Séminaire Dubreil.
Algèbre et théorie
des nombres

JOHN RHODES

Algebraic theory of finite semigroups

Séminaire Dubreil. Algèbre et théorie des nombres, tome 23, n° 2 (1969-1970), exp. n° DG 10, p. DG1-DG9

<http://www.numdam.org/item?id=SD_1969-1970__23_2_A9_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
23e année, 1969/70
Demi-groupes, n° 10, 9 p.

ALGEBRAIC THEORY OF FINITE SEMIGROUPS

by John RHODES

The viewpoint taken here is the following. We assume the semigroups are finite. No other assumptions are made. We then wish to obtain structure theorems as deep and as detailed as possible, valid for arbitrary finite semigroups. We are not, in general, interested in theorems characterizing special classes of finite semigroups satisfying a long list of restrictive conditions. Thus our viewpoint is similar to the current viewpoint in finite group theory.

There are two main reasons why we have adopted this viewpoint. First, because of applications of finite semigroup theory to languages, automata, biology, finite phase state physics, the complexity of organisms and machines, the complexity of games and codes, etc. See [2], [3], and especially in [20] "A generalization of finite group theory with applications" by RHODES.

For example, the theory of finite state sequential machines and the theory of finite semigroups are essentially identical. See the previous references. However, we will not pursue the applications further here.

The second reason is that we are interested in developing a structure theory of finite semigroups from a purely esthetic motivation. Clearly, a deep general theory of semigroups (with no assumptions) is not possible. A condition like compactness or finite is necessary. We choose finite. However we impose no further conditions. Before 1962, it was thought that it was not possible to develop deep structure theorems for arbitrary finite semigroups. They were too "general" unlike groups. We will see that this is not the case.

In the following, we will synthesize the "classical" work with the "modern" work in finite semigroups. The "classical" work (restricted to finite semigroups) is REES [11], which determines the structure of 0-simple semigroups, and hence the "local" structure of finite semigroups ; the important relations of GREEN [5], which are valid in arbitrary semigroup, but also very important in finite semigroups where further $\mathcal{J} = \mathcal{D}$; the result of CLIFFORD [4], on semigroups which are a union of groups ; the work of the Dubreil school on congruences ; the work of SCHÜTZENBERGER leading to the important Schützenberger representations ([21]), and the theorem of Schützenberger-Preston ([10]), which faithfully represents finite regular semigroups as direct sums of row-monomial matrices with coefficients in a

group ; the work of MUNN [9], which determines the irreducible matrix representations of a finite semigroup.

This work covers the period 1940-1958. In broad outline, these theorems have the flavor of ring theory. One thinks of a semigroup as the multiplicative part of a ring. This is especially true of the work of REES, GREEN and MUNN.

The "modern" period begins in 1962 with the theorem of Krohn and Rhodes ([6]), published in 1965. Later, ZEIGER [24] obtains another proof. Complexity for finite semigroups was defined by RHODES in 1963, and the first paper on complexity appeared by KROHN and RHODES [7], in 1968. Recent major papers on the complexity of finite semigroups are RHODES [13], [14], [15], RHODES and TILSON [18], [19], TILSON [23], and STIFFLER [22].

A survey of the "modern" period 1962-1969 can be found in RHODES [16]. A textbook exposition by KROHN, RHODES and TILSON of the results 1962-1968 can be found in chapters 1, 5-9, of [8]. For recent research, see [20].

The flavor of the "modern" period is much more like group theory. For an exposition of this opinion, see in [20] "A generalization of finite group theory with applications" by RHODES. It is interesting to note that the Schützenberger representations lie more in the "modern" period than in the "classical" period.

Around 1968, Dennis ALLEN Jr discovered that a synthesis of the "classical" and "modern" theories might be possible. He was successful in carrying out the details in some special cases ([1]). In 1969, RHODES carried out the general construction in RHODES and ALLEN [17], using the general ideas of ALLEN and the powerful techniques of [14]. The ideas and constructions of REES, GREEN, KROHN, RHODES and ZEIGER are all explicitly combined here. The result is a true synthesis.

In this short paper, we will briefly exposit the work of the "modern" period and of the "synthesis".

The idea of a structure theory is to "build" an arbitrary finite semigroup from "simpler" pieces ; to make this precise, we must define "build" and "simpler". We begin with the definition of "build".

In the following, all semigroups are of finite order.

