Alan J. Cain

Nine Chapters on the Semigroup Art

Lecture notes for M431 Semigroups

2013 | Porto

version 0.36.1 (2013/08/05)

To download the most recent version, visit
www-groups.mcs.st-and.ac.uk/~alanc/teaching/m431/

Contents

Preface

This course is a tour through selected areas of semigroup theory. There are essentially three parts:

- Chapters 1–3 study general semigroups, including semigroup presentations and basic structure theory.
- Chapters 4–6 examine special classes: namely regular, inverse, and commutative semigroups.
- Chapters 7–9 study finite semigroups, their classification using pseudovarieties, and connections with the theory of automata and regular languages.

There are few formal prerequisites: general mathematical maturity is the main one. A course in elementary group theory provides useful context, and some knowledge of linear algebra will help with understanding certain examples, but neither is essential. For Chapters 8 and 9, some background in formal language theory and universal algebra is useful, but not essential; however, some basic topology is necessary to appreciate Chapter 8 fully.

Each chapter ends with a number of exercises. The most important ones are marked with a star ✶ . Some of the starred exercises are used in proofs in later chapters. Full solutions are supplied for all exercises.

Elementary semigroup theory

1

❁ A *binary operation* $\circ$ on a set S is a map $\circ : S \times S \to S$. This operation is *associative* if $x \circ (y \circ z) = (x \circ y) \circ z$ for all element $x, y, z \in S$. A *semigroup* is a set equipped with an associative binary operation.

Semigroups are therefore one of the most basic types of algebraic structure. We could weaken the definition further by removing the associativity condition and requiring only a binary operation on a set. A structure that satisfies this weaker condition is called a *magma* or *groupoid*. (These 'groupoids' are different from the category-theoretic notion of groupoid.)

On the other hand, we can strengthen the definition by requiring an identity and inverses. Structures satisfying this stronger condition are of course groups. However, there are many more semigroups than groups. For instance, there are 5 essentially different groups with 8 elements (the cyclic group C_8, the direct products $C_4 \times C_2$ and $C_2 \times C_2 \times C_2$, the dihedral group D_4, and the quaternion group Q_8), but there are 3 684 030 417 semigroups with 8 elements.

BASIC CONCEPTS AND EXAMPLES

Throughout this chapter, S will denote a semigroup with operation $\circ$. Formally, we write $(S, \circ)$ to indicate that we are considering the set S with the operations $\circ$, but we will only do this when we need to distinguish a particular operation. Unless we need to distinguish between different operations, we will often write xy instead of $x \circ y$ (where $x, y \in S$) and we will call the operation multiplication and the element xy (i.e. the result of applying the operation to x and y) the *product* of x and y.

Associativity

Since the operation is associative, there is no ambiguity in the product $s_1 s_2 \cdots s_n$ (where each $s_i \in S$): the product is the same regardless of how we insert the brackets.

Any group is also a semigroup. The most familiar example of a semigroup that is not a group is the set of natural numbers $\mathbb{N}$ under the operation of addition. This is not a group since it contains no identity. (For our purposes, $\mathbb{N} = \{1, 2, 3, \ldots\}$ does not include 0.)

Identity

Let e be an element of S. If $ex = x$ for all $x \in S$, the element e is a *left identity*. If $xe = x$ for all $x \in S$, the element e is a *right identity*. If $ex = xe = x$ for all $x \in S$, then e is a *two-sided identity* or simply an *identity*. A semigroup that contains an identity is called a *monoid*.

Zero

Let z be an element of S. If $zx = z$ for all $x \in S$, the element z is a *left zero*. If $xz = z$ for all $x \in S$, the element z is a *right zero*. If $zx = xz = z$ for all $x \in S$, then z is a *two-sided zero* or simply a *zero*.

EXAMPLES 1.1. Let us give some examples of semigroups:

a) The integers $\mathbb{Z}$ form a semigroup under two different operations: addition $+$ and multiplication $\cdot$. The semigroup $(\mathbb{Z}, +)$ is a monoid with identity 0; but in $(\mathbb{Z}, \cdot)$, the element 0 is a zero.

Trivial semigroup

b) The *trivial semigroup* contains only one element e, with multiplication obviously defined by $ee = e$. Since e is (trivially) an identity, this semigroup is also called the *trivial monoid*.

Null semigroup

c) A *null semigroup* is a semigroup with a zero z in which the product of any two elements is z. It is easy to see that this multiplication is associative. Notice that we can define a null semigroup on any set by choosing some element z and defining all products to be z.

Right/left zero semigroup

d) If every element of S is a left zero (that is, $xy = x$ for all $x, y \in S$), then S is a *left zero semigroup*. If every element of S is a right zero (that is, $xy = y$ for all $x, y \in S$) is a *right zero semigroup*. We can define a left zero semigroup on any set X by defining the multiplication $xy = x$ for all $x, y \in X$; it is easy to see that this multiplication is associative.

e) Any ring is a semigroup under multiplication.

Uniqueness of an identity

PROPOSITION 1.2. *If e is a left identity of S and f is a right identity of S then $e = f$. Consequently, a semigroup contains at most one identity.*

Proof of 1.2. Since e is a left identity $ef = f$. Since f is a right identity, $e = ef$. Hence $e = ef = f$. 1.2

Uniqueness of a zero

PROPOSITION 1.3. *If z is a left zero of S and z' is a right zero of S then $z = z'$. Consequently, a semigroup contains at most one zero.*

Proof of 1.3. [See Exercise 1.3.] 1.3

It therefore makes sense to use the special notations 0 and 1 for the unique zero and identity of a semigroup. If we need to specify the zero or identity of a particular semigroup S, we will use 0_S and 1_S.

Adjoining an identity or zero

Let 1 be a new element not in the semigroup S. Extend the multiplication on S to $S \cup \{1\}$ by $1x = x1 = x$ for all $x \in S$ and $11 = 1$. It is easy to prove that this extended multiplication is associative. Then $S \cup \{1\}$ is a monoid with identity 1. Similarly, let 0 be a new element not in S and extend the multiplication on S to $S \cup \{0\}$ by $0x = x0 = 00 = 0$ for all

$x \in S$. Again, this extended multiplication is associative. Then $S \cup \{0\}$ is a semigroup with zero 0. For any semigroup S, define

$$S^1 = \begin{cases} S & \text{if } S \text{ has an identity,} \\ S \cup \{1\} & \text{otherwise;} \end{cases} \qquad S^0 = \begin{cases} S & \text{if } S \text{ has a zero,} \\ S \cup \{0\} & \text{otherwise.} \end{cases}$$

The semigroups S^1 and S^0 are called, respectively, the *monoid obtained by adjoining an identity to S if necessary* and the *semigroup obtained by adjoining a zero to S if necessary*.

Notation for maps

Throughout these notes, mappings are written *on the right* and composed *left to right*. To clarify: let $\varphi : X \to Y$ and $\psi : Y \to Z$ be maps. The result of applying φ to an element x of X is denoted $x\varphi$. The composition of φ and ψ is denoted $\varphi \circ \psi$ or simply $\varphi\psi$, and is a map from X to Z with $x(\varphi\psi) = (x\varphi)\psi$ for all $x \in X$.

Cartesian product

Let $\mathcal{X} = \{X_i : i \in I\}$ be a collection of sets. Informally, the *cartesian product* $\prod_{i\in I}^{\times} X_i$ of the sets in $\mathcal{X}$ is the set of tuples with $|I|$ components, where, for each $i \in I$, the i-th component is an element of X_i. More formally, the cartesian product $\prod_{i\in I}^{\times} X_i$ the set of mappings σ from I to $\bigcup_{i\in I} X_i$ such that $i\sigma \in X_i$ for each $i \in I$. We think the map σ as a tuple with i-th component $i\sigma$. We will use both mapping notation and (especially when the index set I is finite) tuple notation for elements of cartesian products. When $I = \{1, \ldots, n\}$ is finite, we write $X_1 \times \ldots \times X_n$ for $\prod_{i\in I}^{\times} X_i$. When the sets X_i are all equal to a set X (that is, when we consider cartesian products of $|I|$ copies of the set X), we write X^I for $\prod_{i\in I}^{\times} X_i$.

Direct product

Let $\mathcal{S} = \{S_i : i \in I\}$ be a collection of semigroups. The *direct product* of the semigroups in $\mathcal{S}$ is their cartesian product $\prod_{i\in I}^{\times} S_i$ with componentwise multiplication: $(i)(st) = (i)s(i)t$, or, using tuple notation, if $(\ldots, s_i, \ldots)(\ldots, t_i, \ldots) = (\ldots, s_i t_i, \ldots)$. It is easy to prove that this componentwise multiplication is associative, and so the direct product is itself a semigroup.

Exponent

For $x \in S$ and $n \in \mathbb{N}$, define

$$x^n = \overbrace{xx\cdots x}^{n \text{ times}}. \tag{1.1}$$

Notice that, in general, x^n is only defined for positive n. If S is a monoid, define $x^0 = 1_S$. An element x of S is an *idempotent* if $x^2 = x$. The set of idempotents of S is denoted $E(S)$.

Idempotent

Product of subsets

For any subsets X and Y of S, define $XY = \{xy : x \in X, y \in Y\}$. Write xY for $\{x\}Y$ and Xy for $X\{y\}$. Since multiplication in S is associative, so is this product of subsets: for subsets X, Y, and Z of S, we have $X(YZ) = (XY)Z$. By analogy with (1.1), for $X \subseteq S$ and $n \in \mathbb{N}$, define

$$X^n = \overbrace{XX\cdots X}^{n \text{ times}}.$$

Nilpotent semigroup, nilsemigroup

The semigroup S is *nilpotent* if it contains a zero and there exists some

$n \in \mathbb{N}$ such that $S^n = \{0\}$. The semigroup S is a *nilsemigroup* if it contains a zero and for every $x \in S$, there exists some $n \in \mathbb{N}$ such that $x^n = \{0\}$.

Cancellativity

The semigroup S is *left cancellative* if

$$(\forall x, y, z \in S)(zx = zy \Rightarrow x = y);$$

right cancellative if

$$(\forall x, y, z \in S)(xz = yz \Rightarrow x = y);$$

and *cancellative* if it is both left and right cancellative. Note that a non-trivial semigroup with zero cannot be cancellative.

Commutativity

The semigroup S is *commutative* if $xy = yx$ for all $x, y \in S$. For instance $(\mathbb{Z}, +)$ and $(\mathbb{Z}, \cdot)$ are both commutative. A non-trivial left zero semigroup is not commutative.

Left and right inverse

Let M be a monoid. Let $x \in M$. Suppose that there exists an element x' such that $xx' = 1$. Then x' is a *right inverse* for x, and x is *right invertible*. Similarly, suppose there exists an element x'' such that $x''x = 1$. Then x'' is a *left inverse* for x, and x is *left invertible*. If x is both left and right invertible, then x is *invertible*.

Right and left inverses coincide

PROPOSITION 1.4. *Let M be a monoid, and let $x \in M$. Let x' be a right inverse of x and x'' a left inverse. Then $x' = x''$.*

Proof of 1.4. Since x' and x'' are, respectively, right and left inverses of x, we have $xx' = 1$ and $x''x = 1$. Hence $x' = 1x' = x''xx' = x''1 = x''$. 1.4

Thus if x is an invertible element of a monoid M, denote the unique right and left inverse of x by x^{-1}. A monoid in which every element is invertible is of course a *group*.

Regular element

Let $x \in S$. If there is an element $y \in S$ such that $xyx = x$, then the element x is *regular*. Notice that in this case, xy and yx are idempotent, since $(xy)^2 = xyxy = (xyx)y = xy$ and $(yx)^2 = yxyx = y(xyx) = yx$. If every element of S is regular, then S is a *regular semigroup*.

Inverse

An element $x' \in S$ such that $x = xx'x$ and $x'xx' = x'$ is an *inverse* of x.

Notice that this is entirely different from the notion of left/right inverses above. We will never use 'inverse' (on its own) to refer to a left or right inverse.

PROPOSITION 1.5. *Let $x \in S$. Then x has an inverse if and only if x is regular.*

Proof of 1.5. Obviously if x has an inverse, then it is regular. So suppose x is regular. Then there exists $y \in S$ such that $xyx = x$. Let $x' = yxy$. Then $xx'x = x(yxy)x = (xyx)yx = xyx = x$ and $x'xx' = (yxy)x(yxy) = y(xyx)yxy = yxyxy = y(xyx)y = yxy = x'$, so x' is an inverse of x. 1.5

In the proof of Proposition 1.5, the element y might not be an inverse of x: for example, let S be a semigroup with a zero and let $x = 0$ and $y \neq 0$.

An element x can have more than one inverse; see Examples 1.6(e). The set of inverses of x is denoted $V(x)$. Notice also a zero 0 of a semigroup has an inverse, namely 0 itself. In general, if $e \in S$ is idempotent, then $e^3 = e^2 = e$ and so e is an inverse of itself. In particular, every idempotent is regular.

Set of inverses $V(x)$

EXAMPLES 1.6. a) Let $U = \{0, \dots, k\}$ for some $k > 0$. Define an operation $\triangle$ on U by $m \triangle n = \min\{m, n\}$. It is easy to see prove that $\triangle$ is associative, and so $(U, \triangle)$ is a semigroup. Notice that $0 \triangle m = m \triangle 0 = 0$ and $k \triangle m = m \triangle k = m$ for all $m \in U$. Hence U has zero 0 and identity k. Furthermore, $m \triangle m = m$ for all $m \in U$, so every element of U is an idempotent. Finally, $m \triangle n = n \triangle m$ for all $m, n \in U$ and so U is commutative.

b) Define a similar associative operation $\triangle$ on $\mathbb{N} \cup \{0\} = \{0, 1, 2, \dots\}$ by $m \triangle n = \min\{m, n\}$. Then $(\mathbb{N}, \triangle)$ has a zero 0 but has no identity. It is commutative and all its elements are idempotents.

c) Consider the set of all 2×2 integer matrices:

$$M_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z} \right\}.$$

With the usual matrix multiplication, $M_2(\mathbb{Z})$ is a monoid with identity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and zero $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. It is easy to see that $M_2(\mathbb{Z})$ is not commutative, that not all of its elements are idempotents. Since $M_2(\mathbb{Z})$ contains a zero, it is not cancellative.

d) Now let V be the set of all 2×2 integer matrices with non-zero determinant. Again, V is a monoid. Let $P, Q, R \in V$. Suppose $RP = RQ$. Since $\det R \neq 0$, the matrix R has an inverse $R^{-1} \in M_n(\mathbb{Q})$. [Note that $R^{-1} \notin V$ whenever $\det R \neq \pm 1$, so V is not a group.] So $R^{-1}RP = R^{-1}RQ$ and so $P = Q$. Hence V is left-cancellative. Similarly, it is right-cancellative and therefore cancellative.

e) Let L be a left zero semigroup and R a right zero semigroup. Let $B = L \times R$. This semigroup is an $|L| \times |R|$ *rectangular band*, or simply a *rectangular band*. For $(\ell_1, r_1), (\ell_2, r_2) \in B$, we have

Rectangular band

$$(\ell_1, r_1)(\ell_2, r_2) = (\ell_1\ell_2, r_1r_2) = (\ell_1, r_2),$$

since (in particular) ℓ_1 is a left zero and r_2 is a right zero. Thus every element of B is idempotent, since $(\ell, r)(\ell, r) = (\ell, r)$ for all $(\ell, r) \in B$. Furthermore, for any $(\ell_1, r_1), (\ell_2, r_2) \in B$, we have

$$(\ell_1, r_1)(\ell_2, r_2)(\ell_1, r_1) = (\ell_1\ell_2\ell_1, r_1r_2r_1) = (\ell_1, r_1)$$
$$(\ell_2, r_2)(\ell_1, r_1)(\ell_2, r_2) = (\ell_2\ell_1\ell_2, r_2r_1r_2) = (\ell_2, r_2).$$

Hence (ℓ_2, r_2) is an inverse of (ℓ_1, r_1). Thus every element is an inverse of every element.

The name 'rectangular band' comes from the following geometric interpretation of the multiplication. To find the product $(\ell_1, r_1)(\ell_2, r_2)$, take the rectangle two of whose vertices have coordinates (ℓ_1, r_1) and (ℓ_2, r_2). Then the product is the vertex vertcally in line with (ℓ_1, r_1) and horizontally in line with (ℓ_2, r_2), as shown in Figure 1.1

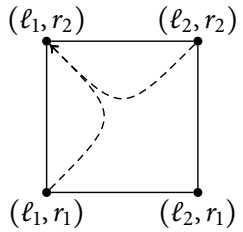


FIGURE 1.1
Geometric interpretation of multiplication in a rectangular band.

GENERATORS AND SUBSEMIGROUPS

Subsemigroup

A non-empty subset T of S is a *subsemigroup* if it is closed under multiplication; that is, if $TT \subseteq T$. A *proper* subsemgroup is any subsemigroup except S itself. A *submonoid* is a subsemigroup that happens to be a monoid. A *subgroup* is a subsemigroup that happens to be a group.

PROPOSITION 1.7. *The set of of invertible elements of a monoid forms a subgroup.*

Proof of 1.7. Let T be the set of invertible elements of a monoid M. Note that T is non-empty since $1 \in T$. Let $x, y \in T$. Then since x and y are invertible we have $y^{-1}x^{-1}xy = y^{-1}y = 1$ and $xyy^{-1}x^{-1} = xx^{-1} = 1$. Hence xy is invertible and so lies in T. Hence T is a subsemigroup of M. Furthermore, $1 \in T$ is also an identity for T and so T is a submonoid of M. Finally, all elements of T are invertible and so T is a subgroup of M. 1.7

Group of units

The set of invertible elements of a monoid is called its *group of units*; Proposition 1.7 justifies this name.

LEMMA 1.8. *Let G be a subset of S. Then $gG = Gg = G$ for all $g \in G$ if and only if G is a subgroup of G.*

Proof of 1.8. Notice first that if G is a subgroup and $g \in G$, then $G = gg^{-1}G \subseteq gG \subseteq G$, so $G = gG$. Similarly $G = Gg$.

For the converse, suppose that $gG = Gg = G$ for all $g \in G$. Let $g, h \in G$. Then $gh \in gG = G$. Hence G is a subsemigroup.

Since $g \in G = Gg$, there exists $e \in G$ such that $eg = g$. Since $h \in G = gG$, we have $h = gx$ for some $x \in G$, whence $eh = egx = gx = h$. Thus e is a left identity for G. Similarly G contains a right identity f, and so $e = f$ is an identity for G by Proposition 1.2. So G is a submonoid with identity 1_G.

Finally, since $1_G \in gG = Gg$, the element g is right and left invertible and its right and left inverses coincide by Proposition 1.4. Since $g \in G$ was arbitrary, G is a subgroup. 1.8

Let $\mathcal{T} = \{T_i : i \in I\}$ be a collection of subsemigroups of S. Then if their intersection $\bigcap \mathcal{T} = \bigcap_{i \in I} T_i$ is non-empty, it is also a subsemigroup. So let $X \subseteq S$ and let $\mathcal{T}$ be the collection of subsemigroups of S that contain X. The collection $\mathcal{T}$ has at least one member, namely the semigroup S itself, and every subsemigroup in $\mathcal{T}$ contains X, so $\bigcap \mathcal{T}$ is non-empty and is thus a subsemigroup. Indeed, it is the smallest subsemigroup of S that contains X. This subsemigroup, denoted $\langle X \rangle$, is called the *subsemigroup generated by X*.

Generating a subsemigroup

If $X \subseteq S$ is such that $\langle X \rangle = S$, then X is a *generating set* for S and X *generates* S. If there is a finite generating set for S, then S is said to be *finitely generated*.

Generating set

PROPOSITION 1.9. *Let $X \subseteq S$. Then $\langle X \rangle = \{x_1 x_2 \cdots x_n : n \in \mathbb{N}, x_i \in X\}$.*

Proof of 1.9. Let $U = \{x_1 x_2 \cdots x_n : x_i \in X\}$. Then U is closed under multiplication and so is a subsemigroup of S. Furthermore, $X \subseteq U$. Hence U must be one of the T_i in $\mathcal{T}$, and so $\langle X \rangle \subseteq U$. Since $X \subseteq \langle X \rangle$ and $\langle X \rangle$ is closed under multiplication, $U \subseteq \langle X \rangle$. Therefore $\langle X \rangle = U$. 1.9

Given a subset X of a monoid M, we can also define the submonoid generated by X. This submonoid is the intersection of all submonoids of M containing whose identities are 1_M: let $\mathcal{T}$ be the collection of submonoids of M containing X and 1_M. The intersection of the submonoids in M is non-empty and thus a submonoid. This is the smallest submonoid of M with identity 1_M that contains X. This submonoid, denoted $\mathrm{Mon}\langle X \rangle$, is called the *submonoid generated by X*. Reasoning similar to the proof of Proposition 1.9 yields the following result:

Generating a submonoid

PROPOSITION 1.10. *Let $X \subseteq M$. Then $Mon\langle X \rangle = \{1_M x_1 x_2 \cdots x_n : n \in \mathbb{N} \cup \{0\}, x_i \in X\}$.* 1.10

Essentially, when we generate a submonoid of a monoid, we always include the identity of the monoid. If $X \subseteq M$ is such that $\mathrm{Mon}\langle X \rangle = M$, then X is a *monoid generating set* for S and *M generates M as a monoid*.

Monoid generator

Notice that if X is a generating set for M, then X is also a monoid generating set; on the other hand, if X is a monoid generating set for M, then $X \cup \{1_M\}$ is a generating set for M. Thus M is finitely generated if and only if there is a finite monoid generating set for M.

Generating set and monoid generating set

Let T be a subset of S. The subset T is a *left ideal* of S if it is closed under left multiplication by any element of S; that is, if $ST \subseteq T$. It is a *right ideal* of S if it is closed under right multiplication by any element of S; that is, if $TS \subseteq T$. It is a *two-sided ideal*, or simply an *ideal*, of S if it is closed under both left and right multiplication by elements of S; that is, if $ST \cup TS \subseteq T$. Every ideal, whether left, right, or two-sided, is a subsemigroup.

