PROCEEDINGS OF THE
Cambridge Philosophical Society

VOL. 36 *October*, 1940 PART 4

ON SEMI-GROUPS

BY D. REES

Communicated by P. HALL

Received 5 May 1940

INTRODUCTION

This paper is an attempt to apply the methods of the theory of algebras to the more general problem of the structure of semi-groups, i.e. systems with one composition, satisfying the associative law.

In the first part, the ideas of "ideal" and "difference semi-group" (analogous to difference, or quotient, ring) are borrowed from the theory of algebras, and an analogous theory is developed. This part closes with the linking of this theory with the earlier theory of finite semi-groups, due to Suschkewitsch.†

The second part deals with the theory of the simple semi-group (the analogue of the simple algebra). Certain restrictions are placed on the simple semi-groups considered, and the structure of the simple semi-groups satisfying these restrictions (termed completely simple semi-groups) is completely determined.

1. A set S is said to form a semi-group if it satisfies the following pair of axioms:

I. If a, b are elements of S, they define a third element of S which we denote by ab and term the product of a and b.

II. This product satisfies the associative law, i.e. if a, b, c are elements of S, then $$a(bc) = (ab)c.$$

In what follows we use the letters S, T to denote semi-groups and the letters $a, b, \ldots, x, y, z$ to denote elements of a semi-group.

1·1. The following definitions are elementary:

(a) The symbol a^n, where n is a positive integer, denotes an element defined inductively as follows: $$a^1 = a, \quad a^{n+1} = a^n a.$$

Then it is easily proved that, as a consequence of II above, a^n satisfies the index laws $$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}.$$

We term a^n a power of a.

† A. Suschkewitsch, "Über die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit," *Math. Ann.* 99 (1928), 30–50.

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press

(*b*) An element e is termed an *idempotent* if it satisfies the equation

$$e^2 = e.$$

(*c*) An element O is termed the zero of a semi-group S if

(i) O is an element of S,

(ii) $Ox = xO = O$ for all elements x of S.

Then it is easily seen that the zero of S, if it exists, is uniquely defined. It is also immediately clear that it is an idempotent.

(*d*) An element 1 is termed the identity of a semi-group S if

(i) 1 is an element of S,

(ii) $1x = x1 = x$ for all elements x of S.

Then the identity of S, if it exists, is uniquely defined and is an idempotent.

1·2. We now consider the properties of a semi-group S with the property that every element of S is a power of a certain element a of S. We shall term a the generator of S.

There are two possible cases. First, a may satisfy no equation of the form $a^m = a^n$ $(m \neq n)$. In this case the elements a^n of S are in 1-1 correspondence with the positive integers n. In this correspondence, the product of two elements x, y of S corresponds to the sum of the integers corresponding to x, y. This gives a representation of S, as the set of positive integers, in which the product in the sense of § 1 corresponds to the sum of the integers in the ordinary sense.

Secondly, a may satisfy a relation of the form $a^m = a^n$ $(n > m)$. If a satisfies such a relation, choose one for which n is a minimum. Then clearly $a, a^2, \ldots, a^{n-1}$ are distinct elements of S. Write $n = m + r$. Then, by a simple induction, if q is any positive integer, we have $a^m = a^{m+qr}$. Now, if N is any integer not less than m, we may write it in the form $N = m + qr + s$ $(0 \leqslant s < r)$. Then, by the above,

$$a^N = a^{m+s}. \tag{1·201}$$

Then it follows that the semi-group consists of the $n-1$ elements $a, a^2, \ldots, a^{n-1}$. Further, the r elements $a^m, a^{m+1}, \ldots, a^{n-1}$ form a cyclic group. For let u be the least integer of the form $qr + 1$ greater than m. Write $y = a^u$. Then, by (1·201) above, the set C consisting of the elements $a^m, \ldots, a^{n-1}$ contains all powers of y. But, since u is prime to r, the numbers $u, 2u, \ldots, ru$, taken in some order, are equivalent (mod r) to the numbers $m, m+1, \ldots, n-1$. Hence the elements $y, y^2, \ldots, y^r$ are distinct from one another and coincide with the elements $a^m, a^{m+1}, \ldots, a^{n-1}$. Again, applying (1·201)

$$y^r y^s = y^s y^r = y^{r+s} = y^s,$$

$$y^{r-s} y^s = y^s y^{r-s} = y^r \quad (s \leqslant r).$$

Then the above shows that c is a cyclic group, generated by y, with identity y^r.

Poole has termed m the order, and r the period of S.

The powers of an element a form a semi-group of the type considered above. If this semi-group is of the second type, we say that a is of finite order. Then one

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press

immediate consequence of the above is that any semi-group containing elements of finite order contains an idempotent.

1·21. It is convenient to give the following definitions here:

(*a*) An element a of a semi-group S is termed nilpotent relative to S if, for some integer n, $a^n = O$, where O is the zero of S. As it will usually be clear which semi-group is meant the words "relative to S" will usually be omitted.

(*b*) A semi-group S is termed nilpotent if, for some n, $S^n = O$, i.e. if all products of n elements of S equal the zero element of S.

1·31. Let T be a set of elements of a semi-group S such that $ST \subseteq T (TS \subseteq T)$. Then we term T a *left* (right) *ideal* of S. If T is both a left and a right ideal of S, we say that T is an *ideal* of S. If T contains at least one non-zero element of S, and also does not contain every element of S, we term S a proper (left, right) ideal of S. Unless otherwise stated, all ideals considered in this paper are assumed to be proper ideals.

