in \mathcal{H}$, since $\text{rk}_X R = 1$, $d_X^\circ R = -(-1) = +1$, $d_Z^\circ R = d_Z^\circ P - d_Z^\circ Q = 0$ for all $z \in G$, $d_H^\circ R = (d_H^\circ P + 1) - (d_H^\circ Q + 1) = 0$ and $\text{rk}_A R = 0$ for all other $A \in \mathcal{E}$. Thus $u \mathcal{C} v$.

Therefore \mathcal{C} is left cancellative. Dually, it is right cancellative, which completes the proof.

LEMMA 2.14. *\mathcal{C} is commutative and associative.*

Proof. It uses the same technique. First, let $a, b \in G$ and set $u = ab, v = ba$. Then $a \in v \cdot b$ and $u \in (v \cdot b)b = f_P(v)$, where $P = (X/b)b$. There, $\text{rk}_X P = d_X^\circ P = +1$, $d_b^\circ P = -1 + 1 = 0$, and $\text{rk}_Y P = 0$ (whence also $d_Y^\circ P = 0$ by 1.5) for all other $Y \in \mathcal{E}$. Therefore $P \in \mathcal{H}$ and $ab \mathcal{C} ba$.

Similarly, let $a, b, c \in G$ and set $u = a(bc), v = (ab)c$. Now $c \in v \cdot ab$ and $u \in a(b(v \cdot ab)) = f_P(v)$, where $P = a \cdot (b \cdot (X/(a \cdot b)))$. Again $\text{rk}_X P = d_X^\circ P = +1$, $d_a^\circ P = +1 - 1 = 0 = d_b^\circ P$, and $\text{rk}_Y P = 0$ (whence also $d_Y^\circ P = 0$) for all other $Y \in \mathcal{E}$. Therefore $P \in \mathcal{H}$ and $a(bc) \mathcal{C} (ab)c$.

This completes the proof of the direct part of Theorem 2.8.

6. The key part of the proof of the converse is the interpretation of all the ranks and degrees of any $P \in \mathcal{A}$ on the following complete description of the relation $x \in \phi(P)$.

LEMMA 2.15. *If $P \in \mathcal{A}$, the relation $x \in \phi(P)$ is equivalent to a finite set of quantified memberships to G or to the $Y \in \mathcal{E}$ which appear in P and of equalities of the form $a = b$ or $a = bc$ or $bc = a$, such that*

- (i) *x appears in exactly one equality, in the left side;*
- (ii) *any element which appears in some equality appears also in exactly one membership, after a quantifier \exists ;*
- (iii) *any element involved in a membership to G (i.e. not involved in a membership to some Y appearing in P) appears once in the left side of an equality and once in a right side;*
- (iv) *for every $Y \in \mathcal{E}$, let r_Y (l_Y) be the number of times that an element involved in a membership to Y appears in the right (left) side of an equality; then*

$$r_Y + l_Y = \text{rk}_Y P, \quad r_Y - l_Y = d_Y^\circ P$$

(in particular, both are zero if Y does not appear in P).

Example. Take $P = (A.B).C$; then $x \in \phi(P)$ is equivalent to

$$(\exists a \in A)(\exists b \in B)(\exists c \in C)(\exists u \in G)$$

such that

$$x = uc, \quad u = ab,$$

and it is readily seen that this set of equalities and memberships has the properties required in the lemma.

Proof. It is by induction on $\text{rk } P$. If $\text{rk } P = 1$, then $P = Y \in \mathcal{E}$ and $x \in \phi(P)$ is equivalent to: $(\exists y \in Y) x = y$. This set of one equality and one membership has the required properties. Assume now that the lemma holds for all $S \in \mathcal{A}$ such that $\text{rk } S < n$ (where $n \geq 2$) and that $\text{rk } P = n$. By 1.1 we have $P = Q.R$ or Q/R or $Q \setminus R$, with $\text{rk } Q < n$, $\text{rk } R < n$.

In the first case, $\phi(P) = \phi(Q)\phi(R)$ (since ϕ is a homomorphism) and $x \in \phi(P)$ is equivalent to: $(\exists y \in G)(\exists z \in G) x = yz$, $y \in \phi(Q)$, $z \in \phi(R)$. The induction hypothesis provides a set of memberships and equalities which is equivalent to $y \in \phi(Q)$; we replace $y \in \phi(Q)$ by this set in the above (without exchanging the sides of any equality since the sides are important). We proceed similarly with $z \in \phi(R)$. We obtain a set of memberships and equalities which is equivalent to $x \in \phi(P)$. Using the induction hypothesis, it is clear that it has properties (i), (ii), (iii). To prove (iv), let r_Y ($r_{Y'}$, $r_{Y''}$) be the number of times an element involved in a membership to Y appears in the right side of an equality of the set of P (Q , R), and l_Y , $l_{Y'}$, $l_{Y''}$ be the analogous numbers for the left sides. Since the sides of the equalities were not exchanged in the substitution, we have $r_Y = r_{Y'} + r_{Y''}$, $l_Y = l_{Y'} + l_{Y''}$, so that

$$r_Y + l_Y = \text{rk}_Y Q + \text{rk}_Y R = \text{rk}_Y P,$$

$$r_Y - l_Y = d_Y^\circ Q + d_Y^\circ R = d_Y^\circ P$$

for all $Y \in \mathcal{E}$.