Ideal

For any $x \in S$, define $L(x) = S^1 x = \{x\} \cup Sx$, $R(x) = xS^1 = \{x\} \cup xS^1$, and $J(x) = S^1 x S^1 = \{x\} \cup xS \cup Sx \cup SxS$. Then $L(x)$, $R(x)$, and $J(x)$ are,

Principal ideal

respectively, the *principal left ideal generated by x*, *principal right ideal generated by x*, and *principal ideal generated by x*. As their names imply, they are, respectively, a left ideal, a right ideal, and a (two-sided) ideal.

EXAMPLES 1.11. a) Consider the semigroup $(\mathbb{N}, +)$. Let $n \in \mathbb{N}$ and let $I_n = \{m \in \mathbb{N} : m \geq n\}$. Then I_n is an ideal of $\mathbb{N}$; indeed, $I_n = L(n) = R(n) = J(n)$.

b) Let S be a right zero semigroup. Let T be a subset of S. Then $ST = T$ since $xy = y$ for any $x \in S$ and $y \in T$. So T is a left ideal of S. On the other hand $TS = S$ and so T a right ideal if and only if $T = S$.

c) Let G be a group. Let T be a subset of G. For any $x \in G$ and $y \in T$, we have $x = xy^{-1}y \in Gy$; hence $Gy = G$. So T is a left ideal if and only if $T = G$; similarly T is a right ideal if and only if $T = G$. So the only left ideal and right ideal of G is G itself.

Monogenic semigroup

Suppose S is generated by a single element x; that is, $S = \langle\{x\}\rangle = \langle x\rangle$. Then by Proposition 1.9, $S = \{x^n : n \in \mathbb{N}\}$ and we call S the *monogenic semigroup* generated by x.

There are two possibilities: either all the powers of x are distinct or there is some $k, m \in \mathbb{N}$ such that $x^k = x^{k+m}$. In the latter case, x is said to be *periodic*. (Notice that in a finite semigroup, all elements are periodic.) Assume further that k and m are minimal. Then S is finite, with $k + m - 1$ elements, namely

$$x, x^2, \ldots, x^{k-1}, x^k, x^{k+1}, \ldots, x^{k+m-1}.$$

We call k the *index* of x and m the *period* of x. Let $K = \{x^k, x^{k+1}, \ldots, x^{k+m-1}$. It is easy to see that K is an ideal of S. Furthermore, K is a subgroup of S since the integers $k, k+1, \ldots, k+m-1$ are representatives for congruence classes of the integers modulo m. In particular, some power of x is the identity of this subgroup and is therefore an idempotent. A *periodic* semigroup is one in which every element is *periodic*.

BINARY RELATIONS

Recall that a relation ρ between a set X and a set Y is simply a subset of $X \times Y$, and $x \rho y$ is equivalent to $(x, y) \in \rho$. The *identity relation* on X is the relation

$$\mathrm{id}_X = \{(x, x) : x \in X\}.$$

The *converse* ρ^{-1} of ρ is the relation

$$\rho^{-1} = \{(y, x) : (x, y) \in \rho\}.$$


The converse relation ρ^{-1} is not in general an inverse of ρ, even when ρ is a mapping.

Composition of relations

Let ρ be a relation between X and Y and σ be a relation between Y and Z. Define the composition of ρ and σ to be

$$\rho \circ \sigma = \big\{(x,z) \in X \times Z : (\exists y \in Y)\big((x\ \rho\ y) \wedge (y\ \sigma\ z)\big)\big\}. \tag{1.2}$$

Notice that $\rho \circ \sigma$ is a relation between X and Z. Furthermore, notice that $\rho \circ \mathrm{id}_Z = \rho$ and $\mathrm{id}_X \circ \sigma = \sigma$.

Partial/full map

For any $x \in X$, let $x\rho = \{y \in Y : x\ \rho\ y\}$. Then ρ is a *partial map* from X to Y if $|x\rho| \leq 1$ for all $x \in X$. Furthermore, ρ a *full map*, or simply a *map* from X to Y if $|x\rho| = 1$ for all $x \in X$.

Suppose ρ is a partial map from X to Y. When $x\rho$ is the empty set, we say that $x\rho$ is undefined; when $x\rho$ is the singleton set $\{y\}$, we say that $x\rho$ is defined and write $x\rho = y$ instead of $x\rho = \{y\}$.

The definition of a map given here, and the notation in the last paragraph, agrees with the standard concept and notation of a map. Furthermore, when ρ and σ are maps, (1.2) simply defines the usual composition of maps. Thus we have recovered the usual notion of maps in a more general setting.

Domain, image, preimage

For any partial map ρ from X to Y, the *domain* of ρ is the set

$$\mathrm{dom}\,\rho = \big\{x \in X : (\exists y \in Y)\big((x,y) \in \rho\big)\big\}. \tag{1.3}$$

That is, $\mathrm{dom}\,\rho$ is the subset of X on which ρ is defined. If ρ is a map, we have $\mathrm{dom}\,\rho = X$. The *image* of ρ is the set

$$\mathrm{im}\,\rho = \big\{y \in Y : (\exists x \in X)\big((x,y) \in \rho\big)\big\}. \tag{1.4}$$

The *preimage* under ρ of $Y' \subseteq Y$ is the set

$$\begin{aligned} Y'\rho^{-1} &= \{x \in X : (\exists y \in Y')((y,x) \in \rho^{-1})\} \\ &= \{x \in X : (\exists y \in Y')((x,y) \in \rho)\}. \end{aligned}$$

$\mathcal{B}_X$

We will be particularly interested in relations on X; that is, relations from X to itself. Let $\mathcal{B}_X$ denote the set of all binary relations on X. It is easy to show that $\circ$ is an associative operation on $\mathcal{B}_X$ and so $(\mathcal{B}_X, \circ)$ is a semigroup. Furthermore, id_X is an identity and $\mathcal{B}_X$ is a monoid.

Partial/full transformation

$\mathcal{P}_X$, $\mathcal{T}_X$, $\mathcal{S}_X$

A partial map from X to itself is called a *partial transformation* of X. A map from X to itself is called a *full transformation*, or simply a *transformation* of X. The set of all partial transformations of X is $\mathcal{P}_X$; the set of all [full] transformations of X is $\mathcal{T}_X$. Finally, $\mathcal{S}_X$ denotes the set of bijections on X. This is the well-known *symmetric group* on X. Clearly $\mathcal{S}_X \subseteq \mathcal{T}_X \subseteq \mathcal{P}_X \subseteq \mathcal{B}_X$.

PROPOSITION 1.12. a) *$\mathcal{P}_X$ is a submonoid of $\mathcal{B}_X$;*

b) *$\mathcal{T}_X$ is a submonoid of $\mathcal{P}_X$;*

c) *$\mathcal{S}_X$ is a subgroup of $\mathcal{T}_X$.*

Proof of 1.12. a) Let $\rho, \sigma \in \mathcal{P}_X$ and suppose $y, y' \in x(\rho \circ \sigma)$. Then by the definition of $\circ$, there exist $z, z' \in X$ such that $(x, z) \in \rho$ and $(z, y) \in \sigma$, and $(x, z') \in \rho$ and $(z', y') \in \sigma$. Since $\rho \in \mathcal{P}_X$, we have $|x\rho| \leq 1$ and so $z = z'$. Since $\sigma \in \mathcal{P}_X$, we have $|z\sigma| \leq 1$ and so $y = y'$. Hence $|x(\rho \circ \sigma)| \leq 1$ and so $\rho \circ \sigma \in \mathcal{P}_X$.

b) Let $\rho, \sigma \in \mathcal{T}_X$. Let $x \in X$. Since $\rho \in \mathcal{T}_X$, we have $|x\rho| = 1$. So let $z = x\rho$. Since $\sigma \in \mathcal{T}_X$, we have $|z\sigma| = 1$. So $x(\rho \circ \sigma)$ contains $(x, z\sigma)$ and so $|x(\rho \circ \sigma)| \geq 1$. By part a), $|x(\rho \circ \sigma)| = 1$. Therefore $\rho \circ \sigma \in \mathcal{T}_X$.

c) This is immediate because the composition of two bijections is a bijection. 1.12

Any bijection $\rho \in \mathcal{S}_X$ can be denoted by the usual disjoint cycle notation from group theory. A partial (or full) transformation $\rho \in \mathcal{P}_X$ can be denoted using a $2 \times |X|$ matrix: the $(1, x)$-th entry is x and the $(2, x)$-th entry is either $x\rho$ (when $x\rho$ is defined) or $*$ (indicating that $x\rho$ is undefined). For example, if $X = \{1, 2, 3\}$ and $1\rho = 2$, 2ρ is undefined, and $3\rho = 1$, then

$$\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & * & 1 \end{pmatrix}$$

EXAMPLE 1.13. Let $X = \{1, 2\}$. Then

- $\mathcal{S}_X$ consists of two elements: $\mathrm{id}_X = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$;
- $\mathcal{T}_X$ consists of four elements: the two elements in $\mathcal{S}_X$, and the transformations $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$;
- $\mathcal{P}_X$ consists of nine elements: the four elements in $\mathcal{P}_X$, and the partial transformations $\begin{pmatrix} 1 & 2 \\ 1 & * \end{pmatrix}$, $\begin{pmatrix} 1 & 2 \\ 2 & * \end{pmatrix}$, $\begin{pmatrix} 1 & 2 \\ * & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 \\ * & 2 \end{pmatrix}$, and $\begin{pmatrix} 1 & 2 \\ * & * \end{pmatrix}$;
- $\mathcal{B}_X$ consists of all sixteen possible subsets of $X \times X$, including the empty set $\varnothing$ and $X \times X$ itself.

Reflexive, (anti-)symmetric, transitive

There are several important properties that a binary relation may have: a relation $\rho \in \mathcal{B}_X$ is

- *reflexive* if $x \rho x$ for all $x \in X$, or, equivalently, if $\mathrm{id}_X \subseteq \rho$;
- *symmetric* if $x \rho y \Rightarrow y \rho x$ for all $x, y \in X$, or, equivalently, if $\rho = \rho^{-1}$;
- *anti-symmetric* if $(x \rho y) \wedge (y \rho x) \Rightarrow x = y$ for all $x, y \in X$, or, equivalently, if $\rho \cap \rho^{-1} = \mathrm{id}_X$;
- *transitive* if $(x \rho y) \wedge (y \rho z) \Rightarrow x \rho z$ for all $x, y, z \in X$, or equivalently, if $\rho^2 \subseteq \rho$.

Notice that 'anti-symmetric' is not the same as 'not symmetric': for example, the identity relation id_X is both symmetric and anti-symmetric.

An *equivalence relation* is a relation that is reflexive, symmetric, and transitive. An equivalence relation on X partitions X into equivalence classes, each made up of related elements.

Equivalence relation

ORDERS AND LATTICES

Let $\rho \in \mathcal{B}_X$. The binary relation ρ is a *partial order* if it is reflexive, anti-symmetric, and transitive. We normally use symbols like $\leq$, $\preceq$, and $\sqsubseteq$ for partial orders. We write $x < y$ to mean $x \leq y$ and $x \neq y$; the obvious analogies apply for $\prec$ and $\sqsubset$. A *partially ordered set* or *poset* is a set S equipped with a partial order $\leq$, formally denoted $(S, \leq)$.

Partial order

A *Hasse diagram* of a partial order $\leq$ on a set X is a diagrammatic representaion of $\leq$. Every element of X is represented by a point on the plane, arranged so that x appears below y whenever $x < y$. If $x < y$ and there is no element z such that $x < z < y$, then a line segment is drawn between x and y.

Hasse diagram

Suppose $\leq$ is a partial order on X. Two elements $x, y \in X$ are *comparable* if $x \leq y$ or $y \leq x$. The partial order $\leq$ is a *total order*, or simply an *order*, if all pairs of elements of X are comparable.

Total order

Suppose $\leq$ is a partial order on X. A *chain* is a subset Y of X in which every pair of elements are comparable. An *antichain* is a subset Y of X in which no pair of elements is comparable.

Chain and antichain

Let $\rho \in \mathcal{B}_X$. Then ρ is a *quasi-order* if it is a reflexive and transitive.

Quasi-order

EXAMPLES 1.14. a) For example, the relation $\leq$ on the integers $\mathbb{Z}$ is a partial order: it is reflexive, since $m \leq m$ for all m; it is anti-symmetric, since $m \leq n$ and $n \leq m$ imply $m = n$; and it is transitive, since $m \leq n$ and $n \leq p$ imply $m \leq p$.

b) Let X be a set. Recall that the power set $\wp X$ is the set of all subsets of X. The relation $\subseteq$ on $\wp X$ is a partial order. Figure 1.2 shows how the Hasse diagram of $\wp\{1, 2, 3\}$. Notice that $\subseteq$ is not a total order: for instance, $\{1\}$ and $\{2, 3\}$ are incomparable.

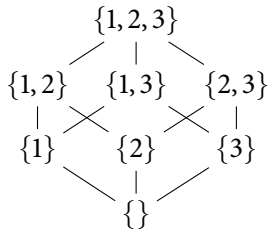


FIGURE 1.2
Hasse diagram for $\subseteq$ on $\wp\{1, 2, 3\}$.

If $x \in X$ is such that there is no element $y \in X$ with $y < x$ (respectively, $x < y$), then x is *minimal* (respectively, *maximal*). If $x \in X$ is such that for all elements $y \in X$, we have $x \leq y$ (respectively $y \leq x$, then x is a *minimum* (respectively, *maximum*). Therefore, in summary:

Minimal/minimum element

$$
\begin{aligned}
x \text{ is minimal} &\Leftrightarrow (\forall y \in X)(y \leq x \Rightarrow y = x);\\
x \text{ is minimum} &\Leftrightarrow (\forall y \in X)(x \leq y);\\
x \text{ is maximal} &\Leftrightarrow (\forall y \in X)(x \leq y \Rightarrow y = x);\\
x \text{ is maximum} &\Leftrightarrow (\forall y \in X)(y \leq x).
\end{aligned}
$$

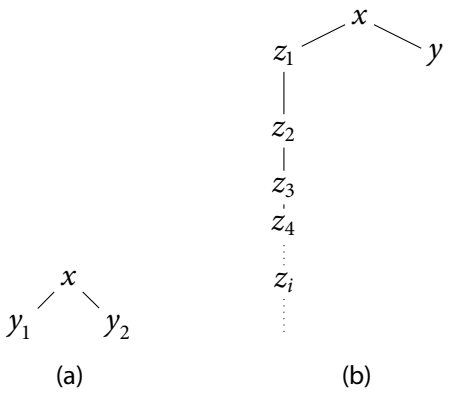


FIGURE 1.3
Examples of partial orders, illustrating minimal/maximal and minimum/maximum elements: (a) has a maximum x and two minimal elements y_1 and y_2; (b) has a unique minimal element y but has no minimum element.

Notice that a minimum element is also minimal, but the converse does not hold. A poset does not have to contain minimum or minimal elements. It contains at most one minimum element, for if x_1 and x_2 are both minimum, then $x_1 \leq x_2$ and $x_2 \leq x_1$, and so $x_1 = x_2$ by anti-symmetry. It may contain many distinct minimal elements.

EXAMPLES 1.15. a) The poset $(\mathbb{Z}, \leq)$ contains neither maximal nor minimal elements.

b) Let $X = \{x, y_1, y_2\}$; define $\leq$ on X by

$$y_1 \leq x, \qquad y_2 \leq x.$$

The Hasse diagram for $(X, \leq)$ is as shown in Figure 1.3(a): x is a (necessarily unique) maximum element, and y_1 and y_2 are both minimal elements.

c) Let $X = \{x, y, z_1, z_2, \dots\}$ and define $\leq$ by

$$\begin{aligned} &y \leq x, \\ &z_i \leq x && \text{for all } i \in \mathbb{N}, \\ &z_i \leq z_j && \text{for all } i, j \in \mathbb{N} \text{ with } i \geq j. \end{aligned}$$

The Hasse diagram for $(X, \leq)$ is as shown in Figure 1.3(b): x is a (necessarily unique) maximum element, and y is the unique minimal element, but y is not a minimum.

Define a relation $\preceq$ on the set of idempotents $E(S)$ by $e \preceq f \Leftrightarrow ef = fe = e$.

PROPOSITION 1.16. *The relation $\preceq$ is a partial order.*

Proof of 1.16. Since $e^2 = e$, we have $e \preceq e$ and so $\preceq$ is reflexive. If $e \preceq f$ and $f \preceq e$, then $ef = fe = e$ and $fe = ef = f$ and so $e = f$; hence $\preceq$ is anti-symmetric. If $e \preceq f$ and $f \preceq g$, then $ef = fe = e$ and $fg = gf = f$ and so $ge = gfe = fe = e$ and $eg = efg = ef = e$ and thus $e \preceq g$; hence $\preceq$ is transitive. Therefore $\preceq$ is a partial order. 1.16

Let $\leq$ be a partial order on a set X. Let $Y \subseteq X$. A *lower bound* for Y is any element z such that $z \leq y$ for all $y \in Y$. Let B be the set of lower bounds for Y. If B is non-empty and contains a maximum element z, then z is the *greatest lower bound* or *meet* of Y. The meet of Y, if it exists, is unique and is denoted by $\bigwedge Y$, or, in the case where $Y = \{x, y\}$, by $z = x \wedge y$.

If $x \wedge y$ exists for all $x, y \in X$, then X is a *meet semilattice* or *lower semilattice*. If $\bigwedge Y$ exists for all $Y \subseteq X$, then X is a *complete meet semilattice* or *complete lower semilattice*.

The obvious definitions apply for *upper bound*, *least upper bound* or *join*, $\bigvee Y$, $x \vee y$, *join semilattice* or *upper semilattice*, and *complete join semilattice* or *complete upper semilattice*.

The ordered set $(X, \leq)$ is a *lattice* if it is an upper and lower semilattice. It is a *complete lattice* if it is an complete upper semilattice and complete lower semilattice.

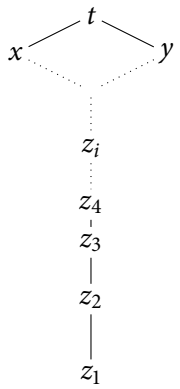


FIGURE 1.4
Partial Hasse diagram for $(X, \leq)$.

EXAMPLE 1.17. a) In the example of $\subseteq$ on $\wp\{1,2,3\}$, we have $\{1,2\} \wedge \{1,3\} = \{1\}$ and $\{1,2\} \wedge \{3\} = \{\}$.

b) Let $X = \{t, x, y, z_1, z_2, \ldots\}$ and define $\leq$ by

$$\begin{aligned} x &\leq t, \\ y &\leq t, \\ z_i &\leq t && \text{for all } i \in \mathbb{N}, \\ z_i &\leq x && \text{for all } i \in \mathbb{N}, \\ z_i &\leq y && \text{for all } i \in \mathbb{N}, \\ z_i &\leq z_j && \text{for all } i, j \in \mathbb{N} \text{ with } i \leq j. \end{aligned}$$

Figure 1.4 shows a partial Hasse diagram for $(X, \leq)$. Notice that x and y do not have a meet, but that every pair of elements have a join. So $(X, \leq)$ is an upper semilattice but not a lower semilattice. However, it is not a *complete* upper semilattice because the subset $\{z_i : i \in \mathbb{N}\}$ does not have a join.

Semilattice = commutative semigroup of idempotents

THEOREM 1.18. a) *Let $(X, \leq)$ be a lower semilattice. Then $(X, \wedge)$ is a commutative semigroup of idempotents.*

Conversely, let $(S, \circ)$ be a commutative semigroup of idempotents. Define a relation $\leq$ on S by $x \leq y \Leftrightarrow x \circ y = x$. Then $\leq$ is a partial order and $(S, \leq)$ is a lower semilattice.

b) *Let $(X, \leq)$ be an upper semilattice. Then $(X, \vee)$ is a commutative semigroup of idempotents.*

Conversely, let $(S, \circ)$ be a commutative semigroup of idempotents. Define a relation $\leq$ on S by $x \leq y \Leftrightarrow x \circ y = y$. Then $\leq$ is a partial order and $(S, \leq)$ is an upper semilattice.

Proof of 1.18. We prove part a); the reasoning for part b) is dual. Suppose $(X, \leq)$ is a lower semilattice. Let $x, y, z \in X$. First, $x \wedge (y \wedge z)$ and $(x \wedge y) \wedge z$

are both the greatest lower bound of $\{x, y, z\}$ and hence $x \wedge (y \wedge z) = (x \wedge y) \wedge z$. So $\wedge$ is associative. Next, $x \wedge y$ and $y \wedge x$ are both the greatest lower bound of $\{x, y\}$, and so $x \wedge y = y \wedge x$. So $(X, \wedge)$ is commutative. The greatest lower bound of $\{x\}$ is x itself, so $x \wedge x = x$. Hence every element of $(X, \wedge)$ is idempotent.

Suppose $(S, \circ)$ is a commutative semigroup of idempotents and define $\leq$ as in the statement of the result. Let $x, y, z \in S$. First, x is idempotent, and so $x \circ x = x$, and thus $x \leq x$. Hence $\leq$ is reflexive. Second, suppose that $x \leq y$ and $y \leq x$. Then $x \circ y = x$ and $y \circ x = y$. Since $(S, \circ)$ is commutative, this shows that $x = y$. Hence $\leq$ is anti-symmetric. Third, suppose $x \leq y$ and $y \leq z$. Then $x \circ y = x$ and $y \circ z = y$. So $x \circ z = (x \circ y) \circ z = x \circ (y \circ z) = x \circ y = x$, and so $x \leq z$. Hence $\leq$ is transitive.

Finally, we want to show that $x \wedge y = x \circ y$. First of all $(x \circ y) \circ x = (x \circ y)$, so $x \circ y \leq x$ and similarly $x \circ y \leq y$. So $x \circ y$ is a lower bound for $\{x, y\}$. Let z be some lower bound for $\{x, y\}$. Then $z \leq x$ and $z \leq y$. Hence $z \circ x = z$ and $z \circ y = z$. So $z \circ (x \circ y) = (z \circ x) \circ y = z \circ y = z$, and so $z \leq (x \circ y)$. Hence $x \circ y$ is the greatest lower bound for $\{x, y\}$. Thus $(S, \leq)$ is a lower semilattice. 1.18

HOMOMORPHISMS

Homomorphism

Let S and T be semigroups. A map $\varphi : S \to T$ is a *homomorphism* if $(xy)\varphi = (x\varphi)(y\varphi)$ for all $x, y \in S$. If S and T are monoids, then φ is a *monoid homomorphism* if if $(xy)\varphi = (x\varphi)(y\varphi)$ for all $x, y \in S$ and $1_S\varphi = 1_T$.