Given S , we write $S' \leqslant S$ if, and only if, S' is a subsemigroup of S . We write $T \ll\!\!- S'$ or $S' \twoheadrightarrow T$, if, and only if, there exists an onto homomorphism or surmorphism of S' onto T . We write $T|S$ (read T divides S), if, and only if, T is a homomorphic image of a subsemigroup of S or $T \ll\!\!- S' \leqslant S$. Then, all divisors T of S can be "built" from S .

We next consider Rees construction analogous with the Wedderburn theory for rings. Let S be a semigroup, A and B finite non-empty sets, and $C : B \times A \to S$. Then $\mathcal{M}(S ; A , B ; C)$, the Rees $A \times B$ matrix semigroup with structure semigroup S and structure matrix C, is by definition the semigroup $(A \times S \times B , .)$ with

$$(a_1 , s_1 , b_1).(a_2 , s_2 , b_2) = (a_1 , s_1 C(b_1 , a_1)s_2 , b_2) .$$

Thus $\mathcal{M}(S ; A , B ; C)$ can be "built" from S.

This Rees construction is the most important construction in the "classical" theory, because it determines the "local structure" of a finite semigroup via the following important theorem.

If G is a multiplicatively written group, G^0 is G with a zero 0, $0 \neq 1$, added. We say $C : B \times A \to G^0$ is regular, if, and only if, C is non-zero at least once in each row and column, i. e., for each $b \in B$, there exists an $a \in A$ so that $C(b , a) \neq 0$ and, for each $a \in A$, there exists a $b \in B$ so that $C(b , a) \neq 0$. I is an ideal of S if, and only if, $SI \subseteq I$ and $IS \subseteq I$.

THEOREM (REES [11]). - Let S be a 0-simple semigroup (i. e. $SS \neq 0$, and I an ideal of S implies $I = \{0\}$ or $I = S$). Then, there exists a group G so that S is isomorphic to $\mathcal{M}(G^0 ; A , B ; C)$ with C regular. The converse also holds.

Another construction very popular is the following. Given S, construct the monoid $S + U$ where $+$ denotes disjoint union ; S is an ideal of $S + U$, $1 \in U$, and U is the group of units of $S + U$, i. e.

$U = \{X \in S + U$: there exists $Y , Z \in U + S$ such that $XY = ZX = 1$, where $1 \in U$ is the identity of $S + U\}$.

Informally we say $S + U$ is given by adding a group of units U to S. We give two examples.

First $S \longmapsto S + \{I\}$, where I is a new 2-sided identity for S. Second, let S be the semigroup of all maps of $X_n = \{1 , \ldots , n\}$ into itself under composition which are not one-to-one. Let U be the symmetric group on X_n, i. e. U is all permutations on X_n. Then let $S + U$ = the semigroup of all maps of X_n into itself. Notice $S + U$ is not uniquely determined by S and U, but one must take account also of the action of U on S.

The "building" operations of division, Rees construction, and adding a group of units are "classical" notions. The "simpler" pieces are groups.

We next introduce the "modern" constructions. We are all familiar with the direct

product of two semigroups $S_2 \times S_1$. A generalization of this is the semidirect product defined as follows. Let $Y : S_1 \to \mathrm{Endo}(S_2)$ be a homomorphism of the semigroup S_1 into the semigroup of endomorphisms of S_2 into itself under composition. **Writing** $Y(s_1)(s_2)$ as ${}^{s_1}(s_2)$, we have

$$ {}^{s_1 s_1'}(s_2) = {}^{s_1}\left({}^{s_1'}(s_2)\right) \ , $$

and

$$ {}^{s_1}(s_2\, s_2') = {}^{s_1}(s_2)\ {}^{s_1}(s_2') \ , $$

for all $s_1 , s_1' \in S_1$, $s_2 , s_2' \in S_2$. These conditions are equivalent with Y being an homomorphism. Then $S_2 \times_Y S_1$ (read the semidirect product of S_2 by S_1 with connecting homomorphism Y) is by definition the semigroup $(S_2 \times S_1 , .)$ with

$$ (s_2 , s_1).(s_2' , s_1') = (s_2\ {}^{s_1}(s_2') , s_1\, s_1') \ . $$

In group theory, semidirect products correspond to split extensions, i. e. $N \lhd G$ and $R < G$, where R is both a subgroup and a set of representatives of the cosets of N in G so $NR = G$ and $N \cap R = \{1\}$, implies G is isomorphic with $N \times_Y R$ with $Y(r)(n) \equiv {}^{r}(n) = rnr^{-1}$. For example, D_{2n} , the dihedral group of order $2n$, is isomorphic with $Z_n \times_Y Z_2$ where Z_n is the cyclic group of order n written additively, $Z_2 = (\{\pm 1\} , .)$ and $Y(\varepsilon)(x) = {}^{\varepsilon}(x) = \varepsilon x$.