In the second case ($P = Q/R$), we have $\phi(P) = \phi(Q) \cdot \phi(R)$, so that $x \in \phi(P)$ is equivalent to: $(\exists y \in G)(\exists z \in G)zx = y, y \in \phi(Q), z \in \phi(R)$. This time z appears in a left side, so that now we exchange the sides of all equalities in the set of R while replacing $z \in \phi(R)$ by this set; but we do not exchange the sides for Q . In that manner, z appears once in a left side and once in a right side in the resulting set, which therefore satisfies (i), (ii), and (iii). Keeping the same notation to verify (iv), we now have $r_Y = r_{Y'} + l_{Y''}, l_Y = l_{Y'} + r_{Y''}$, so that

$$\begin{aligned} r_Y + l_Y &= \text{rk}_Y Q + \text{rk}_Y R = \text{rk}_Y P, \\ r_Y - l_Y &= d_Y^\circ Q - d_Y^\circ R = d_Y^\circ P \end{aligned}$$

for all $Y \in \mathcal{E}$. In the third case ($P = Q \setminus R$) we proceed similarly, this time exchanging the sides of the equalities for Q but not for R .

Using this lemma, we can prove the converse part of Theorem 2.8. Let \mathcal{C}' be an associative, commutative, and cancellative congruence on G such that H is contained in one class of \mathcal{C}' . First we prove that any $\mathcal{R} \in \mathcal{H}^r$ is contained in \mathcal{C}' . Let $P \in \mathcal{H}$ be such that $\mathcal{R} = \mathcal{R}_P$ and $x, y \in G$ be such that $x \mathcal{R} y$. Then $x \in f_P(y) = \phi(P \circ_X y)$.

By 2.15 we have a finite set of equalities and memberships such that:

- (i) x appears once in a left side of some equality;
- (ii) any element involved in an equality is either an element of H or some element of G which appears in P or
- (iii) appears once in a left side and once in a right side;
- (iv) since $d_H^\circ(P \circ_X y) = 0$, the elements of H appear the same number of times on each side; since $d_y^\circ(P \circ_X y) = +1$, y appears once more on the right sides than on the left sides; if z is any other element of G , z appears the same number of times on each side, since $d_z^\circ(P \circ_X y) = 0$.

Form now the product π' (π'') of all the left (right) sides, using the same disposition of parentheses for π' and π'' , so that $\pi' = \pi''$. Observe that π' and π'' differ: (a) by the elements of H which appear in π'' and may be different from the elements of H appearing in π' (although there is the same number of such elements in π' and π''); (b) there is one more y in π'' than in π' and no x in π'' ; (c) the other elements of G appear the same number of times in π' and π'' but perhaps at different places. Since \mathcal{C}' is an associative and commutative congruence, we stay in the same class of \mathcal{C}' if we change the order of the elements in π'' so that they appear in the same order as in π' (without changing the disposition of parentheses); i.e., with the elements of H in the same places, the y 's in the same places with one y in the place of x . In other words, if π''' is this new product, $\pi'' \mathcal{C}' \pi'''$. Since H is contained in one class of \mathcal{C}' , we have also $\pi''' \mathcal{C}' \pi''''$, where π'''' is obtained from π''' by replacing each element of H appearing in π''' by the element of H which appears in π' at the same place. Now π' and π'''' are identical, except that x appears in π' and that y appears at the same place in π'''' . Since $\pi' \mathcal{C}' \pi''''$ and \mathcal{C}' is cancellative, it follows that $x \mathcal{C}' y$.

This shows that \mathcal{C}' contains any $\mathcal{R} \in \mathcal{H}^r$. If now $x, y \in \bar{H}$, then $x \in f_P(h)$, $y \in f_Q(k)$ for some $P, Q \in \mathcal{H}$ and $h, k \in H$. Then $h \mathcal{C}' k$ and also $x \mathcal{C}' h$ and $y \mathcal{C}' k$ by the above. It follows that $x \mathcal{C}' y$.