A *monomorphism* is an injective homomorphism. An *epimorphism* is a surjective homomorphism. If $\varphi : S \to T$ is an epimorphism, then T is a *homomorphic image* of S. An *isomorphism* is a bijective homomorphism. It is easy to prove that a homomorphism $\varphi : S \to T$ is an isomorphism if and only if there is a homomorphism $\varphi^{-1} : T \to S$ such that $\varphi\varphi^{-1} = \mathrm{id}_S$ and $\varphi^{-1}\varphi = \mathrm{id}_T$. If there is an isomorphism $\varphi : S \to T$, then we say S and T are *isomorphic* and denote this by $S \simeq T$.

It is easy to prove that if $\varphi : S \to T$ is a homomorphism and S' and T' are subsemigroups of S and T respectively, then $S'\varphi$ is a subsemigroup of T and $T'\varphi^{-1}$ is a subsemigroup of S. In particular, putting $S' = S$ shows that $\operatorname{im}\varphi$ is a subsemigroup of T. If φ is a monomorphism, then S is isomorphic to the subsemigroup $\operatorname{im}\varphi$ of T.

The *kernel* of a homomorphism $\varphi : S \to T$ is the binary relation

$$\ker\varphi = \{(x, y) \in S \times S : x\varphi = y\varphi\}.$$

Notice that φ is a monomorphism if and only if $\ker\varphi$ is the equality re-

lation (that is, $\ker \varphi = \mathrm{id}_S$).

The following result shows that every semigroup is isomorphic to a subsemigroup of a transformation semigroup. This is the analogue of Cayley's theorem for groups, which states that every group is isomorphic to a subgroup of a symmetric group.

Right regular representation

THEOREM 1.19. *For any $x \in S$, let $\rho_x \in \mathcal{T}_{S^1}$ be the map defined by $s\rho_x = sx$ for all $s \in S^1$. Then the map $\varphi : S \to \mathcal{T}_{S^1}$ given by $x \mapsto \rho_x$ is a monomorphism of S.*

Proof of 1.19. Let $x, y, s \in S$. Then $s\rho_x\rho_y = (sx)\rho_y = (sx)y = s(xy) = \rho_{xy}$; hence $(x\varphi)(y\varphi) = \rho_x\rho_y = \rho_{xy} = (xy)\varphi$. Therefore φ is a homomorphism. Furthermore

$$x\varphi = y\varphi \Rightarrow \rho_x = \rho_y \Rightarrow 1\rho_x = 1\rho_y \Rightarrow 1x = 1y \Rightarrow x = y;$$

hence φ is injective. 1.19

A map $\varphi : S \to T$ is an *anti-homomorphism* if $(xy)\varphi = (y\varphi)(x\varphi)$. An *endomorphism* is a homomorphism from a semigroup S to itself. The set of all endomorphisms on S is denoted $\mathrm{End}(S)$ and forms a subsemigroup of $\mathcal{T}_S$.

$\mathrm{End}(S)$

Group-embeddability

A semigroup S is *group-embeddable* if there is a group G and a monomorphism $\varphi : S \to G$. In this case, S is isomorphic to the subsemigroup $\mathrm{im}\, S$ of G. Clearly any group-embeddable semigroup is cancellative, but we shall see that there exist cancellative semigroups that are not group-embeddable (see Example 2.15).

CONGRUENCES AND QUOTIENTS

Congruence

A binary relation ρ on S is

- *left compatible* if $(\forall x, y, z \in S)(x \rho y \Rightarrow zx \rho zy)$;
- *right compatible* if $(\forall x, y, z \in S)(x \rho y \Rightarrow xz \rho yz)$;
- *compatible* if $(\forall x, y, z, t \in S)((x \rho y) \wedge (z \rho t) \Rightarrow xz \rho yt)$.

A left compatible equivalence relation is a *left congruence*; a right compatable equivalence relation is a *right congruence*; and a compatible equivalence relation is a *congruence*.

Congruences are left/right congruences

PROPOSITION 1.20. *A relation ρ on S is a congruence if and only if it is both a left and a right congruence.*

Proof of 1.20. Suppose ρ is both a left and a right congruence. Let $x, y, z, t \in S$ be such that $x \rho y$ and $z \rho t$. Since ρ is a right congruence, $xz \rho yz$. Since ρ is a left congruence $yz \rho yt$. Since ρ is transitive, $xz \rho yt$. Hence ρ is a congruence.

Suppose now that ρ is a congruence. Ley $x, y \in S$ be such that $x \rho y$. Let $z \in S$. Since ρ is reflexive, $z \rho z$. Since ρ is a congruence, $zx \rho zy$ and $xz \rho yz$. Hence ρ is both a left and a right congruence. 1.20

Factor semigroup

Let ρ be a congruence on S. Let S/ρ denote the quotient set of S by ρ (that is, the set of ρ-classes of S). For any $x \in S$, let $[x]_\rho \in S/\rho$ be the ρ-class of x; that is, $[x]_\rho = \{y \in S : y \rho x\}$. Define a multiplication on S/ρ by

$$[x]_\rho[y]_\rho = [xy]_\rho.$$

This multiplication is well-defined, in the sense that if we chose different representatives for the ρ-classes $[x]_\rho$ and $[y]_\rho$, we would get the same answer:

$$\begin{aligned}
&\big([x]_\rho = [x']_\rho\big) \wedge \big([y]_\rho = [y']_\rho\big) \\
&\Rightarrow (x \rho x') \wedge (y \rho y') \\
&\Rightarrow xy \rho x'y' && \text{[since } \rho \text{ is a congruence]} \\
&\Rightarrow [xy]_\rho = [x'y']_\rho.
\end{aligned}$$

The factor set S/ρ, with this multiplication, is called the *quotient* or *factor* of S by ρ. The *natural map* $\rho^\natural : S \to S/\rho$, defined by $x\rho^\natural = [x]_\rho$ is clearly an epimorphism.

First isomorphism theorem

THEOREM 1.21. *Let $\varphi : S \to T$ be a homomorphism. Then* $\ker\varphi$ *is a congruence, and* $S/\ker\varphi \simeq \operatorname{im}\varphi$.

Proof of 1.21. Let $x, y, z, t \in S$. Then

$$\begin{aligned}
&(x, y) \in \ker\varphi \wedge (z, t) \in \ker\varphi \\
&\Rightarrow (x\varphi = y\varphi) \wedge (z\varphi = t\varphi) && \text{[by definition of } \ker\varphi\text{]} \\
&\Rightarrow (x\varphi)(z\varphi) = (y\varphi)(t\varphi) \\
&\Rightarrow (xz)\varphi = (yt)\varphi && \text{[since } \varphi \text{ is a homomorphism]} \\
&\Rightarrow (xz, yt) \in \ker\varphi && \text{[by definition of } \ker\varphi\text{]}
\end{aligned}$$

Define a map $\psi : S/\ker\varphi \to \operatorname{im}\varphi$ by $[x]_{\ker\varphi}\psi = x\varphi$. Now,

$$\left.\begin{aligned}
&[x]_{\ker\varphi} = [y]_{\ker\varphi} \\
&\Leftrightarrow (x, y) \in \ker\varphi && \text{[by definition of } \ker\varphi\text{-classes]} \\
&\Leftrightarrow x\varphi = y\varphi && \text{[by definition of } \ker\varphi\text{]} \\
&\Leftrightarrow [x]_{\ker\varphi}\psi = [y]_{\ker\varphi}\psi. && \text{[by definition of } \psi\text{]}
\end{aligned}\right\} \quad (1.5)$$

The forward implication of (1.5) shows that ψ is well-defined. The reverse implication shows that ψ is injective. The image of ψ is clearly $\operatorname{im}\varphi$. The map ψ is a homomorphism since φ is a homomorphism. Hence ψ is an isomorphism and so $S/\ker\varphi \simeq \operatorname{im}\varphi$. 1.21

Let I be an ideal of S. Then $\rho_I = (I \times I) \cup \mathrm{id}_S$ is a congruence on S. The factor semigroup S/ρ_I is also denoted S/I, and the element $[x]_{\rho_I}$ is denoted $[x]_I$. The congruence ρ_I is called the *Rees congruence* induced by I and S/I is a *Rees factor semigroup*. The elements of S/I are the ρ_I-classes, which comprise I and singleton sets $\{x\}$ for each $x \in S - I$. It is easy to see that I is a zero of the factor semigroup S/I, so it is often convenient to view S/I as having elements $(S-I) \cup \{0\}$, and thinking of forming S/I by starting with S and merging all elements of I to form a zero; see Figure 1.5.

Rees factor semigroup

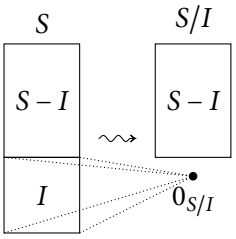


FIGURE 1.5
Forming S/I from S by merging elements of I to form a zero.

PROPOSITION 1.22. *Let I be a proper ideal of S. Let $\mathcal{A}$ be the collection of ideals of S that contain I. Let $\mathcal{B}$ be the collection of the ideals of S/I. Then the map $\varphi : \mathcal{A} \to \mathcal{B}$ given by $J\varphi = J/I$ is a bijection from $\mathcal{A}$ to $\mathcal{B}$ that preserves inclusion, in the sense that $J \subseteq J' \Rightarrow J\varphi \subseteq J'\varphi$.*

A semigroup E is an *ideal extension* of S by T if S is an ideal of E and $E/S \simeq T$. Note that for an ideal extension of S by T to exist, T must contain a zero. Note further that there may be many non-isomorphic semigroups that are ideal extensions of S by T.

Ideal extension

GENERATING EQUIVALENCES AND CONGRUENCES

In this section, we will study how a congruence on a semigroup S is generated by a relation on S. Every result in this section is true for general semigroups, but afterwards we will apply them only to free semigroups and monoids.

For any $\rho \in \mathcal{B}_X$, let

Generating equivalences

$$\rho^{\mathsf{R}} = \bigcap\{\sigma \in \mathcal{B}_X : \rho \subseteq \sigma, \sigma \text{ is reflexive}\},$$
$$\rho^{\mathsf{S}} = \bigcap\{\sigma \in \mathcal{B}_X : \rho \subseteq \sigma, \sigma \text{ is symmetric}\},$$
$$\rho^{\mathsf{T}} = \bigcap\{\sigma \in \mathcal{B}_X : \rho \subseteq \sigma, \sigma \text{ is transitive}\},$$
$$\rho^{\mathsf{E}} = \bigcap\{\sigma \in \mathcal{B}_X : \rho \subseteq \sigma, \sigma \text{ is an equivalence relation}\}.$$

There is at least one element $\sigma \in \mathcal{B}_X$ fulfilling the condition in each of the collections above, namely $\sigma = X \times X$. Furthermore, since every such σ contains ρ, the intersections ρ^{R}, ρ^{S}, ρ^{T}, and ρ^{E} are all non-empty. It is easy to see that

- ρ^{R}, called the *reflexive closure of* ρ, is the smallest reflexive relation containing ρ;
- ρ^{S}, called the *symmetric closure of* ρ, is the smallest symmetric relation containing ρ;

- ρ^{T}, called the *transitive closure of* ρ, is the smallest transitive relation containing ρ;
- ρ^{E}, called the *equivalence relation generated by* ρ, is the smallest equivalence relation containing ρ.

PROPOSITION 1.23. *For any* $\rho \in \mathcal{B}_X$,

a) $\rho^{\mathsf{R}} = \rho \cup \mathrm{id}_X$;
b) $\rho^{\mathsf{S}} = \rho \cup \rho^{-1}$;
c) $\rho^{\mathsf{T}} = \bigcup_{n=0}^{\infty} \rho^n$;
d) $(\rho^{\mathsf{R}})^{\mathsf{S}} = (\rho^{\mathsf{S}})^{\mathsf{R}} = \rho \cup \rho^{-1} \cup \mathrm{id}_X$;
e) $\rho^{\mathsf{E}} = ((\rho^{\mathsf{R}})^{\mathsf{S}})^{\mathsf{T}}$.

Proof of 1.23. [See Exercise 1.19.] 1.23

Generating congruences

For any $\rho \in \mathcal{B}_S$, let

$$\rho^{\mathsf{C}} = \bigcap \{\sigma \in \mathcal{B}_X : \rho \subseteq \sigma, \sigma \text{ is left and right compatible}\},$$
$$\rho^{\#} = \bigcap \{\sigma \in \mathcal{B}_X : \rho \subseteq \sigma, \sigma \text{ is a congruence}\}.$$

It is easy to see that

- ρ^{C} is the smallest left and right compatible relation containing ρ;
- $\rho^{\#}$, called the *congruence generated by* ρ, is the smallest congruence containing ρ.

PROPOSITION 1.24. *For any* $\rho \in \mathcal{B}_S$, *we have* $\rho^{\mathsf{C}} = \{(pxq, pyq) \in S \times S : p, q \in S^1, (x, y) \in \rho\}$.

Proof of 1.24. Let $\sigma = \{(pxq, pyq) \in S \times S : p, q \in S^1, (x, y) \in \rho\}$. To prove $\sigma = \rho^{\mathsf{C}}$, we have to show that σ is the smallest left and right compatible relation on S containing ρ. Notice first that if $(x, y) \in \rho$, then $(x, y) = (1x1, 1y1) \in \sigma$. Hence σ contains ρ. Let $(u, v) \in \sigma$ and $r \in S$. Then $u = pxq$ and $v = pyq$ for some $(x, y) \in \rho$. Let $p' = rp$. Then $(ru, rv) = (p'xq, p'yq) \in \sigma$. Hence σ is left compatible and similarly right compatible.

Now let τ be some left and right compatible relation that contains ρ. Let $(pxq, pyq) \in \sigma$, where $(x, y) \in \rho$ and $p, q \in S^1$. Then $(x, y) \in \tau$ since $\rho \subseteq \tau$. Hence $(pxq, pyq) \in \tau$ since τ is left and right compatible. Hence $\sigma \subseteq \tau$. Hence σ is the smallest left and right compatible relation containing ρ. 1.24

PROPOSITION 1.25. *For any* $\rho, \sigma \in \mathcal{B}_S$,

a) $(\rho \cup \sigma)^{\mathsf{C}} = \rho^{\mathsf{C}} \cup \sigma^{\mathsf{C}}$;
b) $(\rho^{-1})^{\mathsf{C}} = (\rho^{\mathsf{C}})^{-1}$.

Proof of 1.25. [See Exercise 1.20.] 1.25

Characterizing generated congruences

PROPOSITION 1.26. *For any* $\rho \in \mathcal{B}_S$, *we have* $\rho^{\#} = (\rho^{\mathsf{C}})^{\mathsf{E}}$.

Proof of 1.26. We must show that $(\rho^{\mathsf{C}})^{\mathsf{E}}$ is the smallest congruence containing ρ. By definition, $(\rho^{\mathsf{C}})^{\mathsf{E}}$ is an equivalence relation containing ρ^{C}, which in turn contains ρ. So $\rho \subseteq (\rho^{\mathsf{C}})^{\mathsf{E}}$.

Notice that

$$\left.\begin{aligned}
(\rho^{\mathsf{C}})^{\mathsf{E}} &= (((\rho^{\mathsf{C}})^{\mathsf{R}})^{\mathsf{S}})^{\mathsf{T}} && \text{[by Proposition 1.23(e)]}\\
&= (\rho^{\mathsf{C}} \cup (\rho^{\mathsf{C}})^{-1} \cup \mathrm{id}_S)^{\mathsf{T}} && \text{[by Proposition 1.23(d)]}\\
&= ((\rho \cup \rho^{-1} \cup \mathrm{id}_S)^{\mathsf{C}})^{\mathsf{T}} && \text{[by Proposition 1.25]}\\
&= \textstyle\bigcup_{n=0}^{\infty}((\rho \cup \rho^{-1} \cup \mathrm{id}_S)^{\mathsf{C}})^n. && \text{[by Proposition 1.23(c)]}
\end{aligned}\right\} \quad (1.6)$$

Now, for all $x, y, z \in S$,

$$\begin{aligned}
&(x,y) \in (\rho^{\mathsf{C}})^{\mathsf{E}}\\
\Rightarrow\ &(x,y) \in \textstyle\bigcup_{n=0}^{\infty}((\rho \cup \rho^{-1} \cup \mathrm{id}_S)^{\mathsf{C}})^n && \text{[by (1.6)]}\\
\Rightarrow\ &(\exists n \in \mathbb{N})\big((x,y) \in ((\rho \cup \rho^{-1} \cup \mathrm{id}_S)^{\mathsf{C}})^n\big)\\
\Rightarrow\ &(\exists n \in \mathbb{N})(\exists x_0, x_1, \ldots, x_n \in S)\big[(x = x_0) \wedge (x_n = y)\\
&\qquad \wedge (\forall i)\big((x_i, x_{i+1}) \in (\rho \cup \rho^{-1} \cup \mathrm{id}_S)^{\mathsf{C}}\big)\big] && \text{[by definition of } \circ]\\
\Rightarrow\ &(\exists n \in \mathbb{N})(\exists x_0, x_1, \ldots, x_n \in S)\big[(zx = zx_0) \wedge (zx_n = zy)\\
&\qquad \wedge (\forall i)\big((zx_i, zx_{i+1}) \in (\rho \cup \rho^{-1} \cup \mathrm{id}_S)^{\mathsf{C}}\big)\big]\\
&\qquad\qquad \text{[since } (\rho \cup \rho^{-1} \cup \mathrm{id}_S)^{\mathsf{C}} \text{ is left and right compatible]}\\
\Rightarrow\ &(\exists n \in \mathbb{N})\big((zx, zy) \in ((\rho \cup \rho^{-1} \cup \mathrm{id}_S)^{\mathsf{C}})^n\big) && \text{[by definition of } \circ]\\
\Rightarrow\ &(zx, zy) \in \textstyle\bigcup_{n=0}^{\infty}((\rho \cup \rho^{-1} \cup \mathrm{id}_S)^{\mathsf{C}})^n\\
\Rightarrow\ &(zx, zy) \in (\rho^{\mathsf{C}})^{\mathsf{E}}. && \text{[by (1.6)]}
\end{aligned}$$

Therefore $(\rho^{\mathsf{C}})^{\mathsf{E}}$ is left compatible. Similarly, $(\rho^{\mathsf{C}})^{\mathsf{E}}$ is right compatible. Hence $(\rho^{\mathsf{C}})^{\mathsf{E}}$ is a congruence containing ρ.

Now suppose that τ is a congruence containing ρ. Then τ is left and right compatible and so must contain ρ^{C}, which is the smallest left and right compatible relation containing ρ. Furthermore, τ is an equivalence relation, and so it must contain $(\rho^{\mathsf{C}})^{\mathsf{E}}$, which is the smallest equivalence relation containing ρ^{C}. Hence $(\rho^{\mathsf{C}})^{\mathsf{E}} \subseteq \tau$. Therefore $(\rho^{\mathsf{C}})^{\mathsf{E}}$ is the smallest congruence containing ρ. 1.26

Lattice of congruences

Let $\mathcal{E}_S$ be the set of equivalence relations on S and let $\mathcal{C}_S$ be the set of congruences on S. Then $\mathcal{E}_S$ and $\mathcal{C}_S$ both admit $\subseteq$ as a partial order. It is easy to see that both $(\mathcal{E}_S, \subseteq)$ and $(\mathcal{C}_S, \subseteq)$ are actually lattices:

- for any $\rho, \sigma \in \mathcal{E}_S$, we have $\rho \wedge \sigma = \rho \cap \sigma$ and $\rho \vee \sigma = (\rho \cup \sigma)^{\mathsf{E}}$;
- for any $\rho, \sigma \in \mathcal{C}_S$, we have $\rho \wedge \sigma = \rho \cap \sigma$ and $\rho \vee \sigma = (\rho \cup \sigma)^{\#}$.

Suppose $\rho, \sigma \in \mathcal{C}_S$. There seems to be an ambiguity in writing $\rho \vee \sigma$: do we mean the join $(\rho \cup \sigma)^{\mathsf{E}}$ in the lattice of equivalence relations $\mathcal{E}_S$, or the

join $(\rho \cup \sigma)^{\#}$ in the lattice of congruences C_S? However,

$$\begin{aligned}(\rho \cup \sigma)^{\#} &= ((\rho \cup \sigma)^{\mathsf{C}})^{\mathsf{E}} && \text{[by Proposition 1.26]}\\ &= (\rho^{\mathsf{C}} \cup \sigma^{\mathsf{C}})^{\mathsf{E}} && \text{[by Proposition 1.25(a)]}\\ &= (\rho \cup \sigma)^{\mathsf{E}}. && \text{[since } \rho, \sigma \text{ are compatible]}\end{aligned}$$

So there is really no ambiguity in writing $\rho \vee \sigma$.