Let S be a semi-group and T an ideal of S. Let there exist another semi-group S^* and a correspondence between the elements of S and S^* in which each element of S determines an element of S^*, and each element of S^* is determined by at least one element of S. Further, let this correspondence have the following properties:

(i) Every element of T determines the same element of S^*.

(ii) If two elements of S determine the same element of S^*, then both belong to T.

(iii) If a determines a^*, and b determines b^*, then ab determines a^*b^*, i.e. the correspondence between S and S^* is a homomorphism.

It is clear that, given S and T, we can always find a semi-group S^* related to S as above. For take S^* as a set for which a correspondence with S can be defined by (i), (ii) above. Define multiplication in S^* by (iii). Then it can readily be verified that this multiplication is associative. Further, it is clear that the element of S^* determined by T is the zero of S^*. It is also obvious that S^* is uniquely determined, in the sense of isomorphism, by S and T. We term S^* the difference semi-group of S modulo T, and write it as $S - T$.

1·32. Lemma 1·321. *If T_1, T_2 are two ideals of S such that $T_1 \supset T_2$, then*

(i) *$T_1 - T_2$ is an ideal of $S - T_2$,*

(ii) $(S - T_2) - (T_1 - T_2) \cong S - T_1$.

Conversely, if $S - T_2$ contains an ideal X, then the set T_1 of the elements of S which determine the elements of X is an ideal containing T_2 and such that

$$S - T_1 \cong (S - T_2) - X.$$

(i) By the definition, we may consider $T_1 - T_2$ as a subset of $S - T_2$, formed of those elements of $S - T_2$ which are determined by the elements of T_1. Let x^* be an element of $T_1 - T_2$, x an element of T_1 determining it, a^* an element of $S - T_1$,

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press

a an element determining it. Then ax and xa belong to T_1, since T_1 is an ideal. Hence a^*x^*, x^*a^* belong to $T_1 - T_2$, which is therefore an ideal of $S - T_2$.

(ii) The product of the correspondences between S and $S - T_2$, $S - T_2$ and $(S - T_2) - (T_1 - T_2)$ is a homomorphism between S and $(S - T_2) - (T_1 - T_2)$ in which (i), (ii) of § 1·31 are satisfied with $T = T_1$. Hence by definition

$$(S - T_2) - (T_1 - T_2) \cong S - T_1.$$

Conversely, if x^* is any element of X, a^* is any element of $S - T_2$, and x, a are elements of S determining x^*, a^*, respectively, it follows, since x^*a^*, a^*x^* belong to X, that xa, ax belong to the set of elements of S determining the elements of X, i.e. T_1. Hence T_1 is an ideal of S. It is clear that X may be taken as $T_1 - T_2$. Then, by (ii),

$$(S - T_2) - X \cong S - T_1.$$

LEMMA 1·322. *Let T be an ideal of a semi-group, and let R be a sub-semi-group of the same semi-group. Denote by S the set-theory union $R \vee T$ of R and T, and by D the intersection $R \wedge T$. Then S is a semi-group of which T is an ideal, D is an ideal of R and*

$$S - T \cong R - D.$$

Using the alternative notation (T, R) for the set-theory union, we have

$$S^2 = (T, R)^2 = (T^2, TR, RT, R^2) \subseteq (T, R) = S,$$

since T is an ideal of the enveloping semi-group. Hence S is a semi-group.

Since R is a semi-group, $DR \subseteq R$, $RD \subseteq R$. Since $D \subseteq T$, $DR \subseteq T$, $RD \subseteq T$. Hence $DR \subseteq D$, $RD \subseteq D$, i.e. D is an ideal of R.

All elements of S are either in T or R. Hence if we define a correspondence between $S - T$, $R - D$ by making elements correspond which are determined by the same element (considered as an element of S in the first case and as an element of R in the second case), with the addition, if necessary, that the element of $S - T$ determined by T is to correspond to the element of $R - D$ determined by D, this correspondence is easily seen to be an isomorphism between $S - T$ and $R - D$.

The next lemma, both in statement and proof, is a complete analogue of Zassenhaus's lemma in the theory of groups.

LEMMA 1·323. *Let R, S be two sub-semi-groups of a semi-group, and let r, s be ideals of R, S respectively. Write*

$$T = r \vee (R \wedge S), \quad t = r \vee (R \wedge s),$$
$$U = s \vee (R \wedge S), \quad u = s \vee (r \wedge S).$$

Then t, u are ideals of T, U respectively, and

$$T - t \cong U - u.$$

Since $T \subseteq R$, it follows that r is an ideal of T. Further, since s is an ideal of S, $R \wedge s$ is an ideal of $R \wedge S$, as in Lemma 1·322. Hence

$$Tt = Tr \vee \{T(R \wedge s)\} \subseteq t.$$

Similarly

$$tT \subseteq t.$$

Hence t is an ideal of T.

