ON A PROBLEM OF BAAYEN AND KRUYSWIJK

by D. A. BURGESS

(Received 13th December 1967)

1. We shall call a finite semigroup S *arithmetical* if there exists a positive integer N and a monomorphism μ of S into the multiplicative semigroup R_N of the ring of residue classes of the integers modulo N. In 1965 P. C. Baayen and D. Kruyswijk [**1**] posed the problem ' Is every finite commutative semigroup arithmetical? ' The purpose of this paper is to answer this question.

In section **2** I obtain a necessary and sufficient condition for a finite semigroup to be arithmetical. In section **3** I use this criterion to demonstrate that there are finite commutative semigroups which are not arithmetical. In section **4** I use the criterion to prove that certain special classes of commutative semigroups are arithmetical. Finally in section **5** I give the weaker theorem that every finite commutative semigroup is a homomorphic image of an arithmetical semigroup.

2. Let S be a finite commutative semigroup. Let C denote the set of roots of unity (in the field of complex numbers) and let x be an indeterminate. We shall define χ to be a *character of S* if there is a positive integer m such that χ is a homomorphism of S into the semigroup of elements

$$\omega x^{\alpha} \pmod{x^m}$$

under multiplication, where ω is in C and α is a non-negative integer. [This is not the usual definition of a semigroup character (see A. H. Clifford and G. B. Preston [**2**]), but it is a convenient notation for our investigation.] These mappings become representations if we interpret x as a matrix satisfying

$$x^m = 0, \quad x^{m-1} \neq 0.$$

If S is a group then the Abelian group characters are characters in our sense with

$$m = 1.$$

Our principal result is:

Theorem 1. *A finite commutative semigroup S is arithmetical if and only if for each pair of distinct elements a, b of S there is a character $\chi = \chi_{a,b}$ of S for which*

$$\chi(a) \neq \chi(b). \tag{1}$$

Proof. Suppose that S is arithmetical. Thus S can be embedded isomorphically in some R_N. We show that for each pair a, b of distinct elements of R_N there is a χ of R_N satisfying (1).

Let the canonical factorisation of N be

$$N = \prod_{i=1}^{r} p_i^{\alpha(i)}.$$

Then R_N can be represented as the direct sum

$$R_N = \sum_{i=1}^{r} R_{p_i^{\alpha(i)}}.$$

For, by the Chinese remainder theorem, we may choose $k_1, \ldots, k_r$ such that

$$k_i \equiv \begin{cases} 1 \pmod{p_i^{\alpha(i)}} & (i = 1, \ldots, r), \\ 0 \pmod{p_j^{\alpha(j)}} & (j \neq i), \end{cases}$$

and then the representation

$$x \equiv \sum_{i=1}^{r} k_i x_i \pmod{N}$$

gives the required isomorphism, where each x_i runs through the residue classes modulo $p_i^{\alpha(i)}$. Since a and b are distinct there is an i for which a_i and b_i are distinct. Thus, by applying first the projection homomorphism of R_N onto $R_{p_i^{\alpha(i)}}$, it suffices to prove the result in the restricted case when $N = p^\alpha$ is a power of a prime p.

Now if

$$(a, p^\alpha) \neq (b, p^\alpha),$$

where (u, v) denotes the highest common factor of u and v, then the character χ defined by

$$\chi(z) = x^\zeta \pmod{x^\alpha},$$

where $(z, p^\alpha) = p^\zeta$, satisfies (1). If alternatively

$$(a, p^\alpha) = (b, p^\alpha) = p^\beta \text{ say},$$

let ψ be an Abelian group character of the multiplicative group of residue classes modulo $p^{\alpha-\beta}$ that are relatively prime to p for which

$$\psi(a/p^\beta) \neq \psi(b/p^\beta).$$

In this case we define the character χ by

$$\chi(z) = \psi(z/p^\zeta)x^\zeta \pmod{x^{\beta+1}}$$

and again (1) is satisfied.

Next we prove the converse. Let S be a semigroup and a and b be two distinct elements of S. Let $\chi = \chi_{a,b}$ be a character of S such that

$$\chi(a) \not\equiv \chi(b) \pmod{x^m = x^{m(a,b)}}.$$

Let $d = d_{a,b}$ be the least common multiple of the orders of the coefficients of the non-zero monomials which belong to $\operatorname{Im}\chi$. Choose an odd prime $p = p_{a,b}$ for which

$$p \equiv 1 \pmod{d}. \tag{2}$$

Let g be a primitive dth root of unity modulo p^m, and so also modulo p, and let η be a primitive dth root of unity in C. Then the map $\tau = \tau_{a,b}$ given by

$$\tau(\eta^\lambda x^\zeta) = g^\lambda p^\zeta \pmod{p^m}$$

is a monomorphism of $\operatorname{Im}\chi$ into $R_{p^m} = R_{a,b}$ say, and so the homomorphism $\tau\chi$ of S into $R_{a,b}$ has the property

$$\tau\chi(a) \neq \tau\chi(b).$$

By Dirichlet's theorem we may choose all the odd primes $p_{a,b}$ (required only to satisfy (2)) to be distinct. Thus there is a monomorphism

$$\mu\colon S \to \sum_{a,b} R_{a,b} \simeq R_N,$$

where

$$N = \prod_{a,b} p_{a,b}^{m(a,b)},$$

the component of μ in $R_{a,b}$ being $\tau_{a,b}\chi_{a,b}$.