Characterizing join of equivalence relations

PROPOSITION 1.27. *Let $\rho, \sigma \in \mathcal{E}_S$. Then $\rho \vee \sigma = (\rho \circ \sigma)^{\mathsf{T}}$.*

Proof of 1.27. Let $\rho, \sigma \in C_S$. Since $\rho \cup \sigma$ contains both ρ and σ, it follows that

$$\rho \circ \sigma \subseteq (\rho \cup \sigma) \circ (\rho \cup \sigma) = (\rho \cup \sigma)^2,$$

and more generally that $(\rho \circ \sigma)^n \subseteq (\rho \cup \sigma)^{2n}$. Thus

$$(\rho \circ \sigma)^{\mathsf{T}} = \bigcup_{n=0}^{\infty} (\rho \circ \sigma)^n \subseteq \bigcup_{n=0}^{\infty} (\rho \cup \sigma)^n = (\rho \cup \sigma)^{\mathsf{T}}. \tag{1.7}$$

On the other hand, $\rho \circ \sigma$ contains $\rho \circ \mathrm{id}_S = \rho$ (since σ is reflexive) and $\mathrm{id}_S \circ \sigma = \sigma$ (since ρ is reflexive), and thus $\rho \cup \sigma \subseteq \rho \circ \sigma$. Hence $(\rho \cup \sigma)^{\mathsf{T}} \subseteq (\rho \circ \sigma)^{\mathsf{T}}$. Combine this with (1.7) to see that

$$(\rho \cup \sigma)^{\mathsf{T}} = (\rho \circ \sigma)^{\mathsf{T}}. \tag{1.8}$$

Then

$$\begin{aligned}&\rho \vee \sigma\\ &= (\rho \cup \sigma)^{\mathsf{E}}\\ &= (((\rho \cup \sigma)^{\mathsf{R}})^{\mathsf{S}})^{\mathsf{T}} && \text{[by Proposition 1.23(e)]}\\ &= ((\rho \cup \sigma) \cup (\rho \cup \sigma)^{-1} \cup \mathrm{id}_S)^{\mathsf{T}} && \text{[by Proposition 1.23(d)]}\\ &= (\rho \cup \sigma \cup \rho^{-1} \cup \sigma^{-1} \cup \mathrm{id}_S)^{\mathsf{T}}\\ &= (\rho \cup \sigma)^{\mathsf{T}} && \text{[since } \rho \text{ and } \sigma \text{ are reflexive and symmetric]}\\ &= (\rho \circ \sigma)^{\mathsf{T}}. && \text{[by (1.8)]}\end{aligned}$$

This completes the proof. 1.27

Join of commuting equivalence relations

PROPOSITION 1.28. *Let $\rho, \sigma \in \mathcal{E}_S$. If $\rho \circ \sigma = \sigma \circ \rho$, then $\rho \vee \sigma = \rho \circ \sigma$.*

Proof of 1.28. Suppose $\rho \circ \sigma = \sigma \circ \rho$. Then

$$\begin{aligned}(\rho \circ \sigma)^2 &= \rho \circ \sigma \circ \rho \circ \sigma\\ &= \rho \circ \rho \circ \sigma \circ \sigma && \text{[since } \rho \circ \sigma = \sigma \circ \rho]\\ &= \rho \circ \sigma. && \text{[since } \rho \text{ and } \sigma \text{ are transitive]}\end{aligned}$$

Hence $(\rho \circ \sigma)^n = \rho \circ \sigma$ for all n, and hence

$$\begin{aligned}\rho \vee \sigma &= (\rho \circ \sigma)^{\mathsf{T}} && \text{[by Proposition 1.27]}\\ &= \textstyle\bigcup_{n=0}^{\infty} (\rho \circ \sigma)^n && \text{[by Proposition 1.23(c)]}\\ &= \rho \circ \sigma.\end{aligned}$$

1.28

SUBDIRECT PRODUCTS

Let $\mathcal{S} = \{S_i : i \in I\}$ be a collection of semigroups. For each $j \in I$, there is a projection map from the direct product $\prod^{\times}_{i\in I} S_i$ onto S_j, taking an element of the direct product to its j-th compontent:

$$\pi_j : \prod_{i\in I}^{\times} S_i \to S_j, \qquad x\pi_j = (j)x.$$

Notice that every π_j is a epimorphism.

Subdirect product

A *subdirect product* of $\mathcal{S}$ is [a semigroup isomorphic to] a subsemigroup P of the direct product $\prod^{\times}_{i\in I} S_i$ such that $P\pi_j = S_j$ for all $j \in I$.

Separation by epimorphisms

Let S be a semigroup. A collection of epimorphisms $\Phi = \{\varphi_i : S \to S_i : i \in I\}$ is said to *separate* the elements of S if they have the property that

$$(\forall i \in I)(x\varphi_i = y\varphi_i) \Rightarrow x = y.$$

PROPOSITION 1.29. *A semigroup S is a subdirect product of a collection of semigroups $\mathcal{S} = \{S_i : i \in I\}$ if and only if there exists a collection of epimorphisms $\Phi = \{\varphi_i : S \to S_i : i \in I\}$ that separate the elements of S.*

Proof of 1.29. If S is a subdirect product of $\mathcal{S}$, then the collection of projection maps restricted to S (that is, the collection $\{\pi_i|_S : S \to S_i : i \in I\}$) separates the elements of S.

On the other hand, suppose the collection Φ separates the elements of S. Define $\psi : S \to \prod^{\times}_{i\in I} S_i$ by letting the i-th component of $s\psi$ be $s\varphi_i$; that is, $(i)(s\psi) = s\varphi_i$. Then ψ is a homomorphism since each φ_i is a homomorphism. Furthermore, $s\psi = t\psi$ implies that $s\varphi_i = t\varphi_i$ for all $i \in I$, which implies $s = t$ since Φ separates the elements of S. Hence ψ is injective. So S is isomorphic to the subsemigroup $\operatorname{im}\psi$ of $\prod^{\times}_{i\in I} S_i$. Finally, the projection maps π_i are all surjective since each φ_i is surjective. So $\operatorname{im}\varphi$ is a subdirect product of $\mathcal{S}$. 1.29

PROPOSITION 1.30. *Let S be a semigroup and let $\Sigma = \{\sigma_i : i \in I\}$ be a collection of congruences on S. Let $\sigma = \bigcap \Sigma$. Then S/σ is a subdirect product of $\{S/\sigma_i : i \in I\}$.*

Proof of 1.30. For each i there is a homomorphism $\varphi_i : S/\sigma \to S/\sigma_i$ with $[x]_\sigma\varphi_i = [x]_{\sigma_i}$. (These maps are well-defined since $\sigma \subseteq \sigma_i$.) Clearly, the homomorphisms φ_i are surjective. Furthermore, the collection $\Phi = \{\varphi_i : i \in I\}$ separates the elements of S/σ, since if $[x]_\sigma\varphi_i = [y]_\sigma\varphi_i$ for all $i \in I$, then $[x]_{\sigma_i} = [y]_{\sigma_i}$ and thus $(x, y) \in \sigma_i$ for all $i \in I$, which implies $(x, y) \in \sigma = \bigcap \Sigma$ and so $[x]_\sigma = [y]_\sigma$. Therefore S/σ is a subdirect product of $\{S/\sigma_i : i \in I\}$ by Proposition 1.29. 1.30

PROPOSITION 1.31. *Let M be a monoid and let E be an ideal extension of M by T. Then E is a subdirect product of M and T.*

Proof of 1.31. Let $\varphi : E \to T$ be the natural homomorphism $x\varphi = [x]_M$. Let $\psi : E \to M$ be given by $x\psi = x1_M$. Then

$$\begin{aligned}(x\psi)(y\psi) &= x1_M y1_M \\ &= xy1_M && \text{[since } y1_M \text{ lies in the ideal } M \text{ of } E\text{]} \\ &= (xy)\psi.\end{aligned}$$

Thus ψ is a homomorphism. Both φ and ψ are clearly surjective. Furthermore, if $x\varphi = y\varphi$ and $x\psi = y\psi$, then either $x, y \in E - M$ and $[x]_M = [y]_M$ and so $x = y$, or $x, y \in M$ and $x1_M = y1_M$ and so $x = y$. Thus the collection of epimorphisms $\{\varphi, \psi\}$ separates elements of E and so E is a subdirect product of M and T. 1.31

ACTIONS

Semigroup action

A *semigroup action* of a semigroup S on a set A is an operation $\cdot : A \times S \to A$ that is compatible with the semigroup multiplication, in the sense that

$$(a \cdot x) \cdot y = a \cdot (xy) \tag{1.9}$$

for all $a \in A$ and $x, y \in S$. We call such a semigroup action an *action of S on A*, or an *S-action on A*, and say that S *acts on* A.

EXAMPLES 1.32. a) Any subsemigroup S of $\mathcal{T}_A$ acts on A by $a \cdot \rho = a\rho$ (where $\rho \in \mathcal{T}_A$).

b) Let S be a subsemigroup of a semigroup T. Then S acts on T via $t \cdot x = tx$ for all $t \in T$ and $x \in S$. In particular, this holds when $T = S$ or when $T = S^1$.

Given an action $\cdot$, we can define a map $\varphi : S \to \mathcal{T}_A$, where the transformation $s\varphi$ is such that $a(s\varphi) = a \cdot s$. The condition (1.9) implies that φ is a homomorphism. Conversely, given a homomorphism $\varphi : S \to \mathcal{T}_A$, we can define an action $\cdot$ by $a \cdot s = a(s\varphi)$, which satisfies (1.9) since φ is a homomorphism. There is thus a one-to-one correspondence between actions of a semigroup S on A and homomorphisms $\varphi : S \to \mathcal{T}_A$.

Free, transitive, regular actions

An action of S on A is *free* if distinct elements of S act differently on every element of A, or, equivalently,

$$(\forall x, y \in S)\big((\exists a \in A)(a \cdot x = a \cdot y) \Rightarrow x = y\big).$$

An action of S on A is *transitive* if for all $a, b \in A$, there is some element of $s \in S$ such that $a \cdot s = b$. An action is *regular* if it is both free and transitive.

Suppose A is also a semigroup. An action of S on A is *by endomorphisms* if $s\varphi \in \operatorname{End} A$ for each $s \in S$; in this case,

$$ab \cdot x = (a \cdot x)(b \cdot x)$$

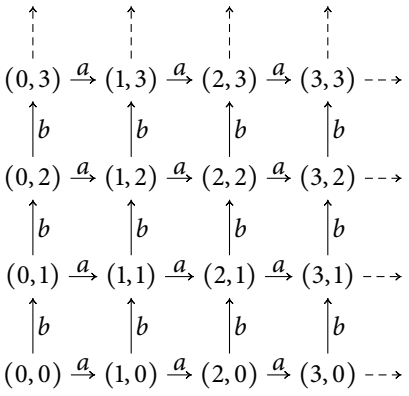


FIGURE 1.6
Cayley graph of $S = (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\})$.

for all $a, b \in A$ and $x \in S$.

Left action

The above discussions concern a *right* semigroup actions. There is a dual notion of a *left semigroup action* of S on A, which is an operation $\cdot : S \times A \to A$ satisfying

$$s \cdot (t \cdot a) = (st) \cdot a;$$

this corresponds to a map $\varphi : S \to \mathcal{T}_A$, where $a(s\varphi) = s \cdot a$. This map φ is an anti-homomorphism since

$$a(t\varphi)(s\varphi) = (t \cdot a)(s\varphi) = s \cdot (t \cdot a) = st \cdot a = a((st)\varphi).$$

The definitions of actions being free, transitive, regular, and by endomorphism also apply to left actions.

The correspondence of right actions with homomorphisms and left actions with anti-homomorphisms depends on writing mappings on the right and composing them left-to-right. When mappings are written on the left and composed right-to-left, right actions correspond to anti-homomorphisms and left actions to anti-homomorphisms.

CAYLEY GRAPHS

Let S be a semigroup with a generating set A. The *right* (respectively, *left*) *Cayley graph* $\Gamma(S, A)$ (respectively, $\Gamma'(S, A)$) of S with respect to A is the directed graph with vertex set S and, for every $x \in S$ and $a \in A$, an edge from x to xa (respectively, ax) labelled by a. By default 'Cayley graph' means 'right Cayley graph'.

EXAMPLES 1.33. a) Let $S = (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\})$. Let $a = (1, 0)$ and $b = (0, 1)$ and let $A = \{a, b\}$. The Cayley graph $\Gamma(S, A)$ is an infinite grid; part of it is shown in Figure 1.6.

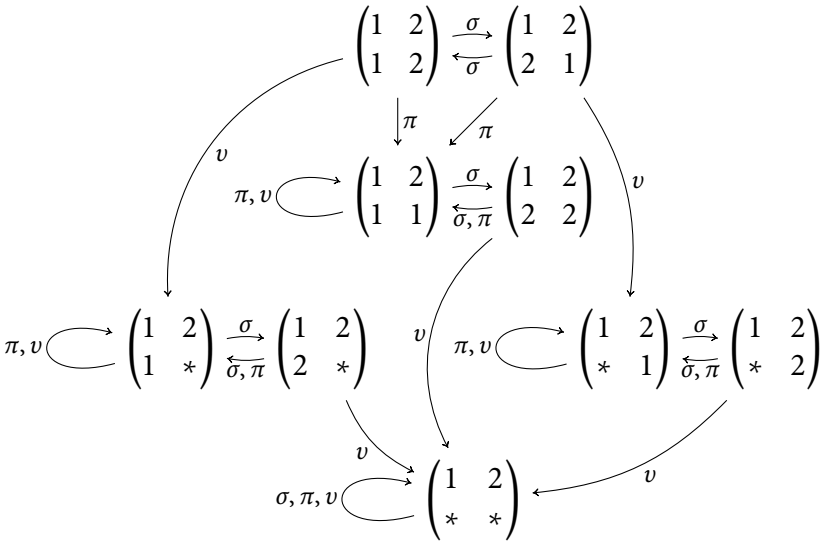


FIGURE 1.7
Cayley graph of $\mathcal{P}_{\{1,2\}}$.

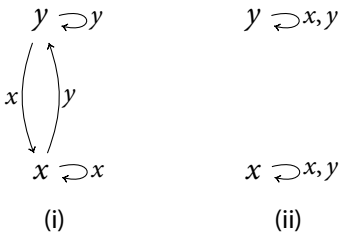


FIGURE 1.8
Right (i) and left (ii) Cayley graphs of a two-element right zero semigroup $\{x, y\}$.

b) Let $X = \{1, 2\}$. Let $A = \{\sigma, \pi, \upsilon\} \subseteq \mathcal{P}_X$, where $\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$, $\pi = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$, and $\upsilon = \begin{pmatrix} 1 & 2 \\ 1 & * \end{pmatrix}$. Then A generates $\mathcal{P}_X$. The Cayley graph $\Gamma(\mathcal{P}_X, A)$ is shown in Figure 1.7.

c) Let $S = A = \{x, y\}$ be a two-element right zero semigroup. The right and left Cayley graphs $\Gamma(S, A)$ and $\Gamma'(S, A)$ are shown in Figure 1.8.

For groups, Cayley graphs have special properties. First, the left and right Cayley graphs are isomorphic. Second, the Cayley graphs are connected, and indeed strongly connected. Third, the Cayley graphs are homogeneous, which essentially means that a neighbourhood of any vertex 'looks like' the corresponding neighbourhood of any other vertex. The graphs in Examples 1.33(c) show that the left and right Cayley graphs of a semigroup need not be isomorphic; the second graph shows that the Cayley graph of a semigroup need not be connected. All the graphs in Examples 1.33 except (c)(ii) show that Cayley graphs of semigroups need not be homogeneous.

EXERCISES

[See pages 139–144 for the solutions.]

✶1.1 Prove that the associativity condition implies that every way of bracketing the product $s_1 s_2 \cdots s_n$ gives the same result. [Hint: Prove by induction on n that every way of bracketing the product gives the same result as $s_1(s_2(\cdots s_{n-1} s_n)\cdots)$.]

1.2 Can a left cancellative semigroup contain an idempotent?

✶1.3 Prove that if a semigroup contains a left zero z and a right zero z', then $z = z'$.

1.4 Prove that if S is a semigroup and $e \in S$ is both a right zero and a right identity, then S is trivial.

1.5 Prove the following:

a) If S is a monoid with identity 1, the semigroup S^0 obtained by adjoining a zero if necessary is also a monoid with identity 1.

b) If S is a semigroup with zero 0, the monoid S^1 obtained by adjoining an identity if necessary also has zero 0.

✶1.6 Let S be a left-cancellative semigroup. Suppose that $e \in S$ is an idempotent. Prove that e is a left identity. Deduce that a cancellative semigroup can contain at most one idempotent, which must be an identity.

✶1.7 Prove that a right zero semigroup is left-cancellative.

✶1.8 Prove that a finite cancellative semigroup is a group.

1.9 Prove that from the definition that id_X is an identity for $\mathcal{B}_X$. Does $\mathcal{B}_X$ contain a zero?

1.10 Does there exist a non-trivial semigroup that does not contain any proper subsemigroups?

✶1.11 Give an [easy] example of an infinite periodic semigroup.

1.12 Does either $\mathcal{T}_X$ or $\mathcal{P}_X$ contain a zero? A left zero? A right zero?

✶1.13 Let $X = \{1, \ldots, n\}$ with $n \geq 3$. Let $\tau = (1\ 2)$ and $\zeta = (1\ 2\ \ldots\ n-1\ n)$. From elementary group theory, we know that $\mathcal{S}_X = \langle \tau, \zeta \rangle$. For any $i, j \in X$, let $|i\ j|$ denote the transformation $\varphi_{i,j} \in \mathcal{T}_X$ such that $i\varphi_{i,j} = j$, $j\varphi_{i,j} = j$, and $x\varphi_{i,j} = x$ for $x \notin \{i, j\}$.

a) Prove the following identities:

$$\begin{aligned}
(1\ i)|1\ 2|(1\ i) &= |i\ 2| && \text{for } i \geq 3;\\
(2\ j)|1\ 2|(2\ j) &= |1\ j| && \text{for } j \geq 3;\\
(1\ i)(2\ j)|1\ 2|(2\ j)(1\ i) &= |i\ j| && \text{for } i, j \geq 3 \text{ and } i \neq j;\\
(i\ j)|i\ j|(i\ j) &= |j\ i| && \text{for } i, j \geq 1 \text{ and } i \neq j.
\end{aligned}$$

b) Let $\varphi \in \mathcal{T}_X$. Suppose $|\operatorname{im} \varphi| = r < n$. Let $i, j \in X$ with $i \neq j$ be such that $i\varphi = j\varphi$. Let $k \in X - \operatorname{im} \varphi$. Show that $\varphi = |i\ j|\varphi'$, where $i\varphi' = k$ and $x\varphi' = x\varphi$ for $x \neq i$.

c) Deduce that $\mathcal{T}_X = \langle \tau, \zeta, |1\ 2| \rangle$.

1.14 Let S be a finite monoid. Prove that $x \in S$ is right-invertible if and only if it is left invertible. [Hint: use the fact that x is periodic.]

✶1.15 Prove than an element of $\mathcal{T}_X$ is

a) left-invertible if and only if it is surjective;

b) right-invertible if and only if it is injective.

1.16 Let $(X, \leq)$ be a totally ordered set. Prove that $(X, \leq)$ is a lattice.

1.17 Let $(S, \wedge, \vee)$ be a lattice.

a) Prove that $(x \wedge y) \vee x = x$ and $(x \vee y) \wedge x = x$ for any $x, y \in S$.

b) Deduce that

$$(\forall x, y, z \in S)\big(x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)\big) \\ \Leftrightarrow (\forall x, y, z \in S)\big(x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)\big).$$

[Equivalently: $\wedge$ distributes over $\vee$ if and only if $\vee$ distributes over $\wedge$.]

✶1.18 Give an example of a map φ from a monoid S to a monoid T that is a homomorphism but not a monoid homomorphism.

✶1.19 Prove Proposition 1.23.

✶1.20 Prove Proposition 1.25.

1.21 Prove that if we restrict the maps ρ_x in Theorem 1.19 to S (instead of S^1), then the map $x \mapsto \rho_x$ may or may not be injective. [Hint: show that it is injective if S is a right zero semigroup but not if it is a left zero semigroup.]

1.22 Let I and J be ideals of S such that $I \subseteq J$. Prove that $S/J \simeq (S/I)/(J/I)$.

1.23 Let I and J be ideals of S. Prove that $I \cap J$ and $I \cup J$ are ideals. [Remember to prove that $I \cap J \neq \varnothing$.] Prove that $(I \cup J)/J \simeq I/(I \cap J)$.

NOTES

Most of the definitions and results in this chapter are 'folklore'. The exposition owes much to the standard accounts in Clifford & Preston, *The Algebraic Theory of Semigroups*, ch. 1, Howie, *Fundamentals of Semigroup Theory*, ch. 1, and to a lesser extent Grillet, *Semigroups*, ch. i. The number of semigroups of order 8 was calculated by Distler, 'Classification and Enumeration of Finite Semigroups'.

Free semigroups & presentations

2

❁ Informally, a free semigroup on a set A is the unique biggest, most 'general' semigroup generated by A, in the sense that all other semigroups generated by A are homomorphic images (and thus factor semigroups) of the free semigroup on A. This chapter studies some of the interesting properties of free semigroups and then explains their role in semigroup presentations, which can be used to define and manipulate semigroups as factor semigroups of free semigroups.

FREE SEMIGROUPS

Free semigroup and monoid

An *alphabet* is an abstract set of symbols called *letters*. Let A be an alphabet. A *word* over A is a finite sequence $(a_1, a_2, \ldots, a_m)$, where each term a_i of the sequence is a letter from A. The *length* of this word is n. There is also a word of length 0, which is the empty sequence $()$. This is called the *empty word*. The set of all words (including the empty word) over A is denoted A^*. The set of all non-empty words (that is, of length 1 or more) over A is denoted A^+. Define multiplication of sequences by concatenation: for all $(a_1, a_2, \ldots, a_m), (b_1, b_2, \ldots, b_n) \in A^*$,

$$(a_1, a_2, \ldots, a_m)(b_1, b_2, \ldots, b_n) = (a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n)$$

It is easy to see that this multiplication is associative and so A^* is a semigroup; furthermore, the empty word $()$ is an identity and so A^* is a monoid. Since the product of two words of non-zero length must itself have non-zero length, A^+ is a subsemigroup of A^*; indeed, A^* is [isomorphic to] $(A^+)^1$. The monoid A^* is called the *free monoid* on A; the semigroup A^+ is called the *free semigroup* on A. Notice that A generates A^+.

Because of associativity, we simply write $a_1a_2\cdots a_n$ for $(a_1, a_2, \ldots, a_n)$ and write ε for the empty word. We denote the length of $u \in A^*$ by $|u|$. Notice that $|u| = 0$ if and only if $u = \varepsilon$.

The Cayley graph $\Gamma(A^*, A)$ is an infinite tree; an example for $A = \{a, b\}$ is shown in Figure 2.1.