Also trying $Y(s_1)(s_2) = {}^{s_1}(s_2) = s_2$, we find $S_2 \times_Y S_1 = S_2 \times S_1$, so the semidirect product indeed generalizes the direct product.

Given $S_n , S_{n-1} , \dots , S_1$, we can form $S_n \times_{Y_{n-1}} S_{n-1}$ by choosing some Y_{n-1} and then forming

$$ (S_n \times_{Y_{n-1}} S_{n-1}) \times_{Y_{n-2}} S_{n-2} \ , \quad \text{etc.} \ , $$

yielding finally

$$ (\dots(S_n \times_{Y_{n-1}} S_{n-1}) \times_{Y_{n-2}} S_{n-2} \times_{Y_{n-3}} \dots) \times_{Y_1} S_1 \ . $$

For notational convenience, we denote this last expression by

$$ S = S_n \times_Y S_{n-1} \times_Y \dots \times_Y S_1 \ . $$

Thus S can be "built" from $S_n , \dots , S_1$.

From the "modern" theory, a trivial but important 3-element semigroup U_3 occurs, with $U_3 = \{a , b , 1\}$ and multiplication table

U_3	1	a	b
1	1	a	b
a	a	a	b
b	b	a	b

so $x \in U_3$ implies $x^2 = x$. U_3 acts faithfully on the right of $\{a , b\}$ by $(\{a , b\} , U_3)$, with $x.a = a$ for $x \in \{a , b\}$, $x.b = b$ for $x \in \{a , b\}$, and $x.1 = x$ for $x \in \{a , b\}$. Thus a "destroys the contents and places a ", b "destroys the contents and places b ", 1 "does nothing", so from an engineering point of view, U_3 is a "flip-flop" or basic binary memory device.

In the "modern" theory, semidirect products and division are the modes of "building", and the simple groups (a group G is simple, if, and only if, $N \trianglelefteq G$ implies $N = \{1\}$ or $N = G$) and U_3 are the "simpler" or irreducible pieces. This is made precise in the following theorem which began the "modern period".

THEOREM (KROHN and RHODES [6]). - Given S , then S divides a semidirect product whose terms are simple groups dividing S or U_3 . Precisely, given S , there exists $S_n , \ldots , S_1$ so that

$$(\star) \qquad S | S_n \times_Y \cdots \times_Y S_1 ,$$

where, for each j with $1 \leqslant j \leqslant n$, either S_j is a simple group dividing S or $S_j = U_3$.

Further, if S satisfies $(\star)$, and P is a simple group dividing S , then P divides S_j for some $j = 1 , \ldots , n$.

For other proofs, see [3], and [8], chapter 5.

By definition, S is a combinatorial semigroup, if, and only if, each subgroup of S is a singleton.

Then we have the following corollary.

COROLLARY 1. - S is a combinatorial semigroup, if, and only if,

$$S | U_3 \times_Y \cdots \times_Y U_3 \qquad (\text{n terms}) ,$$

for some n .

By definition, S is an irreducible semigroup, if, and only if, $S | S_2 \times_Y S_1$ implies $S | S_2$ or $S | S_1$. Then we have the following corollary.

COROLLARY 2. - S is an irreducible semigroup, if, and only if, S is a simple group, or S divides U_3.

How can the Rees theorem and the Krohn-Rhodes theorem be synthesized ? One natural way would be to replace semidirect products, in the latter theorem, by the Rees construction and the construction of adjoining groups of units. We proceed to do this.

Let G be a group. (G , G^*) denotes the semigroup G^* acting on the right of the set G , where $G^* = G + \{C_g : g \in G\}$ with $g_1 \cdot g = g_1 g$, $g_1 \cdot C_g = g$, for all $g \in G$. Thus G^* has group of units G and kernel (= minimal 2-sided ideal) $\{C_g : g \in G\}$ with $C_{g_1} C_{g_2} = C_{g_2}$ for all $g_1 , g_2 \in G$. Further, $g_1 C_{g_2} = C_{g_2}$ and $C_{g_2} g_1 = C_{g_2 g_1}$ for all $g_1 , g_2 \in G$.