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press

Now $t \vee (R \wedge S) = (r \vee (R \wedge s)) \vee (R \wedge S) = r \vee (R \wedge S) = T.$

Hence, by Lemma 1·322,

$$T - t \cong R \wedge S - ((R \wedge S) \wedge t).$$

But $(R \wedge S) \wedge t = (R \wedge S) \wedge (r \vee (R \wedge s)) = \{(R \wedge S) \wedge r\} \vee \{(R \wedge S) \wedge (R \wedge s)\}$

$$= (r \wedge S) \vee (R \wedge s).$$

Hence $T - t \cong R \wedge S - (r \wedge S) \vee (R \wedge s).$

U, u are obtained from T, t by interchanging R, r with S, s. Hence as above we may prove that u is an ideal of U and that

$$U - u \cong R \wedge S - (r \wedge S) \vee (R \wedge s).$$

Thus $$T - t \cong U - u.$$

1·33. Let S be a semi-group. Then, by analogy with the theory of groups, we define a series of S to be a finite descending sequence of sub-semi-groups of S,

$$S = S_0 \supset S_1 \supset \ldots \supset S_r,$$

where the last term of the series is taken to be the semi-group containing no elements and S_{i+1} is an ideal of S_i. We define the factors of the series to be the difference semi-groups, $S_i - S_{i+1}$ $(i = 0, \ldots, r-1)$. The length of the series is the number of factors. A refinement of the series is any series containing every term S_i of the original series. Two series are termed isomorphic if we can put their factors in 1-1 correspondence so that corresponding factors are isomorphic. Then we have

THEOREM 1·33. *Any two series of a semi-group S,*

$$S = S_0 \supset S_1 \supset \ldots \supset S_r$$

and

$$S = T_0 \supset T_1 \supset \ldots \supset T_s$$

have isomorphic refinements.

The required refinements are, respectively,

$$S = S_{00} \supset S_{01} \supset \ldots \supset S_{0s} = S_{10} \supset \ldots \supset S_{rs},$$

$$S = T_{00} \supset T_{10} \supset \ldots \supset T_{r0} = T_{01} \supset \ldots \supset T_{rs},$$

where $$S_{i,k} = S_{i+1} \vee (S_i \wedge T_k), \quad T_{i,k} = T_{k+1} \vee (T_k \wedge S_i).$$

For, by Lemma 1·323, $S_{i,k} - S_{i,k+1} \cong T_{i,k} - T_{i+1,k}.$

Then, if we define a composition series to be a series without refinements, we obtain as a corollary from the above that all composition series of S are isomorphic.

As in the theory of groups, it may be shown that a necessary and sufficient condition for S to have a composition series is that the maximal and minimal chain conditions should hold for the ideals of S.

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press

1·4. A semi-group S in which the product of any two elements of S is the zero of S, we term a zero semi-group.

It is clear that the zero semi-group of order 2 (the order is equal to the number of elements) has no proper ideals. It is not easy to classify this semi-group with the other semi-groups having this property. Accordingly, following Albert's usage in the theory of algebras, we define a *simple semi-group* to be a semi-group having no proper ideals, and which is not the zero semi-group of order 2.

1·5. In this paragraph we limit ourselves to semi-groups of finite order.

Suschkewitsch has defined the "Kerngruppe" of a semi-group as follows. Let y run through all the elements of S. Consider the sets yS. There exist elements $y_1, \ldots, y_t$ for which the number of elements in yS is a minimum, say r. Suschkewitsch terms the set-theory union K of $y_1S, \ldots, y_tS$, the "Kerngruppe" of S.

It is clear that $KS \subseteq K$. Let a be any element of S. Then ay_iS cannot contain more than r, and hence contains exactly r elements. Hence ay_i is one of the elements $y_1, \ldots, y_t$ and so $ay_iS \subset K$. If we let a run through the elements of S, and let i vary from 1 to t we obtain the result $SK \subseteq K$. Hence K is an ideal, although not necessarily a proper ideal, of S.

Let $x = y_iz$ be an element of K. Then $xy_jS = y_i zy_jS \subset y_iS$. Hence, by the definition of y_i, $xy_jS = y_iS$, and hence, summing over j, we have $xK = y_iS$. Repeating the same argument, if $u = y_kv$, $uxK = y_kS$, and, summing over k, we have $KxK = K$ for every $x \subset K$.

Suppose that K^* is an ideal (not necessarily proper) of K and that x is an element of K^*. Then $K = KxK \subseteq KK^*K \subseteq K^*$. Whence $K = K^*$. Hence it follows immediately that K can have no ideal other than itself, and as a consequence can contain no other ideal of S than itself. Hence K is a minimal ideal of S. This defines K uniquely. For if K_1, K_2 were two minimal ideals of S, then K_1K_2 would be an ideal of S contained in both, which is impossible unless $K_1 = K_2$. It is clear from this new characterization of the "Kerngruppe" that the set K' defined similarly in terms of the sets Sy is equal to K.

If S has a zero O, it is clear from the above that K consists of the element O alone. If S has no zero, it is clear that K cannot have a zero (for this would be an ideal of K not equal to K). Hence K must be a simple semi-group without a zero. Further, if S is a simple semi-group without a zero, it contains no ideal other than itself (we are not here assuming ideals to be proper ideals) and hence K must equal S. Hence the class of "Kerngruppen" is identical with the class of finite simple semi-groups without a zero, together with the zero semi-group of order 1.

2·1. We now prove two simple lemmas, both essentially due to Wedderburn, about semi-groups in general.