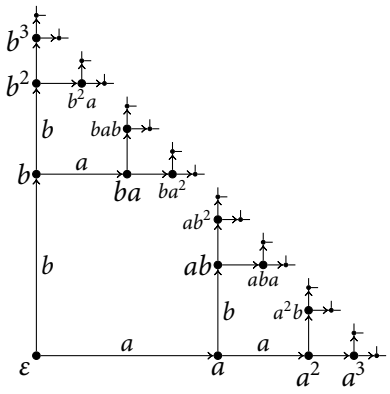


FIGURE 2.1
The Cayley graph of the free monoid on $\{a, b\}$.

PROPERTIES OF FREE SEMIGROUPS

PROPOSITION 2.1. *Let $u, v \in A^*$. Then $|uv| = |u| + |v|$.* 2.1

Equidivisibility

A semigroup S is *equidivisible* if for all $x, y, z, t \in S$, the following holds:

$$xy = zt \Rightarrow \big((\exists p \in S)(x = zp \wedge t = py) \vee (\exists q \in S)(z = xq \wedge y = qt)\big).$$

Every group is equidivisible, because if $xy = zt$, we can take $p = z^{-1}x = ty^{-1}$.

PROPOSITION 2.2. *A^* is equidivisible.*

Proof of 2.2. Suppose $x, y, z, t \in A^*$ are such that $xy = zt$. Let $xy = zt = a_1 \cdots a_n$, where $a_i \in A$. Then, by the definition of multiplication in A^*, we have $x = a_1 \cdots a_k$, $y = a_{k+1} \cdots a_n$, $z = a_1 \cdots a_\ell$, $t = a_{\ell+1} \cdots a_n$, where $0 \leq k, \ell \leq n+1$. (We allow the values 0 and $n+1$ and formally take subwords $a_i \cdots a_j$ where $j < i$ to mean the empty word ε.) If $k \leq \ell$, then the situation is as follows:

$$\overbrace{\underbrace{a_1 \cdots a_k}_{z}\, \underbrace{a_{k+1} \cdots a_\ell}_{y}}^{x}\, \underbrace{a_{\ell+1} \cdots a_n}_{t}$$

and thus we let $q = a_{k+1} \cdots a_\ell$; then $z = xq$ and $y = qt$. On the other hand, if $k \geq \ell$, let $p = a_{\ell+1} \cdots a_k$; then $x = zp$ and $t = py$. 2.2

PROPOSITION 2.3. *Let $A = \{x, y\}$. Let $B = \{b_i : i \in \mathbb{N}\}$. Then A^* contains a submonoid isomorphic to B^*.*

Proof of 2.3. Define a map $\varphi : B \to A^*$ by $b_i\varphi = xy^i x$. Since B^* is free on B, this map φ extends to a unique homomorphism, which we also denote φ, from B^* to A^*.

Suppose, with the aim of obtaining a contradiction, that φ is not injective. Then there exist $u, v \in B^*$ with $u\varphi = v\varphi$.

Suppose u and v begin with the same symbol b; that is, $u = bu'$ and $v = bv'$. Then $(b\varphi)(u'\varphi) = (b\varphi)(v'\varphi)$ and so $u'\varphi = v'\varphi$ by cancellativity in A^*. So we can replace u by u' and v by v' and repeat this process until we have words u and v beginning with different symbols. Therefore assume that u and v begin with symbols b_i and b_j respectively, where $i \neq j$; that is, $u = b_i u'$ and $v = b_j v'$.

Then $xy^i x(u'\varphi) = (b_i\varphi)(u'\varphi) = (b_j\varphi)(v'\varphi) = xy^j x(v'\varphi)$. Assume $i > j$; the other case is similar. By cancellativity in A^*, we have $y^{i-j}x(u'\varphi) = x(v'\varphi)$, which is a contradiction since $i - j > 0$. Therefore φ is injective and so B^* is isomorphic to $\operatorname{im}\varphi$. 2.3

As a consequence of Proposition 2.3, we see that the free monoid on $\{x, y\}$ contains submonoids isomorphic to all free monoids. A similar result holds for free semigroups.

PROPOSITION 2.4. *Let M be a submonoid of A^*. Let $N = M - \{\varepsilon\}$. Then $N - N^2$ is the unique minimal generating set for M.*

Proof of 2.4. Clearly, any generating set for M must contain $N - N^2$. So we must show that $\langle N - N^2\rangle = M$. Clearly $\langle N - N^2\rangle \subseteq M$; we have to prove that $M \subseteq \langle N - N^2\rangle$. We already know that $\varepsilon \in \langle N - N^2\rangle$, so it remains to show that $N \subseteq \langle N - N^2\rangle$. We proceed by induction on the length of elements of N. Let $k = \min\{|u| : u \in N\}$. Then if $|u| = k$ and $u \in N$, then by Proposition 2.1, u cannot be factored as a product of two elements of N. So $u \in N - N^2 \subseteq \langle N - N^2\rangle$. Thus all words of length k in N lie in $\langle N - N^2\rangle$.

So assume that all words of length less than l in N lie in $\langle N - N^2\rangle$. Let $u \in N$ with $|u| = l$. If $u \in N - N^2$, then $u \in \langle N - N^2\rangle$. On other other hand, if $u \notin N - N^2$, then $u \in N^2$ and so $u = u'u''$ for $u', u'' \in N$. By Proposition 2.1, $|u'|, |u''| < |u| = l$. So, by assumption, $u', u'' \in \langle N - N^2\rangle$ and so $u \in \langle N - N^2\rangle$. Hence, by induction, $N \subseteq \langle N - N^2\rangle$. 2.4

Base

The *base* of a submonoid or subsemigroup M of A^* is defined to be $N - N^2$, where $N = M - \{\varepsilon\}$. Thus the base is the unique minimal generating set for M. As an immediate application of Proposition 2.4, we see that A is the base of A^* and A^+.

Words commute $\Leftrightarrow$ powers of a common word

PROPOSITION 2.5. *Let $u, v \in A^+$. Then*

$$uv = vu \Leftrightarrow (\exists w \in A^+)(\exists i, j \in \mathbb{N})(u = w^i \wedge v = w^j).$$

Proof of 2.5. If $u = w^i$ and $v = w^j$, then $uv = w^{i+j} = vu$.

To prove the other direction, we proceed by induction on $|uv|$. If $|uv| \leq 2$, then clearly $uv = vu$ implies $u = v$. So assume the result holds for $|uv| < k$. Suppose $uv = vu$. Interchanging u and v if necessary, assume $|u| \geq |v|$. By Proposition 2.2, there exists $p \in A^*$ such that $u = vp$ and $u = pv$. If $p = \varepsilon$ then $u = v$. Otherwise, $vp = pv$, where $|vp| < |uv|$. So by induction, $v = w^j$ and $p = w^i$ for some $w \in A^*$ and $i, j \in \mathbb{N}$. Thus $u = w^{i+j}$. Hence, by induction, the result holds for all $u, v \in A^*$. 2.5

PROPOSITION 2.6. *A semigroup S is free if and only if every element of S has a unique representative as a product of elements of $S - S^2$.*

Proof of 2.6. Clearly every element of A^+ has a unique representative as a product of elements of $A = A^+ - (A^+)^2$.

So suppose every element of S has a unique representative as a product of elements of $A = S - S^2$. We will show that S satisfies the definition of freedom. Let T be a semigroup and $\varphi : A \to T$ a map. Define a map $\varphi^+ : S \to T$ by letting $s\varphi^+ = (a_1\varphi)(a_2\varphi)\cdots(a_n\varphi)$, where $a_1a_2\cdots a_n$ is the unique representative of s as a product of elements $a_i \in A$. Notice that if $t \in S$ is uniquely represented $b_1\cdots b_m$ where $b_i \in B$, then st has unique representative $a_1\cdots a_nb_1\cdots b_m$. Hence φ^+ is a homomorphism. It is clear that φ^+ is the unique homomorphism extending φ and so S is free on A. 2.6

Free semigroups can contain non-free subsemigroups

EXAMPLE 2.7. Let $A = \{x\}$ and let $S = \langle x^2, x^3\rangle$. Then $S - S^2 = \{x^2, x^3\}$. But $x^5 \in S$ and $x^5 = x^2x^3 = x^3x^2$, so x^5 has two distinct representatives as a product of elements of $\{x^2, x^3\}$. Hence S is not a free semigroup by Proposition 2.6.

Example 2.7 shows that a free semigroup contains subsemigroups that are not themselves free. In contrast, every subgroup of a free group is itself a free group by the famous Nielsen–Schreier theorem.

A *length function* for a semigroup S is a homomorphism $s \mapsto |s|$. A *proper length function* for a monoid M is a length function with the property that $|s| = 0 \Rightarrow s = 1_M$. Notice that the usual notion of length for free monoids is in fact a proper length function.

PROPOSITION 2.8. *A monoid is equidivisible and has a proper length function if and only if it is isomorphic to A^*.*

Proof of 2.8. We have already seen that A^* is equidivisible and has a proper length function.

So suppose that M is an equidivisible monoid with a proper length function. Let $N = M - \{1_M\}$. Notice that N is a subsemigroup since

$$x, y \in N \Rightarrow (|x| \neq 0 \wedge |y| \neq 0) \Rightarrow |xy| = |x| + |y| \neq 0 \Rightarrow xy \neq 1_M.$$

Let $A = N - N^2$. Let $w \in N^2$. Then $w = w'w''$ with $0 < |w'| < |w|$ and $0 < |w''| < |w|$. Continuing this factoring process, we get $w = a_1\cdots a_n$, where $a_i \in A$. So every element of M has a representative as a product of elements of A.

Suppose w has another such representative $b_1\cdots b_m$. We aim to show by induction on $m + n$ that the two representatives are identical. If $m + n = 2$, then $a_1 = w = b_1$. So suppose the result holds for all $m + n < k$. Since $a_1\cdots a_n = b_1\cdots b_m$, equidivisibility shows that there exists $p \in M$ with $a_1 = b_1p$ and $pa_2\cdots a_n = b_2\cdots b_m$. Since $a_1 \in A$, we have $p = 1$ and so $a_1 = b_1$ and $a_2\cdots a_n = b_2\cdots b_m$. Applying the induction hypothesis shows $m = n$ and $a_i = b_i$ for $i \geq 2$.

Thus every element of N has a unique representative as a product of elements of A, and so $N \simeq A^+$ by Proposition 2.6. Hence $M = N \cup \{1\} \simeq A^*$. 2.8

Let x be an element of a monoid M. A *non-trivial left factor* of x is an element y such that $x = yz$ for some $z \in M - \{1\}$.

PROPOSITION 2.9. *A monoid M is free if and only if it has the following four properties:*

a) *the only right- and left-invertible element of M is 1_M;*

b) *M is cancellative;*

c) *M is equidivisible;*

d) *no element of M has infinitely many distinct non-trivial left factors.*

Proof of 2.9. Clearly, A^* has the four properties. So suppose M has the four properties a)–d). We first show that $N = M - \{1_M\}$ is a subsemigroup of M. Let $x, y \in M$ with $xy = 1_M$. Then $(yx)^2 = y(xy)x = yx$. So yx is an idempotent. Since M is cancellative, $yx = 1_M$ by Exercise 1.6. So x and y are left and right inverses of each other and hence $x = y = 1_M$. Therefore $x, y \in N$ implies $xy \in N$ and so N is a subsemigroup.

Now suppose $N = N^2$. Pick $x \in N$. Then there exists some m such that x has exactly m distinct non-trivial left factors. But since $N^{m+2} = N$, we can write $x = y_1 \cdots y_{m+2}$ for $y_i \in N$. The products $y_1 \cdots y_k$ for $k < m + 2$ are all non-trivial left factors of x. Furthermore, they are all distinct, for if $y_1 \cdots y_k = y_1 \cdots y_{k+l}$, then cancellativity shows that $y_{k+1} \cdots y_{k+l} = 1$, which is impossible since N is a subsemigroup. Thus x has at least $m + 1$ distinct non-trivial left factors, which is a contradiction. Hence $N^2 \subsetneq N$. Thus $N - N^2$ is non-empty.

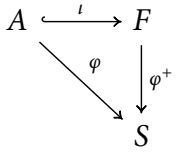
Similarly, suppose $x \in \bigcap\{N^m : m \in \mathbb{N}\}$. Suppose x has exactly m distinct non-trivial left factors. Since $x \in N^{m+2}$, the same contradiction arises. So $\bigcap\{N^m : m \in \mathbb{N}\}$ is empty. Therefore $N \supsetneq N^2 \supsetneq N^3 \supsetneq \ldots$, and hence every element of $x \in N$ lies in $N^m - N^{m+1}$ for some unique m and so x has an expression $n_1 \cdots n_m$ as a product of elements $n_i \in N$. Arguing by equidivisibility as in the proof of Proposition 2.8, we see that each element has a unique expression of this form. So M is free by Proposition 2.6. 2.9

UNIVERSAL PROPERTY

Freedom

Let F be a semigroup and let A be an alphabet A. Let $\iota : A \hookrightarrow F$ be an embedding of A into F. Then the semigroup F is *free*

on A if, for any semigroup S and map $\varphi : A \to S$, there is a unique homomorphism $\varphi^+ : F \to S$ extending φ. That is, $\iota\varphi^+ = \varphi$ or, equivalently, the following diagram commutes:



Uniqueness of free semigroups

PROPOSITION 2.10. *Let A be an alphabet and let F be a semigroup. Then F is free on A if and only if $F \simeq A^+$.*

Proof of 2.10. Suppose $F \simeq A^+$. To show F is free on A, it is sufficient to show that A^+ is free on A. Let $\iota : A \to A^+$ be the embedding map. So let S be a semigroup and $\varphi : A \to S$ be a map. Define $\varphi^+ : A^+ \to S$ by

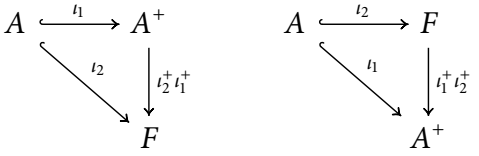
$$(a_1a_2\cdots a_n)\varphi^+ = (a_1\varphi)(a_2\varphi)\cdots(a_n\varphi).$$

It is easy to see that φ^+ is a homomorphism and that $\iota\varphi^+ = \varphi$. We now have to prove that φ^+ is unique. So let $\psi : A^+ \to S$ be an arbitrary homomorphism with $\iota\psi = \varphi$. For any $a_1a_2\cdots a_n \in A^+$,

$$\begin{aligned}(a_1a_2\cdots a_n)\psi &= (a_1\psi)(a_2\psi)\cdots(a_n\psi) && \text{[since } \psi \text{ is a homomorphism]}\\ &= (a_1\varphi^+)(a_2\varphi^+)\cdots(a_n\varphi^+) && \text{[since } \iota\psi = \varphi = \iota\varphi^+\text{]}\\ &= (a_1a_2\cdots a_n)\varphi^+. && \text{[since } \varphi^+ \text{ is a homomorphism]}\end{aligned}$$

and so $\psi = \varphi^+$. Hence φ^+ is the unique homomorphism from A^+ to S with $\iota\varphi^+ = \psi$, and so A^+ is free on A.

Now let F be a semigroup that is free on A. Let $\iota_1 : A \hookrightarrow A^+$ and $\iota_2 : A \hookrightarrow F$ be the embedding maps. Put $\varphi = \iota_2$ and $S = F$ in the definition of F being free on A to see that there is a homomorphism $\iota_2^+ : A^+ \to F$ with $\iota_1\iota_2^+ = \iota_2$. Similarly, since F is free on A, there is a homomorphism $\iota_1^+ : F \to A^+$ with $\iota_2\iota_1^+ = \iota_1$. Therefore $\iota_1 = \iota_1\iota_2^+\iota_1^+$ and $\iota_2 = \iota_2\iota_1^+\iota_2^+$. That is, the following diagrams commute:



Therefore, by the uniqueness requirement in the definition of freedom, $\iota_2^+\iota_1^+ = \mathrm{id}_{A^+}$ and $\iota_1^+\iota_2^+ = \mathrm{id}_F$. Hence ι_1^+ and ι_2^+ are mutually inverse isomorphisms, and so $F \simeq A^+$. 2.10

Every semigroup is a quotient of a free semigroup

The reason why free semigroups are interesting is that every semigroup is isomorphic to a quotient of a free semigroup. To see this, let

$\varphi : A \to S$ be such that $\operatorname{im}\varphi$ generates S. (We could, for instance, choose A to be a set of the same cardinality as S and φ be a bijection.) Then, φ extends to a homomorphism $\varphi^+ : A^+ \to S$. Since $\operatorname{im}\varphi$ generates S, we have $\operatorname{im}\varphi^+ = S$. By Theorem 1.21, $A^+/\ker\varphi^+ \simeq \operatorname{im}\varphi^+ = S$. That is, S is isomorphic to the quotient $A^+/\ker\varphi^+$.

This is slightly interesting, but its real importance is when we turn it around. Instead of starting with a semigroup and knowing that it is a quotient of a free semigroup, we can specify a free semigroup A^+ and a congruence σ and so *define* the corresponding quotient semigroup A^+/σ. This is the idea of a semigroup presentation, which we will study in detail shortly. First of all, we have to examine how a relation on a semigroup can generate a congruence.

PRESENTATIONS

The idea of a semigroup presentation is to specify and reason about a semigroup as a quotient of a free semigroup: that is, as a quotient A^+/σ for some congruence σ on the free semigroup A^+. By Proposition 2.10, in order to specify the free semigroup, it is sufficient to specify the alphabet A. In order to specify the congruence σ, it is sufficient to specify some binary relation ρ that generates σ.

Presentations

A *semigroup presentation* is a pair $\langle A \mid \rho\rangle$, where A is an alphabet and ρ is a binary relation on A^+. This presentation *defines*, or *presents*, [any semigroup isomorphic to] $A^+/\rho^\#$. A presentation is *finite* if both A and ρ are finite. The semigroup is *finitely presented* if can be defined by a finite presentation.

When working with a presentation $\langle A \mid \rho\rangle$, we often call the elements of ρ (which are pairs of words in A^+) *defining relations*. We think of semigroup presented by $\langle A \mid \rho\rangle$ as the largest semigroup generated by A and satisfying the defining relations in ρ.

Representatives

When working with semigroup S given by a presentation $\langle A \mid \rho\rangle$, we view words in A^+ as *representing* elements of S. In particular, the alphabet A represents a generating set for S. In general, an element of S will have more than one representative in A^+. If $u, v \in A^+$ represent the same element of S (that is, if $(u, v) \in \rho^\#$), we say that u and v are *equal in* S and write $u =_S v$.

An elementary ρ-transition is a pair $(u, v) \in (\rho^S)^C$. Thus, by Proposition 1.24, (u, v) is an elementary ρ-transition if and only if v can be obtained from u by substiuting a subword y for a subword x of u, where $(x, y) \in \rho$ or $(y, x) \in \rho$.

PROPOSITION 2.11. *Let S be presented by $\langle A \mid \rho\rangle$. Then $u =_S v$ if and only if there is a sequence $u_0, \ldots, u_n$ with $u_0 = u$, $u_n = v$, and each (u_i, u_{i+1})*

being an elementary ρ-transition.

Proof of 2.11. First of all, notice that

$$\begin{aligned}
& u =_S v \\
\Leftrightarrow\ & (u,v) \in \rho^{\#} \\
\Leftrightarrow\ & (u,v) \in (\rho^{\mathsf{C}})^{\mathsf{E}} && \text{[by Proposition 1.26]} \\
\Leftrightarrow\ & (u,v) \in (((\rho^{\mathsf{C}})^{\mathsf{R}})^{\mathsf{S}})^{\mathsf{T}} && \text{[by Proposition 1.23]} \\
\Leftrightarrow\ & (u,v) \in (\rho^{\mathsf{C}} \cup (\rho^{\mathsf{C}})^{-1} \cup \mathrm{id}_{A^+})^{\mathsf{T}} && \text{[by Proposition 1.23]} \\
\Leftrightarrow\ & (u,v) \in \textstyle\bigcup_{n=1}^{\infty} (\rho^{\mathsf{C}} \cup (\rho^{\mathsf{C}})^{-1} \cup \mathrm{id}_{A^+})^n && \text{[by Proposition 1.23]} \\
\Leftrightarrow\ & (\exists n \in \mathbb{N})\big((u,v) \in (\rho^{\mathsf{C}} \cup (\rho^{\mathsf{C}})^{-1} \cup \mathrm{id}_{A^+})^n\big) \\
\Leftrightarrow\ & (\exists n \in \mathbb{N})(\exists u_0, u_1, \ldots, u_n \in S)\big[(u = u_0) \wedge (u_n = v) \\
& \qquad \wedge (\forall i)\big((u_i, u_{i+1}) \in \rho^{\mathsf{C}} \cup (\rho^{\mathsf{C}})^{-1} \cup \mathrm{id}_{A^+}\big)\big].
\end{aligned}$$

Hence $u =_S v$ if and only if there is there is a sequence $u_0, \ldots, u_n$ with $u_0 = u$, $u_n = v$, and each (u_i, u_{i+1}) being an elementary ρ-transition or with $u_i = u_{i+1}$. Since we can shorten the sequence by removing any steps with $u_i = u_{i+1}$, we get that $u =_S v$ if and only if there is there is such a sequence of elementary ρ-transitions. 2.11

When there is a sequence of elementary ρ-transitions $u = u_0, \ldots, u_n = v$, then we say (u, v) is a *consequence* of ρ, or (u, v) can be *deduced* from ρ.

Monoid presentations

We could repeat the discussion of freedom and presentations, but for monoids instead of semigroups. A monoid F is free on A if and only if $F \simeq A^*$ (the analogy of Proposition 2.10). Every monoid is a quotient of a free monoid. In a monoid presentation $\langle A \mid \rho \rangle$ defining a monoid M, the generators A are monoid generators and the defining relations in ρ can be of the form (u, ε) or (ε, u). Furthermore $u =_M v$ if and only if there is a sequence of elementary transitions from u to v (the analogy of Proposition 2.11).