3. Theorem 2. *There exists a non-arithmetical finite commutative semigroup.*

Proof. We show that the semigroup S given by the multiplication table

	e	a	b	c
e	e	e	e	e
a	e	e	c	e
b	e	c	e	e
c	e	e	e	e

is not arithmetical. It suffices to show that there is no character χ of S with

$$\chi(e) \neq \chi(c). \tag{3}$$

Since e is an idempotent and $ec = e$ we must have

$$\chi(e) \equiv 0 \pmod{x^m}.$$

Next we have

$$\chi(a)^2 \equiv \chi(b)^2 \equiv \chi(e) \equiv 0 \pmod{x^m}.$$

Thus

$$\chi(c)^2 \equiv \chi(a)^2\chi(b)^2 \equiv 0 \pmod{x^{2m}}$$

which implies that

$$\chi(c) \equiv 0 \equiv \chi(e) \pmod{x^m}$$

and so (3) is not satisfied.

4. Theorem 3. *A finite direct sum of arithmetical semigroups is arithmetical.*

Proof. If a, b are two distinct elements of the direct sum S we let τ be the projection homomorphisms of S onto some component T in which $\tau(a) \neq \tau(b)$. Then since T is arithmetical there is a character χ of T with

$$\chi\tau(a) \neq \chi\tau(b),$$

so that $\chi\tau$ is the required character of S.

Theorem 4. *If the finite commutative semigroup S can be partitioned into a set of disjoint groups then S is arithmetical.*

Proof. Let

$$S = \bigcup_{i=1}^{n} S_i$$

where each S_i is a group and has a unique idempotent e_i (the identity).

Now we note that the relation $>$ defined by

$$S_i > S_j \text{ if and only if } e_i e_j = e_i$$

is a partial ordering of the S_i. Also to each pair of integers i, j there corresponds a unique integer k such that

$$S_i S_j \subset S_k \tag{4}$$

since each element of $S_i S_j$ contains among its powers the idempotent $e_i e_j = e_k$ say, and so belongs to S_k. Further we see that if (4) holds then $S_i < S_k$ for we have

$$e_i e_k = e_i e_i e_j = e_i e_j = e_k.$$

Next we consider a pair of distinct elements a, b of S. Suppose that

$$a \in S_i, \quad b \in S_j.$$

If $i \neq j$ then at most one of $S_i < S_j$ and $S_j < S_i$ can hold. We may assume without loss of generality that $S_j < S_i$ is false. We define the character χ by

$$\chi(z) = x^{\zeta} \pmod{x}$$

where if $z \in S_l$ we have

$$\zeta = \begin{cases} 0 \text{ if } S_l < S_i \\ 1 \text{ otherwise.} \end{cases}$$

This χ satisfies (1). On the other hand if $i = j$ there is a character ψ of S_i with

$$\psi(a) \neq \psi(b).$$

Then we define χ by

$$\chi(z) = \begin{cases} \psi(ze_i) & \text{if } S_l < S_i \\ 0 & \text{otherwise,} \end{cases}$$

and again χ satisfies (1).

5. Theorem 5. *Any finite commutative semigroup S is a homomorphic image of an arithmetical semigroup.*

Proof. Let $z_1, \ldots, z_n$ be the elements of S. We may consider S as a commutative semigroup with generators $z_1, \ldots, z_n$ and a certain set R of relations. For each z_i there is a positive integer n_i such that $z_i^{n_i}$ is an idempotent. Write

$$M = \prod_{i=1}^{n} n_i.$$

Then for each z_i

$$z_i^{2M} = z_i^M \tag{5}$$

https://doi.org/10.1017/S0013091500012529 Published online by Cambridge University Press

is a relation in R. Define T to be the commutative semigroup with generators $z_1, \ldots, z_n$ and relations (5) for $i = 1, \ldots, n$. Thus S is a homomorphic image of T. It suffices to show T is arithmetical.

By Theorem 3 it is sufficient to show that the semigroup U on one generator z with the relation

$$z^{2M} = z^M$$

is arithmetical, for T is a direct sum of n copies of U. Choose two elements z^i, z^j of U. If at least one of i, j is less than M then the character χ defined by

$$\chi(z^k) = x^k \pmod{x^m}$$

has the property

$$\chi(z^i) \neq \chi(z^j). \tag{6}$$

On the other hand if both i and j belong to the closed interval $[M, 2M-1]$ then the character χ given by

$$\chi(z^k) = e^{2\pi ik/M} \pmod{x}$$

satisfies (6), and our proof is complete.

REFERENCES

(1) P. C. Baayen and D. Kruyswijk, A note on the multiplicative semigroup of the residue classes modulo n, *Math. Centrum Amsterdam Afd. Zuivere Wisk.* ZW 1965—007.

(2) A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups*, vol. 1, Math. Surveys of the American Math. Soc. 7 (Providence, R. I., 1961).

The University
Nottingham