LEMMA 2·11. *A necessary and sufficient condition for a semi-group S to be simple is that $SxS = S$ for all non-zero x of S.*

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press

Suppose that the condition is not satisfied. Then there exists an element z of S such that, for some non-zero x of S, $SxS \nmid z$. Let T be the set of all x such that $SxS \nmid z$.

Then clearly $TS \subseteq T$, $ST \subseteq T$. Hence, since T contains some non-zero x and since S is simple, $S = T$.

Hence $S^3 = STS \nmid z$. Therefore $S^3 \neq S$. Whence $S^2 \neq S$ (since, if $S^2 = S$, $S^3 = SS^2 = S$). Hence S^2 is an ideal of S. Since S is simple, S^2 is not a proper ideal. Nor is it the zero ideal (that consisting of the zero element alone). Hence we have a contradiction. Hence $S = SxS$ for all non-zero x of S.

The condition is sufficient since, if T is a proper ideal of S and if x is a non-zero element of T, we have $SxS \subseteq T$, which contradicts $SxS = S$.

LEMMA 2·12. *If S is simple, and e is a non-zero idempotent of S, then eSe is simple also.*

For let T be a proper ideal of eSe. Then $STS \subset S$, since

$$eSTSe = eSeTeSe \subseteq T \subset eSe,$$

and so STS is a proper or zero ideal of S. But, since $STS \supset eTe = T$, it cannot be the zero ideal of S. Hence, if eSe is not simple, neither is S, i.e. the simplicity of S implies that of eSe.

2·2. We say that a non-zero idempotent e of S is *under* an idempotent f, if $eSe \subset fSf$, or (what is the same thing) $ef = fe = e$.

We say that an idempotent e is primitive in S if there is no non-zero idempotent of S under e.

We say that a semi-group S is *completely simple* if it satisfies the following three conditions:

(i) It is simple.

(ii) If x is any element of S, there exist idempotents e, f such that $xe = x$, $fx = x$. Or, what is equivalent, every element x of S belongs to at least one set fSe, where e, f are idempotents.

(iii) There is a primitive idempotent f under every non-primitive idempotent e of S.

The next part of this paper is concerned with the structure of completely simple semi-groups.

2·3. *Every idempotent of a completely simple semi-group is primitive.*

Combining Lemma 2·12 with 2·2 (iii), we see that, if e is a non-zero idempotent of S, then eSe is a simple semi-group with an identity e and containing a primitive idempotent f. Then it is clearly sufficient to show that $e = f$.

Since eSe is simple, there exist $x, \bar{x}$ such that $xf\bar{x} = e$, and we can choose $x, \bar{x}$ so that $xf = x, f\bar{x} = \bar{x}$. Then $x\bar{x} = e$. Further $\bar{x}fx = f$. For if $\bar{x}fx = g$, then $g^2 = g$, and $g \neq O$, since otherwise $f = (fx\bar{x})^2 = O$. Further $fg = gf = g$. Therefore, since f

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press

is primitive, $f = g$. Then $f = efe = x.\bar{x}fx.\bar{x} = xf\bar{x} = e$. Hence we may replace 2·2 (iii) by the simpler but equivalent condition:

(iii)′ Every idempotent of S is primitive.

2·4. The additional restrictions placed on a simple semi-group in the definition of a completely simple semi-group may seem rather arbitrary. The following lemma indicates one important class of simple semi-groups, which are completely simple.

LEMMA 2·4. *If S is a simple semi-group all of whose elements are of finite order, then S is completely simple.*

Let x be any non-zero element of S. Then, since S is simple, there exist b, c, such that $bxc = x$. Then, by a simple induction, $b^n x c^n = x$ for all integers n. Then, by a remark in § 2, we may choose r, s such that $e = b^r$ and $f = c^s$ are idempotents. Then $x = b^{rs}xc^{rs} = e^s x f^r = exf$. Hence $ex = x = xf$, and so S satisfies 2·2 (ii).

Let e be any non-zero idempotent of S. Let f be any non-zero idempotent contained in eSe. Then, since eSe is simple, there exist $x, \bar{x}$, in eSe, such that $xf\bar{x} = e$, and $xf = x, f\bar{x} = \bar{x}$. Then $x\bar{x} = xf\bar{x} = e$. Then by induction, since $xe\bar{x} = e$, we have $x^r f \bar{x}^r = e$. Then as above we can choose r such that $g = x^r$ and $h = \bar{x}^r$ are idempotents, and so $gfh = e$. Then, since e is the identity of eSe, we have

$$g = ge = g.gfh = gfh = e.$$

Similarly $h = e$. Hence $e = efe = f$. Thus e is the only non-zero idempotent contained in eSe, and e must be primitive, i.e. 2·3 (iii)′ and the equivalent 2·2 (iii) are satisfied. Hence S is completely simple.

2·5. Let S be any semi-group. Adjoin to S an idempotent O, and define $Ox = xO = O$. Then we term the semi-group S' thus obtained S with zero adjoined, or simply S with zero. If S is a group, we term S' a group with zero. Then we have

LEMMA 2·5. *A completely simple semi-group S with an identity 1 is either a group or group with zero.*

Let x be a non-zero element of S. Then, since S is simple, there exist elements b, c, such that $bxc = 1$. Then xcb, cbx are idempotents. But, by the definition of a completely simple semi-group, 1 is a primitive idempotent and so must be the only non-zero idempotent of S. Hence $xcb = cbx = 1$, and every non-zero element x has an inverse $x^{-1} = cb$. Further, the non-zero elements of S form a semi-group. For if $xy = O$, where O is the zero of S and $x \neq O$, we have $x^{-1}xy = x^{-1}O = O$, and $x^{-1}xy = 1y = y$. Thus the product of two non-zero elements of S is not zero. Hence the non-zero elements of S form a semi-group with identity, all of whose elements have inverses, i.e. S is a group or group with zero.