Finite presentability is independent of the generating set

PROPOSITION 2.12. *Suppose S is finitely presented and that $\langle A \mid \rho \rangle$ be a presentation for S. Then there exists $B \subseteq A$ and $\sigma \subseteq \rho$ such that $\langle B \mid \sigma \rangle$ is a finite presentation for S.*

Proof of 2.12. [We omit this proof. The basic idea is that every relation in ρ is a consequence of a finite subset of σ' of σ, and so we need only finitely many relations in σ to obtain every relation in ρ and so define the semigroup. The technical difficulty is that we have to switch between the generating sets A and B.] 2.12

EXAMPLES 2.13. a) The presentation $\langle A \mid \rangle$ (where there are no defining relations) defines the free semigroup A^+. To see this, note that there are no non-trivial consequences of defining relations, and so

all words over A represent different elements of the semigroup by Proposition 2.11. . Alternatively, notice that $\varnothing^{\#} = \mathrm{id}_A$, and $A^+/\mathrm{id}_A \simeq A^+$.

b) The presentation $\langle a \mid (a^2, a)\rangle$ defines the trivial semigroup, since $a^n = a$ is a consequence of the defining relation.

c) The presentation $\langle A \mid \{(ab, a) : a, b \in A\}\rangle$ defines a left zero semigroup on the set A.

d) Let M be the monoid presented by $\langle a, b \mid (ab, ba)\rangle$. Notice that every element of M is equal to a unique word of the form $a^\alpha b^\beta$. So $M \simeq (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\})$.

e) The monoid presentation $\langle b, c \mid (bc, \varepsilon)\rangle$ defines the *bicyclic monoid*. Every element of the bicyclic monoid is represented by a word $c^\gamma b^\beta$, where $\beta, \gamma \in \mathbb{N} \cup \{0\}$, because if we have a word $w \in \{b, c\}^*$ that contains a subword bc, we can repeatedly use (bc, ε) to remove this subword. This process must end with a word that does not contain bc; that is, a word of the form $c^\gamma b^\beta$. Actually, each element is represented by a unique word of this form; we omit the proof of this.

Bicyclic monoid

We now give two more complicated examples. Example 2.14 shows that a semigroup can be finitely generated but not finitely presented; since the example semigroup in question is a subsemigroup of a free semigroup, this strengthens Example 2.7. Example 2.15 then shows that cancellativity is not a sufficient condition for group-embeddability.

EXAMPLE 2.14. Let $X = \{xyz, yz, yt, xy, zy, zyt\} \subseteq \{x, y, z, t\}^+$. Let S be the subsemigroup of $\{x, y, z, t\}^+$ generated by X. Let $A = \{a, b, c, d, e, f\}$ and let $\varphi : A^+ \to S$ be given by

Finitely generated but not finitely presented

$$\begin{aligned} a\varphi &= xyz, & b\varphi &= yz, & c\varphi &= yt, \\ d\varphi &= xy, & e\varphi &= zy, & f\varphi &= zyt. \end{aligned}$$

Now for any $\alpha \in \mathbb{N} \cup \{0\}$,

$$(ab^\alpha c)\varphi = x(yz)^{\alpha+1}yt = (de^\alpha f)\varphi.$$

Hence, if $\langle A \mid \rho\rangle$ is a presentation for S, then $\rho^{\#}$ must contain $(ab^\alpha c, de^\alpha f)$ for all $\alpha \in \mathbb{N} \cup \{0\}$. Thus there must be an elementary sequence of ρ-transitions from $ab^\alpha c$ to $de^\alpha f$. But ab^α is the unique word over A representing $(ab^\alpha)\varphi = x(yz)^{\alpha+1}$, and $b^\alpha c$ is the unique word over A representing $(b^\alpha c)\varphi = (zy)^{\alpha+1}t$. Hence in an elementary sequence of ρ-transitions starting from $ab^\alpha c$, the first step must involve a defining relation from ρ one side of which is $ab^\alpha c$. Thus, ρ must contain infinitely many defining relations. Hence S is finitely generated but not finitely presented.

EXAMPLE 2.15. Let $A = \{a, b, c, d, e, f, g, h\}$ and let $\rho = \{(ae, bf), (cf, de), (dg, ch)\}$. Let S be the semigroup presented by $\langle A \mid \rho\rangle$.

Cancellative but not group-embeddable

Proving that S is cancellative is involves many cases, so we prove one case; the others are similar. Suppose that $cu =_S cv$; we aim to prove that $u =_S v$. There is a sequence of elementary ρ-transitions from

$$cu = w_0, \ldots, w_n = cv. \tag{2.1}$$

Without loss of generality, assume that n is minimal among all such sequences. Suppose, with the aim of obtaining a contradiction, that at some step in this sequence the initial symbol c is altered. This must involve applying one of the defining relation (cf, de) or (dg, ch). Assume the former; the latter case is similar. So for some $i \in \{0, \ldots, n\}$, we have $w_i = cfw'$ and $w_{i+1} = dew'$. Now, no defining relation has one side starting with a symbol a symbol e, so the symbol e must remain in the terms of the sequence until a the relation (cf, de) is applied again with $w_j = dew''$ and $w_{j+1} = cfw''$. (We know that this relation must be applied because the symbol d must be removed because $w_n = cv$.) Because the symbols de are not involved in any of the intermediate steps, there is no need to apply (cf, de) twice. That is, there is a shorter sequence of elementary transitions from cu to cv. This contradicts the minimality of n. Hence the initial symbol c is never altered. Thus we can delete the initial symbol c from each step in (2.1) to obtain a sequence of elementary ρ-transitions from u to v. Hence $u =_S v$.

Reasoning in this way for every symbol in A shows that S is left-cancellative; symmetrical arguments show that S is right cancellative. Thus S is cancellative.

Suppose S is group embeddable. Then there is a monomorphism $\varphi : S \to G$, where G is a group. Then

$$\begin{aligned}
(ag)\varphi &= (a\varphi)(g\varphi) \\
&= (a\varphi)(e\varphi)(e\varphi)^{-1}(g\varphi) \\
&= (b\varphi)(f\varphi)(e\varphi)^{-1}(g\varphi) && [\text{since } ae =_S bf] \\
&= (b\varphi)(c\varphi)^{-1}(c\varphi)(f\varphi)(e\varphi)^{-1}(g\varphi) \\
&= (b\varphi)(c\varphi)^{-1}(d\varphi)(e\varphi)(e\varphi)(g\varphi) && [\text{since } cf =_S de] \\
&= (b\varphi)(c\varphi)^{-1}(d\varphi)(g\varphi) \\
&= (b\varphi)(c\varphi)^{-1}(c\varphi)(h\varphi) && [\text{since } dg =_S ch] \\
&= (b\varphi)(h\varphi) \\
&= (bh)\varphi.
\end{aligned}$$

But $ag \neq_S bh$, since there is no sequence of ρ-transitions from ag to bh since ag does not contain a subword that forms one side of a defining relation in ρ. This a contradiction and so no such monomorphism φ exists. Hence S is not group-embeddable.

So S is an example of a cancellative semigroup that is not group-embeddable.

EXERCISES

[See pages 144–146 for the solutions.]

2.1 Let $u, v, w \in A^+$ be such that $uv = vw$.

a) Using induction on $|v|$, prove that there exist $p, q \in A^*$ and $k \in \mathbb{N} \cup \{0\}$ such that $u = pq$, $v = (pq)^k p$, and $w = qp$.

b) Prove part a) in a different way by letting k be maximal (possibly $k = 0$) such that $v = u^k p$ for some $p \in A^*$.

✶2.2 Let S be an equidivisible semigroup. Two elements u and v of S are *conjugate*, denoted $u \sim v$, if there exist $x, y \in S^1$ such that $u = xy$ and $v = yx$.

a) Prove that if S is a group then $u \sim v$ if and only if u and v are conjugate in the group-theoretic sense.

b) Prove that $\sim$ is an equivalence relation.

c) Prove that in A^*, we have $u \sim v$ if and only if there exists $w \in A^*$ such that $uw = wv$.

✶2.3 Let $u, v \in A^+$. Show that the subsemigroup $\langle u, v \rangle$ is free if and only if $uv \neq vu$.

2.4 Let S be a semigroup and let X be a generating set for S, with $|X| \geq 2$. Suppose that for all $x_i, y_i \in X$ and $n \in \mathbb{N}$, we have $x_1 \cdots x_n = y_1 \cdots y_n \Rightarrow (\forall i \in \{1, \ldots, n\})(x_i = y_i)$. Prove that S is free with basis X.

✶2.5 Let $n \in \mathbb{N}$. Let $A = \{a_1, \ldots, a_n\}$ and $\rho = \{(a_i^2, a_i), (a_i a_j, a_j a_i) : i, j \in \{1, \ldots, n\}\}$. Let M be the monoid presented by $\langle A \mid \rho \rangle$.

a) Prove that every element of M is represented by a word $a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n}$, where each $k_i \leq 1$. [Since this is a monoid presentation, we can have the empty word, where all $k_i = 0$.]

b) Prove that each element of M is represented by a *unique* word of this form.

c) Let $X = \{x_1, x_2, \ldots, x_n\}$. Show that M is [isomorphic to] $\wp X$ under the operation of union. [Hint: $\wp X$ is generated by elements $\{x_1\}, \{x_2\}, \ldots, \{x_n\}$.]

2.6 Let B be the bicyclic monoid $\langle b, c \mid (bc, \varepsilon) \rangle$.

a) Prove that $c^\gamma b^\beta$ is idempotent if and only if $\beta = \gamma$.

b) Prove that $c^\gamma b^\beta$ is right-invertible if and only if $\gamma = 0$. [Dual reasoning will show that $c^\gamma b^\beta$ is left-invertible if and only if $\beta = 0$.]

✶2.7 Let B be the bicyclic monoid $\langle b, c \mid (bc, \varepsilon) \rangle$. Draw a part of the Cayley graph $\Gamma(B, \{b, c\})$ including all elements $c^\gamma b^\beta$ with $\gamma, \beta \leq 3$.

NOTES

Example 2.15 is based on Malcev, 'On the immersion of an algebraic ring into a field'. Exercise 2.4 is adapted from Gallagher, 'On the Finite Generation and Presentability of Diagonal Acts, Finitary Power Semigroups and Schützenberger Products', Proof of Proposition 3.1.12.

Structure of semigroups

3

The aim of this chapter is to understand better the structure of semigroups. We want to divide the semigroup into sections in such a way that we can understand the semigroup in terms of those parts and their interaction. One goal is to understand the semigroup in terms of groups; then we assume that our work is done and we hand on the problem to a group theorist.

GREEN'S RELATIONS

Green's relations

The most fundamental tools in understanding a semigroup are its Green's relations. These relate elements depending on the ideals they generate, and, as we shall see, give a lot of information about the structure of a semigroup and how its elements interact. There are five Green's relations: $\mathcal{H}$, $\mathcal{L}$, $\mathcal{R}$, $\mathcal{D}$, and $\mathcal{J}$. We start by defining $\mathcal{L}$, $\mathcal{R}$, and $\mathcal{J}$:

$\mathcal{L}$, $\mathcal{R}$, and $\mathcal{J}$

$$\begin{aligned} x \mathcal{L} y &\Leftrightarrow S^1 x = S^1 y, \\ x \mathcal{R} y &\Leftrightarrow x S^1 = y S^1, \\ x \mathcal{J} y &\Leftrightarrow S^1 x S^1 = S^1 y S^1. \end{aligned} \tag{3.1}$$

It is easy to see that $\mathcal{L}$, $\mathcal{R}$, and $\mathcal{J}$ are all equivalence relations. Alternative, equivalent, definitions for $\mathcal{L}$, $\mathcal{R}$, and $\mathcal{J}$ are the following:

$$\begin{aligned} x \mathcal{L} y &\Leftrightarrow (\exists p, q \in S^1)\big((px = y) \wedge (qy = x)\big), \\ x \mathcal{R} y &\Leftrightarrow (\exists p, q \in S^1)\big((xp = y) \wedge (yq = x)\big), \\ x \mathcal{J} y &\Leftrightarrow (\exists p, q, r, s \in S^1)\big((pxr = y) \wedge (qys = x)\big). \end{aligned} \tag{3.2}$$

PROPOSITION 3.1. $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$.

$\mathcal{L}$ and $\mathcal{R}$ commute

Proof of 3.1. Let $(x, y) \in \mathcal{L} \circ \mathcal{R}$. Then there exists $z \in S$ such that $x \mathcal{L} z$ and $z \mathcal{R} y$. Hence there exist $p, q, r, s \in S^1$ such that $px = z$, $qz = x$, $zr = y$, and $ys = z$.

Let $z' = qzr$. Then $xr = qzr = z'$ and $z's = qzrs = qys = qz = x$, so $x \mathcal{R} z'$, and $qy = qzr = z'$ and $pz' = pqzr = pxr = zr = y$, so $z' \mathcal{L} y$. Hence $(x, y) \in \mathcal{R} \circ \mathcal{L}$.

Thus $\mathcal{L} \circ \mathcal{R} \subseteq \mathcal{R} \circ \mathcal{L}$. Similarly $\mathcal{R} \circ \mathcal{L} \subseteq \mathcal{L} \circ \mathcal{R}$ and so $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$. 3.1

$\mathcal{H}$ and $\mathcal{D}$

As a consequence of Propositions 1.28 and 3.1, we see that $\mathcal{L} \vee \mathcal{R} = \mathcal{L} \circ \mathcal{R}$. The meet and join of $\mathcal{L}$ and $\mathcal{R}$ play an important role, so they are also counted as Green's relations and have particular notations:

$$\mathcal{H} = \mathcal{L} \wedge \mathcal{R},$$
$$\mathcal{D} = \mathcal{L} \vee \mathcal{R}.$$

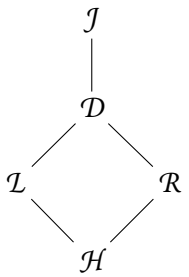


FIGURE 3.1
Hasse diagram of Green's relations in a general semigroup

From either (3.1) or (3.2), one sees that $\mathcal{L} \subseteq \mathcal{J}$ and $\mathcal{R} \subseteq \mathcal{J}$. So $\mathcal{J}$ is an upper bound for $\{\mathcal{L}, \mathcal{R}\}$ and so $\mathcal{D} = \mathcal{L} \vee \mathcal{R} \subseteq \mathcal{J}$. Furthermore, it is immediate that $\mathcal{H} \subseteq \mathcal{L}$ and $\mathcal{H} \subseteq \mathcal{R}$. In fact, all of these inclusions are in general strict by Exercises 3.5 and 3.6; see Figure 3.1. However, in some special classes of semigroups we do have equality of some of the relations.

For instance, let G be a group. Then in G, all of Green's relations are equal to the universal relation $G \times G$. That is, all elements of G are $\mathcal{H}$-, $\mathcal{L}$-, $\mathcal{R}$-, $\mathcal{D}$, and $\mathcal{J}$-related.

$\mathcal{D} = \mathcal{J}$ for periodic semigroups

PROPOSITION 3.2. *In a periodic semigroup, the Green's relations $\mathcal{D}$ and $\mathcal{J}$ coincide.*

Proof of 3.2. Suppose S is periodic. We already know $\mathcal{D} \subseteq \mathcal{J}$, so we have to prove the opposite inclusion.

Let $x \mathcal{J} y$. Then there exist $p, q, r, s \in S^1$ such that $pxr = y$ and $qys = x$. So $x = qpxrs$ and so $x = (qp)^n x (rs)^n$ for all $n \in \mathbb{N}$, and similarly $y = (pq)^n y (sr)^n$ for all $n \in \mathbb{N}$. Since S is periodic, there exist $k, \ell \in \mathbb{N}$ such that $(qp)^k$ and $(sr)^\ell$ are idempotent. Let $z = px$. Then

$$\begin{aligned} x &= (qp)^k x (rs)^k = (qp)^{2k} x (rs)^k \\ &= (qp)^k \big((qp)^k x (rs)^k \big) = (qp)^k x = \big((qp)^{k-1} q \big) z. \end{aligned}$$

Hence $x \mathcal{L} z$. Similarly, $zr = pxr = y$ and

$$\begin{aligned} z = px &= p(qp)^{\ell+1} x (rs)^{\ell+1} = (pq)^{\ell+1} pxr (sr)^\ell s = (pq)^{\ell+1} pxr (sr)^{2\ell} s \\ &= (pq)^{\ell+1} y (sr)^{2\ell} s = (pq)^{\ell+1} y (sr)^{\ell+1} (sr)^{\ell-1} s = y \big((sr)^{\ell-1} s \big). \end{aligned}$$

Hence $z \mathcal{R} y$.

Therefore $x \mathcal{D} y$. Thus $\mathcal{J} \subseteq \mathcal{D}$ and so $\mathcal{D} = \mathcal{J}$. 3.2

PROPOSITION 3.3. a) *The relation $\mathcal{L}$ is a right congruence.*
b) *The relation $\mathcal{R}$ is a left congruence.* 3.3

Proof of 3.3. See Exercise 3.1 3.3

H_a, L_a, R_a, D_a, and J_a

For $x \in S$, denote by H_a, L_a, R_a, D_a, and J_a, respectively, the $\mathcal{H}$-, class of $\mathcal{L}$-, $\mathcal{R}$-, $\mathcal{D}$, and $\mathcal{J}$-classes of x. By the containment between Green's relations described above, $H_a \subseteq L_a$, $H_a \subseteq R_a$, $L_a \subseteq D_a$, $R_a \subseteq D_a$, and $D_a \subseteq J_a$.

Partial order of $S/\mathcal{L}$, $S/\mathcal{R}$, and $S/\mathcal{J}$

There are natural partial orders on the collection of $\mathcal{L}$-classes $S/\mathcal{L}$,

the collection of $\mathcal{R}$-classes S/gR, and the collection of $\mathcal{J}$-classes $S/\mathcal{J}$ induced by inclusion order of ideals:

$$\begin{aligned} L_x \leq L_y &\Leftrightarrow S^1x \subseteq S^1y \\ R_x \leq R_y &\Leftrightarrow xS^1 \subseteq yS^1 \\ J_x \leq J_y &\Leftrightarrow S^1xS^1 \subseteq S^1yS^1 \end{aligned} \tag{3.3}$$

It follows immediate from (3.3) that for all $x \in S$ and $p, q \in S^1$,

$$L_{px} \leq L_x, \qquad R_{xq} \leq R_x, \qquad J_{pxq} \leq J_x.$$

SIMPLE AND 0-SIMPLE SEMIGROUPS

A semigroup is *simple* if it contains no proper ideals. A semigroup S with a zero is 0-*simple* if it is not null and its only proper ideal is $\{0\}$.

The notion of a simple semigroup is not a generalization of a 'simple group', in the sense of a group that contains no proper non-trivial normal subgroups. Groups never contains proper ideals, so groups are always simple semigroups.

An ideal of a semigroup is *minimal* if it does not properly contain any ideal. An ideal of a semigroup with zero is 0-*minimal* if the only proper ideal it contains is $\{0\}$.

PROPOSITION 3.4. *A semigroup contains at most one minimal ideal.*

Uniqueness of minimal ideals

Proof of 3.4. Suppose I and J are minimal ideals of a semigroup S. Then IJ is an ideal of S and $IJ \subseteq IS \subseteq I$ and $IJ \subseteq SJ \subseteq J$. Hence, by the minimality of I and J, we have $I = IJ$ and $J = IJ$ and hence $I = J$. 3.4

A semigroup S might not contain a minimal ideal. But Proposition 3.4 shows that a semigroup S contains a minimal ideal, it is unique. Such a unique minimal ideal is called a *kernel* and is denoted $K(S)$. Notice that if S is a semigroup with zero, $K(S) = \{0\}$.

LEMMA 3.5. *A semigroup S is 0-simple if and only if $SxS = S$ for all $x \in S - \{0\}$.*

No non-zero proper principal ideals in a 0-simple semigroup

Proof of 3.5. Suppose S is 0-simple. First note that S^2 is an ideal of S. Hence $S^2 = S$ since S is 0-simple. Therefore $S^3 = S^2S = SS = S$.

For any $x \in S$, the ideal SxS is either $\{0\}$ or S since S is 0-simple. Let $T = \{x \in S : SxS = \{0\}\}$. It is easy to prove that T is an ideal of S. Since S is 0-simple, it follows that $T = S$ or $T = \{0\}$. Suppose that $T = S$. Then $SxS = \{0\}$ for all $x \in S$, which implies $S^3 = \{0\}$, which is a contradiction. Hence $T = \{0\}$, and so $SxS = S$ for all $x \in S - \{0\}$.

For the converse, suppose $SxS = S$ for all $x \in S - \{0\}$. Let I be some ideal of S. Suppose $I \neq \{0\}$. Then there exists some $y \in I - \{0\}$, and $SyS = S$. Hence $S = SyS \subseteq I \subseteq S$ and so $I = S$. So for any ideal I of S, either $I = \{0\}$ or $I = S$, and so S is 0-simple. 3.5

0-minimal ideals are 0-simple or null

PROPOSITION 3.6. a) *A 0-minimal ideal of a semigroup with zero is either null or 0-simple.*

b) *A minimal ideal of a semigroup is simple.*

Proof of 3.6. a) Let I be a 0-minimal ideal of a semigroup S that has a zero. Suppose I is not null. Then $I^2 \neq \{0\}$. Hence, since $I^2 \subseteq I$ is an ideal of S and I is 0-minimal, we have $I^2 = I$ and so $I^3 = I$. Let $x \in I - \{0\}$. Then S^1xS^1 is a ideal of S contained in I. Since $x \in S^1xS^1$, we have $S^1xS^1 \neq \{0\}$; hence $S^1xS^1 = I$ since I is 0-minimal. Hence $I = I^3 = IS^1xS^1I \subseteq IxI \subseteq I$. Hence $IxI = I$ for all $x \in I - \{0\}$ and so I is 0-simple by Lemma 3.5.

b) See Exercise 3.4. 3.6

For any $x \in S$, let $J(x) = S^1xS^1$. Recall that the $\mathcal{J}$-class of x, denoted J_x, is the set of all elements of the semigroup that generate (as a principal ideal) $J(x)$. Let $I(x) = J(x) - J_x$. Notice that $I(x) = \{y \in S : J_y < J_x\}$.