Suppose groups $G_1 , \dots , G_n$ are given. Then, consider the constructions

$$G_1 \longmapsto G_1^* \longmapsto \mathcal{M}(G_1^* ; A_1 , B_1 ; C_1) \equiv R(G_1^*)$$

$$\longmapsto R(G_1^*) + G_2 \longmapsto \mathcal{M}(R(G_1^*) + G_2 ; A_2 , B_2 ; C_2) \equiv R(R(G_1^*) + G_2)$$

$$\longmapsto R(R(G_1^*) + G_2) + G_3 , \text{ etc.}$$

Here R(S) denotes some Rees matrix semigroup over S , i. e. $\mathcal{M}(S ; A , B ; C)$ for some A , B and C , and $S \longmapsto S + U$ denotes, as was introduced before, adjoining a group of units U to S . Then the promised synthesis is the following.

THEOREM (RHODES and ALLEN [17]). - Let S be given. Then there exists groups $G_1 , G_2 , \dots , G_n$ with G_j dividing S (we allow $G_j = \{1\}$) such that

$$(\star\star) \qquad S \mid \underset{\sim}{R} = R(\dots(R(R(G_1^*) + G_2) + G_3)\dots) + G_n \ .$$

Thus every finite semigroup can be obtained up to division, by using Rees construction, and by adjoining groups of units.

The Rhodes-Allen theorem is deeper than the Krohn-Rhodes theorem, because of the following. In $(\star\star)$, let $S|R$ be given by $S \ll\!\!- T \leq \underset{\sim}{R}$ with $Q : T \twoheadrightarrow S$. Then Q can be choosen to be very "nice", and often T can be choosen to be $\underset{\sim}{R}$. What do we mean by "nice" homomorphisms ?

Let α denote one of the four Green relations $\mathcal{H}$, $\mathcal{L}$, $\mathcal{R}$, or $\mathcal{J} = \mathcal{D}$. Then, by definition, $Q : S \xrightarrow[\gamma(\alpha)]{} T$ if, and only if, Q is one-to-one restricted to each α-class of S . Thus $Q : S \xrightarrow[\gamma(\mathcal{H})]{} T$ if, and only if, $s_1 , s_2 \in S$ and $s_1 \neq s_2$ and $S^1 s_1 = S^1 s_2$ and $s_1 S^1 = s_2 S^1$ all imply $Q(s_1) \neq Q(s_2)$.

Also, by definition, $Q : S \xrightarrow[\alpha]{} T$ if, and only if,

$$Q(s_1) = Q(s_2) \quad \text{implies} \quad s_1 \, \alpha s_2 \text{ in } S .$$

Thus $Q : S \xrightarrow[\mathcal{J}]{} T$ if, and only if,

$$Q(s_1) = Q(s_2) \quad \text{implies} \quad S^1 s_1 S^1 = S^1 s_2 S^1 .$$

Then we have that every arbitrary surmorphism can be decomposed into $\gamma(\mathcal{K})$ and $\mathcal{K}$-epimorphisms, or the following proposition.

PROPOSITION (RHODES [12]). - Let $Q : S \twoheadrightarrow T$. Then there exists

$$S = S_0 , S_1 , \cdots , S_k = T ,$$

and surmorphisms

$$Q_j : S_{j-1} \twoheadrightarrow S_j , \qquad \text{for } j = 1 , \cdots , k + 1 ,$$

such that $Q_k \cdots Q_1 = Q$ and $Q_1 , Q_3 , Q_5 , \cdots$ are $\gamma(\mathcal{K})$, and $Q_2 , Q_4 , Q_6 , \cdots$ are $\mathcal{K}$-surmorphisms.

Now, the restriction of a α-surmorphism to a subsemigroup need not stay a α-surmorphism. To remedy this, one introduces, by definition, $Q : S \xrightarrow[\alpha']{} T$ if, and only if, s_1 and s_2 regular elements of S and $Q(s_1) = Q(s_2)$ imply $s_1 \, \alpha s_2$. Then, it can be proved, using a lemma of Tilson, that the restriction of α'-surmorphism to subsemigroups stay α'-surmorphisms.

Then, in the division $S|R$ of (☆☆) given by $S \xleftarrow{Q} T \leq R$, we can choose R, T and Q satisfying the conditions of the theorem, and such that Q is both a $\gamma(\mathcal{K})$ and $\mathcal{J}'$-surmorphism. Also, if S is regular, we can choose T to be regular, and Q to be $\gamma(\mathcal{K})$ and $\mathcal{J}$. Thus Q can always be chosen to be very "nice".

Also, very often, T can be taken to be all of R. However, precise conditions under which this is the case will not be given here.

Thus, the equation (☆☆) gives a powerful method to study the structure of an arbitrary finite semigroup S.