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press

Corollary. If S is completely simple and e is a non-zero idempotent of S, then eSe is a group or group with zero. For eSe is then completely simple and has the identity e.

2·6. The following lemmas are based on analogous lemmas of Wedderburn in the theory of algebras, and are essentially the same in proof.

LEMMA 2·61. *If e,f,g are non-zero idempotents of a simple semi-group S, then*
(i) *$eSffSg = eSg$, and*
(ii) *eSf contains at least one non-zero element.*

(i) This follows immediately, since $SfS = S$, by Lemma 2·11.

(ii) If eSf contained only the zero of S, the same would be true of

$$eSe = eSffSe,$$

and this is clearly false, since eSe contains the non-zero element e.

We now make the following notational conventions. We denote non-zero idempotents of a completely simple semi-group S by e,f,g, with or without suffixes, and these symbols are used exclusively for this purpose. This convention is adopted for the rest of the paper. For the remainder of this section we denote the set of elements of e_iSe_j by A_{ij}. Elements of A_{ij} are denoted by the use of the suffixes i,j; for example, x_{ij}. The set of non-zero elements of A_{ij} is denoted by A^*_{ij}.

LEMMA 2·62. (i) *If $x_{ji} \neq O$, then $A_{ij}x_{ji} = A_{ii}$ and $x_{ji}A_{ij} = A_{jj}$*
(ii) *If $x_{ij} \neq O$ and $x_{jk} \neq O$, then $x_{ij}x_{jk} \neq O$.*
(iii) *If $x_{ij} \neq O$, then $x_{ij}A_{jk} = A_{ik}$ and $A_{ki}x_{ij} = A_{kj}$.*
(iv) *If $y_{ij}, y_{ji}, y_{ik}, y_{ki} \neq O$, then $y_{ij}A_{jk}y_{ki} = A_{ii}$ and $y_{ji}A_{ii}y_{ik} = A_{jk}$.*

(i) Let $A_{ij}x_{ji} = P$. Then, since $A_{ji}P = A_{ji}A_{ij}x_{ji} = A_{jj}x_{ji}$ (by Lemma 2·61 (i)), which contains $e_jx_{ji} = x_{ji}$, P must contain an element of A^*_{ii}, say x_{ii}. Then $P = A_{ii}A_{ij}x_{ji} = A_{ii}P \supseteq A_{ii}x_{ii} = A_{ii}$, the last step following from the corollary to Lemma 2·5. Hence $A_{ij}x_{ji} = A_{ii}$. Similarly $x_{ji}A_{ij} = A_{jj}$.

(ii) By (i), there exists a y_{kj} such that $x_{jk}y_{kj} = e_j$, since $x_{jk} \neq O$. Hence $x_{ij}x_{jk}y_{kj} = x_{ij} \neq O$. Therefore $x_{ij}x_{jk} \neq O$.

(iii) $x_{ij}A_{jk} = x_{ij}A_{ji}A_{ik} = A_{ii}A_{ik} = A_{ik}$; $A_{ki}x_{ij} = A_{kj}A_{ji}x_{ij} = A_{kj}A_{jj} = A_{kj}$.

(iv) Apply (iii) twice.

LEMMA 2·63. *The groups A^*_{ii} are isomorphic to one another.*

Choose any two such groups A^*_{ii}, A^*_{jj}. Let y_{ij} be a non-zero element of A_{ij}. There exists such an element by Lemma 2·61 (ii). Then, by 2·62 (i), there exists, in A_{ji}, a non-zero element y_{ji} such that $y_{ij}y_{ji} = e_i$. Then $y_{ji}y_{ij}$ is an idempotent in A_{jj} and is not zero by 2·62 (ii). Hence $y_{ji}y_{ij} = e_j$. Thus the correspondence $x_{ii} \to x_{jj} = y_{ji}x_{ii}y_{ij}$, having the inverse $x_{jj} \to x_{ii} = y_{ij}x_{jj}y_{ji}$, defines an isomorphism between A^*_{ii} and A^*_{jj}.

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press

2·7. LEMMA 2·7. *The sets e_iS and e_jS either have no non-zero elements in common or are identical. Similarly for the sets Se_i and Se_j.*

For suppose e_iS, e_jS have the non-zero element x in common. Then it follows from 2·2 (ii) and Lemma 2·62 (i) that there exists a non-zero element y such that $xy = e_j$. Hence, since $x = e_ix$, $e_iS \supseteq xS \supseteq xyS = e_jS$. Similarly $e_jS \supseteq e_iS$, and so $e_iS = e_jS$.

As a consequence of this lemma it follows that the idempotents fall into classes, two idempotents e_i, e_j belonging to the same class if $e_iS = e_jS$, and to different classes if e_iS, e_jS have no non-zero elements in common. We denote the sets $e_iS, \ldots$ by the symbol R with a suffix, for example R_i, and we adopt the convention that if the suffixes are distinct the sets are distinct. Similarly the sets Se_i are denoted by L with a suffix. The symbol A_{ij} is now used to denote $R_i \wedge L_j$.