LEMMA 3.7. *Either $I(x)$ is empty or an ideal of S.*

Proof of 3.7. Suppose $I(x) \neq \varnothing$. Let $y \in I(x)$ and $z \in S$. Then $yz \in J(x)$ since $J(x)$ is an ideal. But $J(yz) \subseteq J(y) \subsetneq J(x)$ (since $J(y) = J(x)$ would imply $y \in J_x$). Hence $yz \in I(x)$. Similarly $zy \in I(x)$. Hence $I(x)$ is an ideal. 3.7

Principal factors

The factor semigroups $J(x)/I(x)$ (where x is such that $I(x) \neq 0$) and the kernel $K(S)$ are called the *principal factors* of S.

PROPOSITION 3.8. *Let S be a semigroup. If the kernel $K(S)$ exists, it is simple. All principal factors $J(x)/I(x)$ are either null or 0-simple.*

Proof of 3.8. By Proposition 3.6(b), if $K(S)$ exists, it is simple.

The principal factor $J(x)/I(x)$ is a 0-minimal ideal of $S/I(x)$ and so is 0-simple by Proposition 3.6(a). 3.8

A *principal series* of a semigroup S is a finite chain of ideals

$$K(S) = S_1 \subsetneq S_2 \subsetneq \ldots \subsetneq S_n = S \tag{3.4}$$

that is maximal in the sense that there is no ideal I such that $S_i \subsetneq I \subsetneq S_{i+1}$.

Not all semigroups admit principal series. Indeed, even if a semigroup has a kernel, it may not admit a principal series: for example, let S by the semigroup $(\mathbb{N}, +)$. Then S^0 has a minimal ideal $\{0\}$ but no principal series.

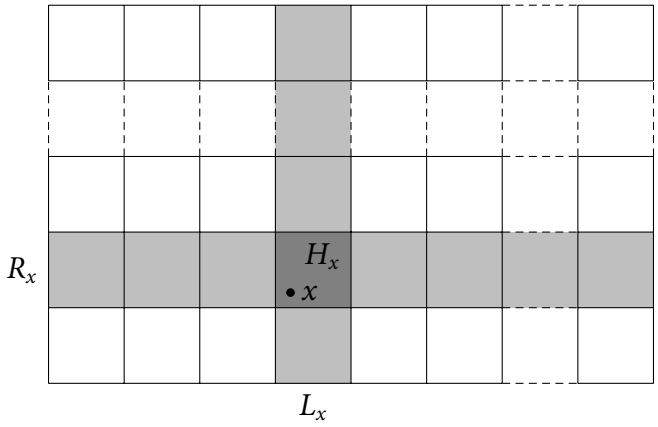


FIGURE 3.2
An egg-box diagram for the $\mathcal{D}$-class D_x.

THEOREM 3.9. *Let S be a semigroup admitting a principal series (3.4). Then the factors S_{i+1}/S_i are, in some order, isomorphic to the principal factors of S.*

'Jordan–Hölder Theorem' for semigroups

Proof of 3.9. [Not especially difficult, but technical and omitted.] 3.9

$\mathcal{D}$-CLASS STRUCTURE

Since $\mathcal{L} \subseteq \mathcal{D}$ and $\mathcal{R} \subseteq \mathcal{D}$, every $\mathcal{D}$-class must be both a union of $\mathcal{L}$-classes and a union of $\mathcal{R}$-classes. On other hand, suppose an $\mathcal{L}$-class L_x and a $\mathcal{R}$-class R_y intersect. Then there is some element $z \in L_x \cap R_y$. So $x \mathcal{L} z \mathcal{R} y$ and so $x \mathcal{D} y$. Hence L_x and R_y are both contained within the same $\mathcal{D}$-class. Therefore an $\mathcal{L}$-class and an $\mathcal{R}$-class intersect if and only if they are contained within the same $\mathcal{D}$-class.

Thus we can visualize a $\mathcal{D}$-class in the following useful way: Imagine the element of this $\mathcal{D}$-class arranged in a rectangular pattern. This pattern is divided into a grid of cells. Each column of cells is an $\mathcal{L}$-class; each row is an $\mathcal{R}$-class, and every cell is the $\mathcal{H}$-class that is the intersection of the $\mathcal{L}$- and $\mathcal{R}$-class forming the column and row containing that cell. This visualization is called an *egg-box diagram*. (See Figure 3.2.)

LEMMA 3.10. a) *Let $x, y \in S$ be such that $x \mathcal{L} y$ and let $p, q \in S^1$ be such that $px = y$ and $qy = x$. Then the maps $\lambda_p|_{R_x}$ and $\lambda_q|_{R_y}$ (where $t\lambda_z = zt$) are mutually inverse bijections between R_x and R_y, and both of these maps preserve $\mathcal{L}$-classes. (See Figure 3.3.)*

Green's lemma

b) *Let $x, y \in S$ be such that $x \mathcal{R} y$ and let $p, q \in S^1$ be such that $xp = y$ and $yq = x$. Then the maps $\rho_p|_{L_x}$ and $\rho_q|_{L_y}$ (where $t\rho_z = tz$) are mutually inverse bijections between L_x and L_y, and both of these maps preserve $\mathcal{R}$-classes.*

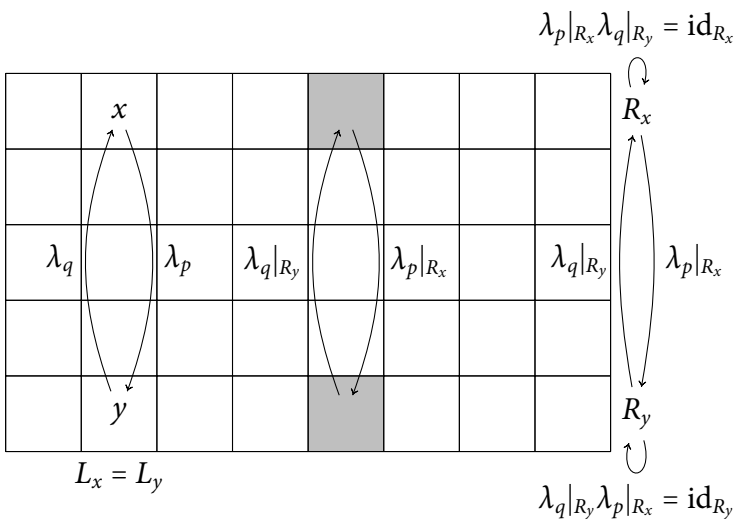


FIGURE 3.3
Green's lemma.

Proof of 3.10. We prove only part a); the other part is proved by a dual argument.

First, notice that

$$\begin{aligned} z \in R_x &\Rightarrow z \mathcal{R} x \\ &\Rightarrow z\lambda_p|_{R_x} = pz \mathcal{R} px = y \qquad \text{[since } \mathcal{R} \text{ is a left congruence]} \\ &\Rightarrow z\lambda_p|_{R_x} \in R_y. \end{aligned}$$

So, $\lambda_p|_{R_x}$ maps R_x to R_y and similarly $\lambda_q|_{R_y}$ maps R_y to R_x.

Second, suppose $z \in R_x$. Then there exists $r \in S^1$ such that $xr = z$. Then $z\lambda_p|_{R_x}\lambda_q|_{R_y} = (xr)\lambda_p|_{R_x}\lambda_q|_{R_y} = qpxr = pyr = xr = z$. Hence $\lambda_p|_{R_x}\lambda_q|_{R_y} = \mathrm{id}_{R_x}$. Similarly $\lambda_q|_{R_y}\lambda_p|_{R_x} = \mathrm{id}_{R_y}$. So $\lambda_p|_{R_x}$ and $\lambda_q|_{R_y}$ are mutually inverse bijections.

Finally, if $z = t\lambda_p|_{R_x}$, then $z = pt$ and $t = z(\lambda_p|_{R_x})^{-1} = z\lambda_q|_{R_y} = qz$ and so $z \mathcal{L} t$. Hence $\lambda_p|_{R_x}$ preserves $\mathcal{L}$-classes. 3.10

$\mathcal{H}$-classes in the same $\mathcal{D}$-class have the same cardinality

PROPOSITION 3.11. *Let $x, y \in S$ be such that $x \mathcal{D} y$. Then $|H_x| = |H_y|$.*

Proof of 3.11. Suppose $x \mathcal{D} y$. Then there exists z such that $x \mathcal{L} z$ and $z \mathcal{R} y$. Let $p, q, r, s \in S^1$ be such that $px = z$, $qz = x$, $zr = y$, and $ys = z$. By Lemma 3.10, $\lambda_p|_{H_x} : H_x \to H_z$ is a bijection, and $\rho_r|_{H_z} : H_z \to H_y$ is a bijection. So $\lambda_p|_{H_x}\rho_r|_{H_z} : H_x \to H_y$ is a bijection, and hence $|H_x| = |H_y|$. 3.11

PROPOSITION 3.12. *Let H be an $\mathcal{H}$-class of S. Then either:*

a) *$H^2 \cap H = \varnothing$, or*

b) *the following equivalent statements hold:*

   i) *$H^2 \cap H \neq \varnothing$;*

   ii) *H contains an idempotent;*

   iii) *$H^2 = H$;*

iv) *H is a subsemigroup of S;*

v) *H is a subgroup of S.*

Proof of 3.12. If $H^2 \cap H = \varnothing$ there is nothing further to prove. So suppose that $H^2 \cap H \neq \varnothing$. Then there exist $x, y \in H$ such that $xy \in H$. Then $x \mathcal{H} xy$. In particular, $x \mathcal{R} xy$. So by Lemma 3.10(b) $\rho_y|_H$ is a bijection from H to itself. Similarly, $y \mathcal{L} xy$ and by Lemma 3.10(a) $\lambda_x|_H$ is a bijection from H to itself.

Now let $z \in H$. Then $xz = z\lambda_x|_H$ and $zy = z\rho_y|_H$ are both in H. Again by Lemma 3.10, $\rho_z|_H$ and $\lambda_z|_H$ are bijections from H to itself. Since $z \in H$ was arbitrary, it follows that $zH = Hz = H$ for all $z \in H$. Therefore H is a subgroup by Lemma 1.8.

We have shown that condition i) implies condition v). Condition v) clearly implies conditions ii), iii), and iv), and each of these implies condition i). So all five conditions are equivalent. 3.12

A *maximal subgroup* is a subgroup that does not lie inside any larger subgroup.

Maximal subgroup = $\mathcal{H}$-class containing an idempotent

PROPOSITION 3.13. *The maximal subgroups of S are precisely the $\mathcal{H}$-classes of S that contain idempotents.*

Proof of 3.13. Since every element of a subgroup is $\mathcal{H}$-related, it follows that any subgroup is contained within a single $\mathcal{H}$-class. So a maximal subgroup G is contained within a single $\mathcal{H}$-class H. But H therefore contains an idempotent 1_G and so is itself a subgroup. Hence $H = G$. 3.13

COROLLARY 3.14. *An $\mathcal{H}$-class contains at most one idempotent.* 3.14

Idempotents are left/right identities for their $\mathcal{R}/\mathcal{L}$-classes

PROPOSITION 3.15. *Let $e \in S$ be idempotent. Then e is a left identity for R_e and a right identity for L_e.*

Proof of 3.15. Suppose $x \in R_e$. Then there exist $p \in S^1$ such that $ep = x$. Hence $ex = eep = ep = x$. Hence e is a left identity for R_e. Similarly e is a right identity for L_e. 3.15

Products located by idempotents

PROPOSITION 3.16. *Let $x, y \in S$ with $x \mathcal{D} y$. Then $xy \in L_y \cap R_x$ if and only if $L_x \cap R_y$ contains an idempotent.*

Proof of 3.16. Suppose that $xy \in L_y \cap R_x$. In particular $xy \mathcal{R} x$. Hence there exists $q \in S^1$ such that $xyq = x$. By Lemma 3.10, $\rho_y|_{L_x} : L_x \to L_y$ and $\rho_q|_{L_y} : L_y \to L_x$ are mutually $\mathcal{R}$-class preserving bijections. Hence $(yq)^2 = yqyq = y\rho_q|_{L_y}\rho_y|_{L_x}\rho_q|_{L_y} = y\rho_q|_{L_x} = yq$. Hence yq is idempotent. Furthermore, $yq = y\rho_q|_{L_y} \in L_x \cap R_y$.

Now suppose that $L_x \cap R_y$ contains an idempotent e. Then $ey = y$ by Proposition 3.15. Since $e \mathcal{R} y$, the map $\rho_y|_{L_e} : L_e \to L_y$ is an $\mathcal{R}$-class preserving bijection by Lemma 3.10. Hence $xy \in R_x \cap L_y$. 3.16

INVERSES AND $\mathcal{D}$-CLASSES

Proposition 3.16 shows a close relationship between the product of two elements of a $\mathcal{D}$-class and idempotents in that $\mathcal{D}$-class. It is thus not surprising that idempotents and inverses in a $\mathcal{D}$-class are also connected.

Either every element of D_x is regular or none are

PROPOSITION 3.17. *If $x \in S$ is regular, then every element of D_x is regular.*

Proof of 3.17. Suppose x is regular. Then there exists $y \in S$ such that $xyx = x$. Suppose $z \mathcal{L} x$. Then there exist $p, q \in S^1$ such that $pz = x$ and $qx = z$. Hence $z = qx = qxyx = zypz$ and so z is regular. So every element of L_x is regular. A dual argument shows that if $t \in S$ is regular, every element of R_t is regular. Combining these, we see that if x is regular, every element of D_x is regular. 3.17

Regular/irregular $\mathcal{D}$-classes

A $\mathcal{D}$-class is *regular* if all its elements are regular, and otherwise is *irregular*.

PROPOSITION 3.18. *In a regular $\mathcal{D}$-class, every $\mathcal{L}$-class and every $\mathcal{R}$-class contains an idempotent.*

Proof of 3.18. Let $x \in S$ be such that D_x is regular. In particular, x is regular and so $xyx = x$ for some $x \in S$. Now, $yx \mathcal{L} x$ and $(yx)^2 = yxyx = yx$. So yx is an idempotent in L_x. Similarly xy is an idemponent in R_x. Thus every $\mathcal{L}$-class and $\mathcal{R}$-class contains an idempotent. 3.18

Recall that $V(x)$ is the set of inverses of x.

PROPOSITION 3.19. *If x lies in a regular $\mathcal{D}$-class and $x' \in V(x)$, then:*

a) *$x \mathcal{R} xx' \mathcal{L} x'$ and $x \mathcal{L} x'x \mathcal{R} x'$ and so $x \mathcal{D} x'$;*

b) *if $z \in D_x$ is such that $L_z \cap R_x$ contains an idempotent e and $R_z \cap L_x$ contains an idempotent f, then H_z contains some $t \in V(x)$ with $xt = e$ and $tx = f$;*

c) *an H-class contains at most one member of $V(x)$.*

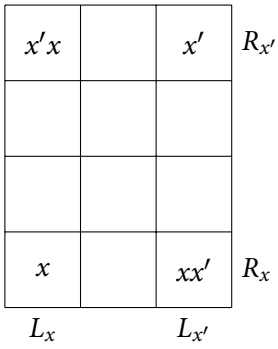


FIGURE 3.4
x and $x' \in V(x)$ in a regular $\mathcal{D}$-class

Proof of 3.19. a) Let $x' \in V(x)$. Then $xx'x = x$ and $x'xx' = x'$. Then $x \mathcal{R} xx' \mathcal{L} x'$ and so $x \mathcal{D} x'$. (See Figure 3.4.)

b) Since $x \mathcal{R} e$, there exists $p, q \in S^1$ with $xp = e$ and $eq = x$. Let $t = fpe$. Then

$$\begin{aligned} xtx &= xfpex && \text{[by choice of } t\text{]} \\ &= xpx && \text{[by Proposition 3.15]} \\ &= ex && \text{[since } xp = e\text{]} \\ &= x && \text{[by Proposition 3.15]} \end{aligned}$$

and

$$\begin{aligned} txt &= fpexfpe && \text{[by choice of } t\text{]} \\ &= fpxpe && \text{[by Proposition 3.15]} \\ &= fpe^2 && \text{[since } xp = e\text{]} \\ &= fpe && \text{[since } e \text{ is idempotent]} \\ &= t. && \text{[by choice of } t\text{]} \end{aligned}$$

Hence $t \in V(x)$. Furthermore, $xt = xfpe = xpe = e^2 = e$. Finally, note that $\rho_p|_{L_x} : L_x \to L_e$ and $\rho_q|_{L_e} : L_e \to L_x$ are mutually inverse $\mathcal{R}$-class preserving bijections by Lemma 3.10. Hence

$$\begin{aligned} tx &= fpex && \text{[by choice of } t\text{]} \\ &= (f\rho_p|_{L_x})ex && \text{[by definition of } \rho_p|_{L_x}\text{]} \\ &= (f\rho_p|_{L_x})e^2q && \text{[since } eq = x\text{]} \\ &= (f\rho_p|_{L_x})eq && \text{[since } e \text{ is idempotent]} \\ &= (f\rho_p|_{L_x})q && \text{[by Proposition 3.15, since } f\rho_p|_{L_x} \in L_e\text{]} \\ &= f\rho_p|_{L_x}\rho_q|_{L_e} && \text{[by definition of } \rho_q|_{L_e}\text{]} \\ &= f. && \text{[since } \rho_p|_{L_x} \text{ and } \rho_q|_{L_e} \text{ are mutually inverse]} \end{aligned}$$

In particular, $t \in L_e \cap R_f = H_z$. (See Figure 3.5.)

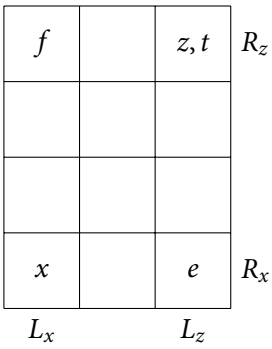


FIGURE 3.5
Inverse t corresponding to idempotents e and f in a regular $\mathcal{D}$-class

c) Suppose $x', x'' \in V(x)$ and $x' \mathcal{H} x''$; we aim to show $x' = x''$. Then xx' and xx'' are idempotents lying inside $L_{x'} \cap R_x = L_{x''} \cap R_x$. Hence $xx' = xx''$ by Corollary 3.14. Similarly $x'x = x''x$. Therefore $x' = x'xx' = x'xx'' = x''xx'' = x''$. 3.19

COROLLARY 3.20. *Let $e, f \in S$ be idempotents. Then $e \mathcal{D} f$ if and only if there exist $x \in S$ and $x' \in V(x)$ such that $xx' = e$ and $x'x = f$.*

Proof of 3.20. Suppose $e \mathcal{D} f$. Then $D_e = D_f$ is a regular $\mathcal{D}$-class. Let $x \in R_e \cap L_f$. Then by Proposition 3.19(b), there is an inverse $x' \in V(x)$ such that $xx' = e$ and $x'x = f$.

Suppose now that $x \in S$ and $x' \in V(x)$ are such that $xx' = e$ and $x'x = f$. Then $x \mathcal{R} e$ and so $D_x = D_e$ is regular. Then by Proposition 3.19(a), $e \mathcal{R} x \mathcal{L} f$ and so $e \mathcal{D} f$. 3.20

SCHÜTZENBERGER GROUPS

$\mathrm{Stab}(H)$ and σ_H

Let S be a semigroup and let H be an $\mathcal{H}$-class of S. Let $\mathrm{Stab}(H) = \{x \in S : Hx = H\}$. Define a relation $\sigma_H = \{(x, y) \in S \times S : (\forall h \in H)(hx = hy)\}$. It is easy to see that $\mathrm{Stab}(H)$ is a subsemigroup of S and σ_H is a congruence on $\mathrm{Stab}(H)$. Let $\Gamma(H)$ denote the factor semigroup $\mathrm{Stab}(H)/\sigma_H$.

PROPOSITION 3.21. *$\Gamma(H)$ is a group.*

Proof of 3.21. Let $h \in H$ and let $x \in \mathrm{Stab}(H)$. Then $hx \in H$. In particular, $hx \mathcal{R} h$ and so there exists $q \in S^1$ such that $hxq = h$. Since $hx(qxq) = hxq = h$, we can replace q by qxq to guarantee that $q \in S$. Hence by Lemma 3.10, $\rho_x|_H$ and $\rho_q|_H$ are mutually inverse bijections. In particular, $Hq = H\rho_q = H$, and so $q \in \mathrm{Stab}(H)$.

Let $[z]_{\sigma_H} \in \mathrm{Stab}(H)/\sigma_H$. Then for any $h \in H$,

$$hzxq = hz\rho_x|_H\rho_q|_H = hz$$

Hence $z \; \sigma_H \; zxq$, and so $[z]_{\sigma_H} = [z]_{\sigma_H}[xq]_{\sigma_H}$. Similarly $[z]_{\sigma_H} = [xq]_{\sigma_H}[z]_{\sigma_H}$. Thus $[xq]_{\sigma_H}$ is an identity for $\mathrm{Stab}(H)/\sigma_H$. Furthermore, $[x]_{\sigma_H}^{-1} = [q]_{\sigma_H}$ and so (since $x \in \mathrm{Stab}(H)$ was arbitrary), every element of $\mathrm{Stab}(H)/\sigma_H$ has an inverse. Hence $\Gamma(H)$ is a group. 3.21

Schützenberger group

The group $\Gamma(H)$ is called the *Schützenberger group* of H. This notions provides a way to find a group corresponding to *any* $\mathcal{H}$-class, not just those for which $H^2 \cap H \neq \varnothing$ (see Proposition 3.12).

$\Gamma(H)$ acts regularly on H

PROPOSITION 3.22. *Let H be an $\mathcal{H}$-class of a semigroup. The Schützenberger group $\Gamma(H)$ acts regularly on H via $h \cdot [x]_{\sigma_H} = hx$.*

Proof of 3.22. First of all, note that the action $h \cdot [x]_{\sigma_H} = hx$ is well-defined.

Let $h, h' \in H$. Since in particular $h \mathcal{R} h'$, there exists $p, q \in S^1$ such that $hp = h'$ and $h'q = h$. Let $[e]_{\sigma_H}$ be the identity of $\Gamma(H)$. Then $h \cdot [pe]_{\sigma_H} = hp = h'$. So $\Gamma(H)$ acts transitively on H.