Therefore we have proved that $\mathcal{C} \subseteq \mathcal{C}'$, which completes the proof of Theorem 2.8.

7. As consequences of the main theorem we obtain the results announced in the introduction.

COROLLARY 2.16. *H is a class of some associative, commutative, and cancellative congruence on G if and only if $H \neq \emptyset$ and $f(H) \subseteq H$ for all $f \in \mathcal{H}^f$.*

Proof. H is a class of some associative, commutative, and cancellative congruence on G if and only if it is a class of the congruence \mathcal{C} of Theorem 2.8, if and only if $H = \bar{H} \neq \emptyset$ (by 2.11), if and only if $H \neq \emptyset$ and $\bar{H} \subseteq H$ since always $H \subseteq \bar{H}$.

COROLLARY 2.17. *If $H \neq \emptyset$, the smallest subset of G which is a class of some associative, commutative, and cancellative congruence on G and contains H is precisely \bar{H} .*

Proof. By 2.11, \bar{H} is a class of \mathcal{C} and contains H . If K is a class of some associative, commutative, and cancellative congruence \mathcal{C}' on G and contains H , then $\mathcal{C} \subseteq \mathcal{C}'$ and $\bar{H} \subseteq K$.

COROLLARY 2.18. *The smallest associative, commutative, and cancellative congruence on G is the union of all the \mathcal{R}_P such that P is a G -force element of $\bar{\mathcal{A}}$.*

Proof. By Theorem 2.8, it is the union of all the \mathcal{R}_P such that P is a $(G \cup \{\emptyset\})$ -force element of $\bar{\mathcal{A}}$, for we obtain it by taking $H = \emptyset$. Let P be such an element of $\bar{\mathcal{A}}$. If \emptyset does not appear in P , then P is a G -force element of $\bar{\mathcal{A}}$. If \emptyset appears in P , then $f_P(A) = \emptyset$ for all $A \in \mathcal{E}$ by 2.1, so that $\mathcal{R}_P = \emptyset$. The result follows.

3. The case of a semigroup. In a semigroup S , any congruence is associative and 2.8, 2.16, 2.17, 2.18 become:

THEOREM 3.1. *The congruence \mathcal{C} constructed from H as in Theorem 2.8 is the smallest commutative and cancellative congruence on S in a class of which H is contained.*

COROLLARY 3.2. *H is a class of some commutative and cancellative congruence on S if and only if $H \neq \emptyset$ and $f(H) \subseteq H$ for all $f \in \mathcal{H}^f$.*

COROLLARY 3.3. *If $H \neq \emptyset$, the smallest subset of S which is a class of some commutative and cancellative congruence on S and contains H is precisely \bar{H} .*

COROLLARY 3.4. *The smallest commutative and cancellative congruence on S is the union of all the \mathcal{R}_P such that P is an S -force element of $\bar{\mathcal{A}}$.*

4. The case of a quasigroup.

1. If Q is a quasigroup, then Q itself may be turned into a PQ-algebra (cf. introduction, example B). The set Q freely generates another PQ-algebra \mathcal{B} and there is a canonical homomorphism ψ of \mathcal{B} onto Q . Let $\overline{\mathcal{B}}$ be the free PQ-algebra generated by $Q \cup \{X\}$, where X is an indeterminate, $X \notin \mathcal{E}$.

The PQ-algebras \mathcal{E} , \mathcal{A} , $\overline{\mathcal{A}}$ of §2 are now over-algebras of Q , \mathcal{B} , $\overline{\mathcal{B}}$, respectively. An element of $\overline{\mathcal{A}}$ is in $\overline{\mathcal{B}}$ if and only if only X and the elements of Q may appear in it. In particular, every Q -force element of $\overline{\mathcal{A}}$ is in $\overline{\mathcal{B}}$ and is then a Q -force element of $\overline{\mathcal{B}}$. Hence 2.18 can be expressed in terms of $\overline{\mathcal{B}}$ only. We shall do so after a closer investigation of the Q -force elements.

2. Let $P \in \overline{\mathcal{B}}$ and let f_P^i denote the restriction of f_P to the domain Q . Then f_P^i maps Q into itself: indeed, for any $a, b \in Q$, $a \cdot b = a/b$, $a \cdot b = a \setminus b$, so that $\phi(P \circ_X y)$ is an element of Q whenever $y \in Q$. We call any mapping of the form f_P^i an *inner rational mapping*, and an *inner simple mapping* if P is simple in X .