2·8. Let S be a semi-group with a zero. (If S has no zero, we may consider the semi-group consisting of S with zero adjoined.) Let L, M be two sets, whose elements are to be used as suffixes. Let $\mathbf{A}$ be a set of elements a_{ik} of S, i varying over L, k over M. We term $\mathbf{A}$ an (L, M) matrix with elements in S. We also denote the matrix whose general element is x_{ik} by (x_{ik}); and the matrix for which $x_{ik} = O$ (the zero of S) for all pairs (i, k) except one, say (a, b), for which $x_{ab} = x$, is denoted by $(x)_{ab}$.

Let $\mathbf{A} = (a_{ij})$ be an (L, M) matrix and $\mathbf{B} = (b_{jk})$ an (M, N) matrix, both matrices having elements in S. Suppose that, for any i, k, at most one of the products $a_{ij}b_{jk}$ is not zero. Define c_{ik} to be equal to the non-zero product $a_{ij}b_{jk}$ if it exists and O (the zero of S) if no such product exists. Then we term the (L, N) matrix $\mathbf{C} = (c_{ik})$ the product of $\mathbf{A}, \mathbf{B}$ and write $\mathbf{C} = \mathbf{AB}$.

Now suppose that S is a semi-group with an identity l. Let $\mathbf{A}$ be an (L, M) matrix subject to the following restrictions:

(i) For any suffix j of L, exactly one a_{jk} does not vanish; and, for any suffix l of M, exactly one a_{il} does not vanish.

(ii) If a_{ik} does not vanish, then it possesses an inverse. Then we term $\mathbf{A}$ a reversible matrix. If (ii) is replaced by the stronger condition that every non-zero $a_{ik} = 1$, we term $\mathbf{A}$ a permutation matrix. It is clear that a necessary and sufficient condition for there to be reversible (L, M) matrices is that L and M should have the same cardinal.

We have the almost trivial

LEMMA 2·8. *If $\mathbf{A} = (a_{lk})$ is a reversible (L, M) matrix, then there exists a reversible (M, L) matrix $\mathbf{A}^* = (a^*_{kl})$ such that $\mathbf{AA}^*, \mathbf{A}^*\mathbf{A}$ are both permutation matrices.*

Define
$$a^*_{ki} = a^{-1}_{ik}, \quad \text{if} \quad a_{ik} \neq O,$$
$$= O, \quad \text{if} \quad a_{ik} = O.$$

Then $\mathbf{A}^* = (a^*_{kl})$ is the required matrix, and is termed the inverse of $\mathbf{A}$.

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press

It is also clear that the product of an (L, M) reversible matrix and an (M, N) reversible matrix exists and is an (L, N) reversible matrix.

Let $\mathbf{A}$ be an (L, M) matrix and $\mathbf{A}^*$ an (L^*, M^*) matrix. Then we term $\mathbf{A}, \mathbf{A}^*$ equivalent matrices if there exist a reversible (L^*, L) matrix $\mathbf{P}$ and a reversible (M, M^*) matrix $\mathbf{Q}$ such that $\mathbf{A}^* = \mathbf{PAQ}$. The justification of the use of the term equivalent is almost immediate.

We also require the following definition. Let ϕ be an automorphism of S and denote the element corresponding to x in ϕ by $x\phi$. Then, if $\mathbf{A} = (a_{ik})$ is a matrix with elements in S, we write $\mathbf{A}\phi$ for the matrix $(a_{ik}\phi)$ and term $\mathbf{A}\phi$ an automorph of $\mathbf{A}$.

2·9. Let S be a semi-group, whose elements are the set of all the (L, M) matrices $(x)_{ab}$, x varying over the non-zero elements of a group with zero G, together with the (L, M) matrix $\mathbf{O}$, all of whose elements equal the zero of G, and in which multiplication is defined in the following manner:

$$(x)_{ab}(y)_{cd} = (x)_{ab}\mathbf{P}(y)_{cd} = (xp_{bc}y)_{ad},$$

$\mathbf{P} = (p_{ki})$ being an (M, L) matrix with elements in G, and the multiplication on the right being the matrix multiplication of 2·8. Then it is easily verified that this definition of multiplication satisfies the associative law. We term S a *matrix semi-group over* G, with defining matrix $\mathbf{P}$. If $\mathbf{P}$ satisfies the conditions that for every suffix l of M, at least one $p_{li} \neq O$ (the zero of G), and that for every suffix j of L at least one $p_{kj} \neq O$, we term S a *regular matrix semi-group, over* G.

With the element $(x)_{ab}$ of S are associated the suffixes a, b of L, M respectively. We term these the first and second suffixes of $(x)_{ab}$. Then, from the definition of multiplication, it follows that the first suffix of a product is the first suffix of its first term and the second suffix of a product is the second suffix of its last term. Hence the set of all elements with a given first suffix a together with the zero matrix (which may be considered to have arbitrary suffixes) form a right ideal R_a, and those with a given second suffix b a left ideal L_b. If S is regular, then there exists a $p_{ka} \neq O$, and accordingly p_{ka}^{-1} exists for some k. Then $(p_{ka}^{-1})_{ak}$ is a non-zero idempotent; and since $(x)_{ab} = (p_{ka}^{-1})_{ak}(x)_{ab}$, we have $R_a = (p_{ka}^{-1})_{ak}S$. Similarly there is a j such that p_{bj}^{-1} exists and $L_b = S(p_{bj}^{-1})_{jb}$. Further $A_{ab} = R_a \subset L_b$ is a sub-semi-group of S. If $pb_a = O$, then $(x)_{ab}(y)_{ab} = (O)_{ab} = \mathbf{O}$, i.e. A_{ab} is a zero semi-group, since $\mathbf{O}$ is clearly the zero of S, and *a fortiori* of A_{ab}. If $p_{ba} \neq O$, then the correspondence $(xp_{ba}^{-1})_{ab} \longleftrightarrow x$ is an isomorphism between G and A_{ab}.