We might mention in closing that the complexity $\#_G(S)$ of a finite semigroup S is defined as the smallest non-negative integer n such that

$$S | C_n \times_Y G_n \times_Y C_{n-1} \times_Y \cdots \times_Y C_1 \times_Y G_1 \times_Y C_0 ,$$

where $G_1 , \cdots , G_n$ are groups, and $C_0 , \cdots , C_n$ are combinatorial semigroups.

Thus, complexity is the first step in determining all the "minimal" solutions of (☆) given S. Much is known about the complexity of finite semigroups, and it is

important in applications. See [2], [7], [8], [13], [14], [15], [16], [18], [19], [20], [22] and [23].

REFERENCES

[1] ALLEN (D.). - Structure theorems for regular semigroups, Trans. Amer. math. Soc. (to appear).

[2] ARBIB (M. A.), Editor. - Algebraic theory of machines, languages and semigroups. - New York, Academic Press, 1968.

[3] ARBIB (Michael A.). - Theories of abstract automata. - Englewood Cliffs, Prentice-Hall, 1969 (Prentice-Hall Series in Automatic Computation).

[4] CLIFFORD (A. H.). - Semigroups admitting relative inverses, Ann. of Math., 2nd series, t. 42, 1941, p. 1037-1049.

[5] GREEN (J. A.). - On the structure of semigroups, Ann. of Math., 2nd series, t. 54, 1951, p. 163-172.

[6] KROHN (Kenneth) and RHODES (John). - Algebraic theory of machines, I, Trans. Amer. math. Soc., t. 116, 1965, p. 450-464.

[7] KROHN (Kenneth) and RHODES (John). - Complexity of finite semigroups, Ann. of Math., 2nd series, t. 88, 1968, p. 128-160

[8] KROHN (K.), RHODES (J.) and TILSON (B. R.). - [Some lectures on the algebraic theory of finite semigroups and finite-state machines] in Algebraic theory of machines, languages and semigroups, Edited by M. A. Arbib ; chapters 1, 5-9. - New York, Academic Press, 1968.

[9] MUNN (W. D.). - Semigroups and their algebras, Dissertation, Cambridge University, 1955.

[10] PRESTON (G. B.). - Matrix representations of semigroups, Quart. J. Math., Oxford Series, t. 9, 1958, p. 169-176.

[11] REES (D.). - On semigroups, Proc. Cambridge phil. Soc., t. 36, 1940, p. 387-400.

[12] RHODES (John). - A homomorphism theorem for finite semigroups, Math. Systems Theory, t. 1, 1967, p. 289-304.

[13] RHODES (John). - The fundamental lemma of complexity for arbitrary finite semigroups, Bull. Amer. math. Soc., t. 74, 1968, p. 1104-1109.

[14] RHODES (John). - A proof of the fundamental lemma of complexity (weak version) for arbitrary finite semigroups, J. of Comb. Theory (to appear).

[15] RHODES (John). - A proof of the fundamental lemma of complexity (strong version) for arbitrary finite semigroups, J. of Comb. Theory (to appear).

[16] RHODES (John). - Algebraic theory of finite semigroups, Semigroups, Proceedings of a Symposium on semigroups [1968. Detroit], p. 125-162. - New York, Academic Press, 1969.

[17] RHODES (J.) and ALLEN (D.). - Synthesis of the classical and modern theory of finite semigroups, Adv. in Math. (to appear) [See [20]].

[18] RHODES (J.) and TILSON (B. R.). - Lower bounds for complexity of finite semigroups, J. of pure and applied Algebra (to appear).

[19] RHODES (J.) and TILSON (B. R.). - Improved lower bounds for the complexity of finite semigroups, Adv. in Math. (to appear) [See [20]].

[20] RHODES (J.) and TILSON (B. R.), Editors. - Representation theorems for finite semigroups, Adv. in Math. (to appear).

[21] SCHÜTZENBERGER (Marcel Paul). - $\mathcal{D}$ représentations des demi-groupes, C. R. Acad. Sc. Paris, t. 244, 1957, p. 1994-1996.

[22] STIFFLER (P.). - Phil. D. Thesis, Dept of Math., University of California, 1970, to eventually appear in J. of pure and applied Algebra.

[23] TILSON (B. R.). - Complexity of two $\mathcal{J}$-class semigroups, Adv. in Math. (to appear) [See [20]].

[24] ZEIGER (H. P.). - Cascade synthesis of finite-state machines, Inform. and Control, t. 10, 1967, p. 419-433, and erratum.

(Texte reçu le 22 septembre 1970)

John RHODES
Department of Mathematics
University of California
BERKELEY, Calif. (Etats-Unis)