PROPOSITION 4.1. *The set of all inner simple mappings of Q is a group of bijections, with $f_R^i \circ f_S^i = f_{R \circ_X S}^i$, $(f_R^i)^{-1} = f_{R^*}^i$ for all simple $R, S \in \overline{\mathcal{B}}$. In fact, the group of all inner simple mappings is just the group generated by all mappings $x \rightarrow xa, ax, x/a, a/x, x \setminus a, a \setminus x$ (elementary inner simple mappings).*

Proof. Clearly, a mapping of Q into Q is inner simple if and only if it is a finite product of elementary inner simple mappings. Since Q is a quasigroup, the elementary inner simple mappings are bijections (i.e., one-to-one and onto) and so are the inner simple mappings. The two formulae follow then from 2.3 and 2.5 and imply that the inner simple mappings form a group, obviously generated by the elementary inner simple mappings.

We call f_P^i a *force mapping* of Q when P is a Q -force element of $\overline{\mathcal{B}}$.

PROPOSITION 4.2. *The force mappings of Q form a subgroup of the group of all inner simple mappings.*

Proof. In view of the formulae in 4.1, this follows from 1.15 and 1.16.

3. Now 2.18 takes the form

THEOREM 4.3. *The smallest associative commutative and cancellative congruence on Q is the transitivity equivalence of the group of all force mappings of Q .*

Proof. This is clear since the transitivity equivalence of a group of bijections is precisely defined by $x = f(y)$ for some f in the group.

If Q happens to be a group (so that all congruences on Q are associative and cancellative) the congruence of Theorem 4.3 is the congruence defined by the commutator subgroup. One form of Theorem 4.3 is then the following well-known result: x belongs to the commutator subgroup if and only if x can be written as a product of powers of elements x_1, \dots, x_n of the group so that the sum of the powers of x_i in that product is 0 for all i .

5. Related topics and references. It is convenient in a semigroup to call a condition of the form $f(H) \subseteq H$, where $f \in \mathcal{H}^f$, a *force* condition. Then 3.2 gives the subsets satisfying all force conditions. Examples of subsets characterized by a single force condition are: the strong (*fort*) subsets of Dubreil (4), the bilaterally strong subsets of Croisot (2), the semistrong subsets of Desq (3), the partially right or left strong (on one side) subsets of Grillet (8), as readily verified. More generally, the family of all subsets which satisfy a given set of force conditions is closed under intersection and inductive, so the smallest subset of the family containing a given subset can be constructed by an inductive process (7).

Dubreil already noted that every class of a cancellative congruence is strong (4). More generally, it is possible to construct a family of force conditions which characterizes the classes of the equivalence relations satisfying any subset of the following set of conditions: compatible on one side, cancellative on one side, commutative (6). It would be interesting to have a characterization of these families purely in terms of PQ-algebras. All we can do is build an analogous theory for *tas* (cf. 8) instead of semigroups, using PQ-like algebras, which can be applied to equivalence relations which are compatible on one side, cancellative on the same side, and commutative.

As for quasigroups, the idea of turning them into PQ-algebras is not new (see 1). A group smaller than the group of inner simple mappings has been proved useful in quasigroup theory (10) and it is perhaps possible to use the group of all force mappings in a similar fashion.

REFERENCES

1. R. H. Bruck, *A survey of binary systems* (Springer-Verlag, Berlin-Göttingen-Heidelberg, 1958).
2. R. Croisot, *Equivalences principales bilatères définies dans un demi-groupe*, J. Math. Pures Appl. (9), 36 (1957), 373–417.
3. R. Desq, *Etude dans un demi-groupe D d'une relation d'équivalence liée à un complexe H*, C. R. Acad. Sci. Paris, 254 (1962), 2117–2119.
4. P. Dubreil, *Contribution à la théorie des demi-groupes*, Mém. Acad. Sci. Paris, 63 (1941), 52 pp.
5. M.-L. Dubreil-Jacotin, L. Lesieur, and R. Croisot, *Leçons sur la théorie des treillis, des structures algébriques ordonnées et des treillis géométriques*, Gauthier-Villars, Paris, 1953.
6. P.-A. Grillet, *Equivalences compatibles, équivalences prépermises*, Séminaire Dubreil-Pisot (Univ. de Paris), 15 (1961/62), numéro 2.
7. ——— *Les applications de préfermeture*, C. R. Acad. Sci. Paris, 253 (1961), 2824–2826.
8. ——— *Homomorphismes principaux de tas et de groupoïdes* (Thèse Sci. Math.), Bull. Soc. Math. France, Mém. numéro 3 (1965).
9. P. Lefebvre, *Sur la plus fine équivalence régulière et simplifiable d'un demi-groupe*, C. R. Acad. Sci. Paris, 251 (1960), 1265–1267.
10. G. Mattenet, *Sur les quasi-groupes*, Séminaire Dubreil-Pisot (Univ. de Paris), 15 (1961/62), numéro 12.

Kansas State University,
Manhattan Kansas