By direct calculation it follows that all non-zero idempotents of S are of the form $(p_{kj}^{-1})_{jk}$. Hence, by the above, it follows that the set eS, where e is an idempotent of S, is the set of all elements having a certain first suffix, and Se is the set of elements with a certain second suffix. Also eSe is isomorphic with G.

THEOREM 2·91. *If two regular matrix semi-groups S and S^* over G, with defining matrices $\mathbf{P}, \mathbf{P}^*$, are isomorphic, then $\mathbf{P}^*$ is equivalent to an automorph of $\mathbf{P}$. Conversely, if $\mathbf{P}^*$ is equivalent to an automorph of $\mathbf{P}$, S^* is isomorphic with S.*

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press

Let $\mathbf{P} = (p_{ki})$ be an (L, M) matrix and let $\mathbf{P}^* = (p^*_{k'i'})$ be an (L', M') matrix. Let α be an isomorphic mapping of S on S^* and denote the image of an element $(x)_{ab}$ of S in this mapping by $(x)_{ab}\alpha$.

The set R_i, of elements of S with the given first suffix i, is the set eS, e being a non-zero idempotent of S. Then $R_i\alpha = (e\alpha)S^*$, and so, since $e\alpha$ is a non-zero idempotent of S^*, $R_i\alpha = R^*_{i'}$, $R^*_{i'}$ being the set of elements of S^* with a given first suffix i'. This fact shows that α defines a mapping of L in L', and since α is an isomorphism, this mapping is a 1-1 correspondence between L and L'. Write this correspondence $i \longleftrightarrow i'$, $(i \subset L, i' \subset L')$. Similarly a 1-1 correspondence $k \longleftrightarrow k'$ may be defined between M and M'.

Then, by the definition of these correspondences, $A_{ik}\alpha = A_{i'k'}$. But A_{ik} (or $A^*_{i'k'}$) is isomorphic with G, if p_{ki} (or $p^*_{k'i'}$) is not zero; and is a zero semi-group if p_{ki} (or $p^*_{k'i'}$) is zero. Hence $p_{ki} = O$ implies $p^*_{k'i'} = O$ and vice versa.

Choose a, b from L, M so that $p_{ba} \neq O$. (This is possible by the assumption of regularity.) Then, by the above, $p^*_{b'a'} \neq O$.

Denote the isomorphic mappings of G on $A_{ab}, A^*_{a'b'}$, given by $x \to (xp^{-1}_{ba})_{ab}$, $x \to (xp^{*-1}_{b'a'})_{a'b'}$, respectively, by ϕ, ψ. Then $\gamma = \phi\alpha\psi^{-1}$ is an automorphism of G.

Introduce the elements

$$l_{ib} = (p^{-1}_{ba})_{ib}, \quad m_{ak} = (1)_{ak}, \quad l^*_{i'b'} = (p^*_{b'a'})_{i'b'}, \quad m^*_{a'k'} = (1)_{a'k'},$$

1 being the identity of G. Then

$$p_{ki}\phi = m_{ak}l_{ib} \tag{2·911}$$

$$p^*_{k'i'}\psi = m^*_{a'k'}l^*_{i'b'}. \tag{2·912}$$

(The image of an element x in a mapping β is denoted by $x\beta$.)

Write

$$l^*_{i'b'}\alpha^{-1} = (c_i)_{ib}, \quad m^*_{a'k'}\alpha^{-1} = (d_k)_{ak}.$$

Then, since $l^*_{i'b'}, m^*_{a'k'}$ are non-zero elements of S^*, c_i, d_k are non-zero elements of G. Then, using the fact that α, ϕ, ψ, and their inverses are all isomorphisms, we have

$$p^*_{k'i'} = (p^*_{k'i'}\psi\alpha^{-1})\alpha\psi^{-1} = (m^*_{a'k'}l^*_{i'b'}\alpha^{-1})\phi^{-1}\gamma,$$

since $\alpha\psi^{-1} = \phi^{-1}\gamma$ by definition of γ, and by (2·912). Thus

$$\begin{aligned} p^*_{k'i'} &= (m^*_{a'k'}\alpha^{-1}l^*_{i'b'}\alpha^{-1})\phi^{-1}\gamma = \{(d_k)_{ak}(c_i)_{ib}\}\phi^{-1}\gamma \\ &= (d_kp_{ki}c_i)_{ab}\phi^{-1}\gamma = (d_k\gamma)p_{ki}\gamma(c_ip_{ba})\gamma. \end{aligned}$$

Write $u_k = d_k\gamma$, $v_i = (c_ip_{ba})\gamma$, and define the (M', M) matrix $\mathbf{U}$ over G by $\mathbf{U} = (u_{l'k})$, where $u_{k'k} = d_k\gamma$, $u_{l'k} = O$ $(l' \neq k)$, and the (L, L') matrix $\mathbf{V} = (v_{ij'})$ by $v_{ii'} = (c_ip_{ba})\gamma$, $v_{ij'} = O$ $(j' \neq i')$. Then $\mathbf{U}, \mathbf{V}$ are reversible matrices and the above shows that $\mathbf{P}^* = \mathbf{UP}\gamma\mathbf{V}$, i.e. $\mathbf{P}^*$ is equivalent to the automorph $\mathbf{P}\gamma$ of $\mathbf{P}$.

Conversely, if $\mathbf{P}^* = \mathbf{UP}\gamma\mathbf{V}$, then, since $\mathbf{U}, \mathbf{V}$ are reversible matrices, there exist inverses $\mathbf{U}^{-1}, \mathbf{V}^{-1}$, and the correspondence $(x)_{ab} \longleftrightarrow \mathbf{V}^{-1}(x^\gamma)_{ab}\mathbf{U}^{-1}$ is an isomorphism between S and S^*. The verification is left to the reader.

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press

The relevance of the introduction of matrix semi-groups depends on the next two theorems.

THEOREM 2·92. *A regular matrix semi-group S over a group with zero G is completely simple.*

Let the elements of S be (L, M) matrices and let $\mathbf{P} = (p_{ki})$ be the defining matrix. Let $(x)_{ab}$ be a non-zero element of S, so that x is a non-zero element of G and so has an inverse x^{-1}. Let $(y)_{cd}$ be any element of S. Then, since S is regular, there exists α in M, β in L, such that $p_{\alpha a}, p_{b\beta}$ are non-zero elements of G and so have inverses. Then $(yp_{\alpha a}^{-1})_{c\alpha}(x)_{ab}(p_{b\beta}^{-1}x^{-1})_{\beta d} = (y)_{cd}$. Hence, by Lemma 2·11, S is simple.

Secondly, with α, β as above, we have $(x)_{ab} = (p_{\alpha a}^{-1})_{a\alpha}(x)_{ab}(p_{b\beta}^{-1})_{\beta b}$. As has already been shown, $(p_{\alpha a}^{-1})_{a\alpha}$, $(p_{b\beta}^{-1})_{\beta b}$ are non-zero idempotents of S. Hence the above equation shows that the second condition for complete simplicity is satisfied.

Thirdly, let $e = (p_{ba}^{-1})_{ab}, f = (p_{dc}^{-1})_{cd}$ be two non-zero idempotents of S. Then if $ef = fe = f$, clearly $a = c$, $b = d$ and $p_{ba} = p_{dc}$. Hence all idempotents of S are primitive and so the third condition for complete simplicity is satisfied.

THEOREM 2·93. *A completely simple semi-group S, with zero, is isomorphic with a regular matrix semi-group over a group G with zero. G is isomorphic with eSe, e being any non-zero idempotent of S.*

Let e be any idempotent of S, and let $R_a = eS$, $L_b = Se$, so that $A_{ab} = eSe$ is a group with zero.

Let G be a group isomorphic with A_{ab}, and let

$$x \longleftrightarrow x_{ab}, \quad x \subset G, \quad x_{ab} \subset A_{ab} \tag{2·931}$$

be an isomorphic correspondence between G and A_{ab}.

From each of the sets A_{ak} choose a non-zero element q_{ak} and, from each of the sets A_{ib}, a non-zero element p_{ib}. The possibility of this choice involves Zermelo's axiom. Then by Lemma 2·62 (iv), we have $p_{ib}A_{ab}q_{ak} = A_{ik}$, so that every element x_{ik} of S can be expressed in the form $p_{ib}x_{ab}q_{ak}$.

Further, there exist p_{bi}, q_{ka}, such that $p_{bi}p_{ib} = e = q_{ak}q_{ka}$. Thus if

$$x_{ik} = p_{ib}x_{ab}q_{ak},$$

then

$$x_{ab} = p_{bi}x_{ik}q_{ka}.$$

Hence the above expression is unique.

The element $q_{ak}p_{ib}$ is clearly an element in A_{ab}. Denote its correlate in G in the correspondence (2·931) by a_{ki}. Denote the (M, L) matrix (a_{ki}) by $\mathbf{A}$, M, L being the sets of suffixes of the L_k and R_i respectively.

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press

Consider the regular matrix semi-group S^* over G, whose elements are the (L, M) matrices $(x)_{ik}$, and whose defining matrix is $\mathbf{A}$. Correlate with the matrix $(x)_{ik}$ the element $p_{ib}x_{ab}q_{ak}$ of S.

Then clearly the correspondence $(x)_{ik} \longleftrightarrow p_{ib}x_{ab}q_{ak}$ is an isomorphism between S and S^*. Hence the theorem is proved.

Corollary. If S is a completely simple group without zero, then S is isomorphic to the semi-group of non-zero elements of a matrix semi-group over a group with zero. For if we adjoin a zero to a completely simple semi-group it remains completely simple.

In conclusion, I would like to express my gratitude to Mr P. Hall, both for his encouragement, while this paper was being written, and his very considerable assistance in preparing the paper for publication.

SIDNEY SUSSEX COLLEGE
CAMBRIDGE

https://doi.org/10.1017/S0305004100017436 Published online by Cambridge University Press