To show that $\Gamma(H)$ acts freely on H, we have to show that $[pe]_{\sigma_H}$ is the unique element that acts on h to give h'. So suppose $h \cdot [y]_{\sigma_H} = h'$. Let $g \in H$. Since $g \mathcal{L} h$, there exists $q \in S^1$ such that $qh = g$. Then

$$gy = qhy = qh \cdot [y]_{\sigma_H} = qh' = qh \cdot [pe]_{\sigma_H} = qhpe = gpe.$$

Since this holds for all $g \in H$, it follows that $(y, pe) \in \sigma_H$ and so $[y]_{\sigma_H} = [pe]_{\sigma_H}$. Hence $\Gamma(H)$ acts freely on H.

Thus the action of $\Gamma(H)$ on H is regular. 3.22

An $\mathcal{H}$-class and its Schützenberger group have the same size

COROLLARY 3.23. *Let H be an $\mathcal{H}$-class of a semigroup. Then $|\Gamma(H_x)| = |H_x|$.*

Proof of 3.23. Since $\Gamma(H_x)$ acts regularly on H_x, there is a one-to-one correspondence between elements of H_x and elements of $\Gamma(H_x)$ and so $|H_x| = |\Gamma(H_x)|$. 3.23

Strictly speaking, $\Gamma(H)$ is the *right* Schützenberger group of H, because the definitions of $\mathrm{Stab}(H)$ and σ_H are in terms of right multiplication of elements of H. This seems arbitrary, because we could make

similar definitions using left multiplication:

$$\begin{aligned}\mathrm{Stab}'(H) &= \{x \in S : xH = H\},\\ \sigma'(H) &= \{(x,y) \in S \times S : (\forall h \in H)(xh = xh)\},\\ \Gamma'(H) &= \mathrm{Stab}'(H)/\sigma'(H).\end{aligned}$$

Clearly, reasoning dual to the proofs of Propositions 3.21 and 3.22 shows that $\Gamma'(H)$ is a group that acts on H *on the left* via $[x]_{\sigma'(H)} \cdot h = xh$.

PROPOSITION 3.24. $\Gamma(H) \simeq \Gamma'(H)$.

Right and left Schützenberger groups are isomorphic

Proof of 3.24. Fix some $h \in H$. Define a map $\varphi : \Gamma(H) \to \Gamma'(H)$ as follows. For any $s \in \Gamma(H)$, since $\Gamma'(H)$ acts regularly on H, there is a unique $s' \in \Gamma'(H)$ such that $h \cdot s = s' \cdot h$. Define $s\varphi$ to be this s'. Similarly, since $\Gamma(H)$ acts regularly on H, we can define a map $\psi : \Gamma'(H) \to \Gamma(H)$ by letting $t\psi$ be the unique element of $\Gamma(H)$ such that $t \cdot h = h \cdot (t\psi)$. Clearly φ and ψ are mutually inverse and so are bijections.

Let $[x]_{\sigma_H} \in \Gamma(H)$ and $[y]_{\sigma'_H} \in \Gamma'(H)$. Let $g \in H$. Then

$$[y]_{\sigma'_H} \cdot (g \cdot [x]_{\sigma_H}) = [y]_{\sigma'_H} \cdot (gx) = ygx = (yg) \cdot [x]_{\sigma_H} = ([y]_{\sigma'_H} \cdot g) \cdot [x]_{\sigma_H}. \quad (3.5)$$

Let $s, t \in \Gamma(H)$. Then

$$\begin{aligned}&(s\varphi)(t\varphi) \cdot h\\ &= (s\varphi) \cdot (h \cdot t) && \text{[by definition of } \varphi\text{]}\\ &= \big((s\varphi) \cdot h\big) \cdot t && \text{[by (3.5)]}\\ &= (h \cdot s) \cdot t && \text{[by definition of } \varphi\text{]}\\ &= h \cdot (st) && \text{[by the axioms of an action]}\\ &= \big((st)\varphi\big) \cdot h. && \text{[by definition of } \varphi\text{]}\end{aligned}$$

Since $\Gamma'(H)$ acts regularly on H, it follows that $(s\varphi)(t\varphi) = (st)\varphi$. Therefore φ is an isomorphism. 3.24

PROPOSITION 3.25. *If $x \mathcal{D} y$, then $\Gamma(H_x) \simeq \Gamma(H_y)$.*

Schützenberger groups are the same throughout a $\mathcal{D}$-class

Proof of 3.25. Suppose first that $x \mathcal{L} y$. Then there exist $p, q \in S^1$ such that $px = y$ and $qy = x$. So by Lemma 3.10, $\lambda_p|_H : H_x \to H_y$ and $\lambda_q|_H : H_y \to H_x$ are mutually inverse bijections. Hence $pH_x = H_y$ and $qH_y = H_x$. Suppose that $z \in \mathrm{Stab}(H_x)$. Then $H_y z = pH_x z \subseteq pH_x = H_y$ and so $z \in \mathrm{Stab}(H_y)$. Thus $\mathrm{Stab}(H_x) \subseteq \mathrm{Stab}(H_y)$ and similarly $\mathrm{Stab}(H_y) \subseteq \mathrm{Stab}(H_x)$. So $\mathrm{Stab}(H_x) = \mathrm{Stab}(H_y)$.

Now let $z, t \in \mathrm{Stab}(H_x)$. Suppose $(z,t) \in \sigma(H_x)$. Then $xz = xt$ and so $yz = pxz = pxt = yt$ and so $(z,t) \in \sigma(H_y)$. Hence $\sigma(H_x) \subseteq \sigma(H_y)$. Similarly $\sigma(H_y) \subseteq \sigma(H_x)$ and so $\sigma(H_x) = \sigma(H_y)$. Therefore $\Gamma(H_x) \simeq \Gamma(H_y)$.

On the other hand, if $x \mathcal{R} y$, dual reasoning shows that $\Gamma'(H_x) \simeq \Gamma'(H_y)$. The result follows from Proposition 3.24. 3.25

Notice that from Corollary 3.23 and Proposition 3.25 we immediately recover Proposition 3.11.

PROPOSITION 3.26. *If H is a group, then $\Gamma(H) \simeq H$.*

Proof of 3.26. Suppose H is a group. Then $H \subseteq \mathrm{Stab}(H)$. The natural map $\sigma_H^\natural|_H : H \to \mathrm{Stab}(H)/\sigma_H$, which maps h to $[h]_{\sigma_H}$, is a homomorphism.

Let $s \in \Gamma(H)$. Let $h = 1_H \cdot s$. Then since $1_H \cdot [h]_{\sigma_H} = h$ and $\Gamma(H)$ acts freely on H, we have $s = [h]_{\sigma_H}$. Hence $\sigma_H^\natural|_H$ is surjective.

Let $g, h \in H$ with $g\sigma_H^\natural|_H = h\sigma_H^\natural|_H$. Then $[h]_{\sigma_H} = [g]_{\sigma_H}$ and so $g = 1_H \cdot [g]_{\sigma_H} = 1_H \cdot [h]_{\sigma_H} = h$. Hence $\sigma_H^\natural|_H$ is injective.

So $\sigma_H^\natural|_H$ is an isomorphism from H to $\Gamma(H)$. Hence $\Gamma(H) \simeq H$. 3.26

Propositions 3.25 and 3.26 have the following consequence:

COROLLARY 3.27. *If H and H' are group $\mathcal{H}$-classes within the same $\mathcal{D}$-class, then $H \simeq H'$.* 3.27

EXERCISES

[See pages 147–152 for the solutions.]

✶3.1 Prove that $\mathcal{L}$ is a right congruence and $\mathcal{R}$ is a left congruence.

✶3.2 Prove that any two elements of a subgroup of a semigroup are $\mathcal{H}$-related.

3.3 Prove that in a free monoid A^*, we have $\mathcal{H} = \mathcal{L} = \mathcal{R} = \mathcal{D} = \mathcal{J} = \mathrm{id}_{A^*}$.

3.4 Prove part b) of Proposition 3.6.

✶3.5 Let $B = L \times R$ be a rectangular band. Prove that the $\mathcal{R}$-classes of B are the sets $\{\ell\} \times R$ where $\ell \in L$, that the $\mathcal{L}$-classes of B are the sets $L \times \{r\}$ where $r \in R$, that B consists of a single $\mathcal{D}$-class, and that $\mathcal{H}$ is the equality relation.

3.6 Prove that if S is a cancellative semigroup and does not contain an identity element, then $\mathcal{H} = \mathcal{L} = \mathcal{R} = \mathcal{D} = \mathrm{id}_S$.

✶3.7 Let

$$S = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \in \mathbb{R}, a, b > 0 \right\} \subseteq M_2(\mathbb{R}).$$

Prove that S is a subsemigroup of $M_2(\mathbb{R})$. Prove that S is cancellative and has no identity, so that $\mathcal{H} = \mathcal{L} = \mathcal{R} = \mathcal{D} = \mathrm{id}_S$ by Exercise 3.6. Prove that S is simple, so that $\mathcal{J} = S \times S$.

✶3.8 Let X be a set and let $\sigma, \tau \in \mathcal{T}_X$. Prove the following:

a) $\sigma \mathcal{L} \tau \Leftrightarrow \mathrm{im}\,\sigma = \mathrm{im}\,\tau$;

b) $\sigma \mathcal{R} \tau \Leftrightarrow \ker \sigma = \ker \tau$;

c) $\sigma \mathcal{D} \tau \Leftrightarrow \sigma \mathcal{J} \tau \Leftrightarrow |\operatorname{im} \sigma| = |\operatorname{im} \tau|$.

3.9 Recall that the bicyclic monoid B is presented by $\langle b, c \mid (bc, \varepsilon) \rangle$ and that every element of B has a unique representative of the form $c^\gamma b^\beta$. Prove that the $\mathcal{R}$-classes of B are sets $\{c^\gamma b^\beta : \beta \in \mathbb{N} \cup \{0\}\}$ (where $\gamma \in \mathbb{N} \cup \{0\}$ is fixed) and $\mathcal{L}$-classes of B are sets $\{c^\gamma b^\beta : \gamma \in \mathbb{N} \cup \{0\}\}$ (where $\beta \in \mathbb{N} \cup \{0\}$ is fixed). Deduce that B has a single $\mathcal{D}$-class.

3.10 Let R be an $\mathcal{R}$-class and L an $\mathcal{L}$-class of a semigroup S and suppose $L \cap R$ contains an idempotent. Let D be the $\mathcal{D}$-class containing L and R. Prove that $LR = D$.

✶3.11 A semigroup is *right simple* if it contains no proper right ideals. A semigroup is a *right group* if is right simple and left cancellative.

a) Let S be a right group. Prove that S contains an idempotent.

b) Let S be a right simple semigroup that contains an idempotent. Let E be the set of idempotents of S. Prove that E is a right zero subsemigroup of S. Prove that every element of E is a left identity in S. Prove that Se is a subgroup of S for every $e \in E$. Let $G = Sf$ for some fixed $f \in E$. Define a map $\varphi : G \times E \to S$ by $(x, e) = xe$. Prove φ is an isomorphism.

c) Let G be a group and Z a right zero semigroup. Prove that $G \times Z$ is a right group. Deduce that every right group is isomorphic to the direct product of a group and a right zero semigroup.

3.12 Let S be a left-cancellative semigroup. Let G be a subgroup of S. Suppose G is also a left ideal of S. Prove that S is a right group.

3.13 Let S be a simple semigroup that contains an idempotent e, contains at least one minimal left ideal and does not contain a zero.

a) Prove that S is the union of its minimal left ideals.

b) Prove that Se is a left group.

c) Prove that eSe is a group.

d) Prove that eS is a minimal right ideal of S.

NOTES

The definition of the relations $\mathcal{L}$, $\mathcal{R}$, and $\mathcal{J}$, the results on principal series, Green's lemma, and the basic structure of $\mathcal{D}$-classes are all from Green, 'On the structure of semigroups'. The interaction of inverses and $\mathcal{D}$-classes is due to Miller & Clifford, 'Regular $\mathcal{D}$-classes in semigroups'. Schützenberger groups first appear, in a rather different form, in Schützenberger, '$\overline{\mathcal{D}}$ représentation des demi-groupes'.

Regular semigroups

4

Properties of group inverses

❁ If S is a group, every element x has a unique inverse x^{-1}. The map $x \mapsto x^{-1}$ is a unary operation on S and satisfies certain properties. For instance, by definition $xx^{-1} = x^{-1}x = 1_S$ for all $x \in S$. But $^{-1}$ also satisfies other properties: for all $x, y \in S$,

$$\begin{aligned} (x^{-1})^{-1} &= x, & (xy)^{-1} &= y^{-1}x^{-1}, & x^{-1}x &= xx^{-1}, \\ xx^{-1}x &= x, & xx^{-1}yy^{-1} &= yy^{-1}xx^{-1} & xx^{-1} &= yy^{-1}. \end{aligned}$$

If we require that the operation $^{-1}$ satisfy only some of these relations, we no longer have a group. Instead, we obtain different types of semigroup depending on which conditions are required.

Regular semigroups

Let S be equipped with an operation $^{-1}$. If S satisfies the condition that for all $x \in S$,

$$xx^{-1}x = x, \tag{4.1}$$

then S is clearly regular. If S satisfies the conditions that for all $x \in S$,

$$xx^{-1}x = x, \qquad (x^{-1})^{-1} = x, \tag{4.2}$$

then again S is regular and for any $y \in S$, we have $yy^{-1}y = y$ and $y^{-1}yy^{-1} = y^{-1}(y^{-1})^{-1}y^{-1} = y^{-1}$ and so y^{-1} is an inverse of y.

Completely regular semigroups

If S satisfies the three conditions that for all $x \in S$,

$$(x^{-1})^{-1} = x, \qquad x^{-1}x = xx^{-1}, \qquad xx^{-1}x = x, \tag{4.3}$$

it is a *completely regular semigroup*. We will look at completely regular semigroups later in this chapter.

Inverse semigroups

If S satisfies the four conditions that for all $x, y \in S$,

$$\begin{aligned} (x^{-1})^{-1} &= x, & (xy)^{-1} &= y^{-1}x^{-1}, \\ xx^{-1}x &= x, & xx^{-1}yy^{-1} &= yy^{-1}xx^{-1}, \end{aligned} \tag{4.4}$$

it is an *inverse semigroup*.

Clifford semigroups

Finally, if S satisfies the four conditions that for all $x \in S$,

$$\begin{aligned} (x^{-1})^{-1} &= x, & x^{-1}x &= xx^{-1}, \\ xx^{-1}x &= x, & xx^{-1}yy^{-1} &= yy^{-1}xx^{-1}, \end{aligned} \tag{4.5}$$

it is a *Clifford semigroup*. We will look at inverse semigroups and Clifford semigroups in Chapter 5.

COMPLETELY 0-SIMPLE SEMIGROUPS

The aim of this section is to introduce the concept of a completely 0-simple semigroup and to present a classification result for such semigroups, the Rees–Suschkewitsch Theorem. We study completely 0-simple semigroups for two reasons. First, we saw that the principal factors of a semigroup are either 0-simple or null, and completely 0-simple semigroup are an important subclass of 0-simple semigroups. Furthermore, studying completely 0-simple semgroups will lead naturally to studying completely simple semigroups, and we will see that a simple semigroup is completely simple if and only if it is completely regular.

Primitive idempotents

Recall that the set of idempotents $E(S)$ of a semigroup S admits a natural partial order given by $e \preceq f \Leftrightarrow ef = fe = e$. (See Proposition 1.16.) In a semigroup with a zero, 0 is the unique minimal idempotent; in such a semigroup, an idempotent is *primitive* if it is minimal within the set of non-zero idempotents of the semigroup. A semigroup is *completely 0-simple* if it is 0-simple and contains a primitive idempotent.

Completely 0-simple

Finite 0-simple ⇒ completely 0-simple

PROPOSITION 4.1. *A finite 0-simple semigroup is completely 0-simple.*

Proof of 4.1. Let S be a finite 0-simple semigroup. Now, if there are non-zero idempotents in S, there must be a primitive idempotent in S, since otherwise there would be infinite descending chains of idempotents, and this is impossible since S is finite. So we must simply rule out the possibility that 0 is the only idempotent.

So suppose, with the aim of obtaining a contradiction, that the only idempotent in S is 0. Let $x \in S - \{0\}$. Then by Lemma 3.5 there exist $p, q \in S$ with $pxq = x$. Hence $p^n x q^n = x$ for all $n \in \mathbb{N}$. Since S is finite and thus periodic, some p^m is idempotent. Thus $p^m = 0$ since 0 is the only idempotent in S. Therefore $x = p^m x q^m = 0 x q^m = 0$, which contradicts the choice of x. So it is impossible for 0 to be the only idempotent of S. This completes the proof. 4.1

Rees matrix semigroups

We are now going to show how to construct examples of completely 0-simple semigroups. Let G be a group, let I and Λ be abstract index sets, and let P be a regular $\Lambda \times I$ matrix with entries from G^0. (Recall that a matrix is *regular* if every row and every column contains at least one non-zero entry. By a '$\Lambda \times I$ matrix' we mean simply a matrix whose rows are indexed by Λ and whose columns are indexed by I.) Let $p_{\lambda i}$ be the (λ, i)-th entry of P. Let S be the set $I \times G^0 \times \Lambda$. Define a multiplication on S by

$$(i, x, \lambda)(j, y, \mu) = (i, x p_{\lambda j} y, \mu).$$

This multiplication is associative since

$$\begin{aligned}(i,x,\lambda)\big((j,y,\mu)(k,z,v)\big) &= (i,x,\lambda)(j,yp_{\mu k}z,v)\\ &= (i,xp_{\lambda j}yp_{\mu k}z,v)\\ &= (i,xp_{\lambda j}y,\mu)(k,z,v)\\ &= \big((i,x,\lambda)(j,y,\mu)\big)(k,z,v),\end{aligned}$$

and so S is a semigroup. Let $T = I \times \{0\} \times \Lambda$. It is easy to see that T is an ideal of S. Clearly, $S - T = I \times G \times \Lambda$. Notice that if $(i,x,\lambda), (j,y,\mu) \in S - T$, then $(i,x,\lambda)(j,y,\mu) \in T$ if and only if $p_{\lambda j} = 0$.

Let $\mathcal{M}_0[G;I,\Lambda;P]$ be the Rees factor semigroup S/T. Then the semigroup $\mathcal{M}_0[G;I,\Lambda;P]$ can be viewed as the set $(S - T) \cup \{0\}$: that is, $\mathcal{M}_0[G;I,\Lambda;P]$ can be viewed as the set $(I \times G \times \Lambda) \cup \{0\}$ under the multiplication

$$(i,x,\lambda)(j,y,\mu) = \begin{cases}(i,xp_{\lambda j}y,\mu) & \text{if } p_{\lambda j} \neq 0,\\ 0 & \text{if } p_{\lambda j} = 0,\end{cases}$$

$$0(i,x,\lambda) = (i,x,\lambda)0 = 00 = 0.$$

The semigroup $\mathcal{M}_0[G;I,\Lambda;P]$ is called the $I \times \Lambda$ *Rees matrix semigroup over* G^0 *with regular sandwich matrix* P.

Rees matrix ⇒ completely 0-simple

PROPOSITION 4.2. *For any group G, index sets I and Λ, and matrix P over G^0, the semigroup $\mathcal{M}_0[G;I,\Lambda;P]$ is completely 0-simple.*

Proof of 4.2. For brevity, let $S = \mathcal{M}_0[G;I,\Lambda;P]$.

Let $(i,x,\lambda) \in S - \{0\}$. Let $(j,y,\mu) \in S - \{0\}$. Since P is regular, we can choose $v \in \Lambda$ and $k \in I$ such that $p_{vi} \neq 0$ and $p_{\lambda k} \neq 0$. Then

$$\begin{aligned}&(j,1_G,v)(i,x,\lambda)(k,p_{\lambda k}^{-1}x^{-1}p_{vi}^{-1}y,\mu)\\ &= (j,1_G p_{vi}xp_{\lambda k}p_{\lambda k}^{-1}x^{-1}p_{vi}^{-1}y,\mu)\\ &= (j,y,\mu).\end{aligned}$$

Hence, since $(j,y,\mu) \in S - \{0\}$ was arbitrary, and since $0 = 0(i,x,\lambda)0$, we have $S \subseteq S(i,x,\lambda)S$. Since $(i,x,\lambda) \in S - \{0\}$ was arbitrary, S is 0-simple by Lemma 3.5.

Now, $(i,x,\lambda) \in S - \{0\}$ is an idempotent if and only if $(i,x,\lambda)(i,x,\lambda) = (i,xp_{\lambda i}x,\lambda) = (i,x,\lambda)$, which is true if and only if $p_{\lambda i} \neq 0$ and $x = p_{\lambda i}^{-1}$. Hence the idempotents in $S - \{0\}$ are elements of the form $(i,p_{\lambda i}^{-1},\lambda)$. Furthermore,

$$\begin{aligned}&(i,p_{\lambda i}^{-1},\lambda) \leq (j,p_{\mu j}^{-1},\mu)\\ \Leftrightarrow\ &(i,p_{\lambda i}^{-1},\lambda)(j,p_{\mu j}^{-1},\mu) = (j,p_{\mu j}^{-1},\mu)(i,p_{\lambda i}^{-1},\lambda) = (i,p_{\lambda i}^{-1},\lambda)\\ \Leftrightarrow\ &(i,p_{\lambda i}^{-1}p_{\lambda j}p_{\mu j}^{-1},\mu) = (j,p_{\mu j}^{-1}p_{\mu i}p_{\lambda i}^{-1},\lambda) = (i,p_{\lambda i}^{-1},\lambda)\\ \Leftrightarrow\ &(i=j) \wedge (\lambda = \mu)\\ \Leftrightarrow\ &(i,p_{\lambda i}^{-1},\lambda) = (j,p_{\mu j}^{-1},\mu).\end{aligned}$$

Hence every idempotent in $S - \{0\}$ is primitive. So S certainly contains primitive idempotents and so is 0-simple. 4.2

Proposition 4.2 gives a method for constructing completely 0-simple semigroups. In fact, as the following result shows, *all* completely 0-simple semigroups arise in this way:

Completely 0-simple ⇒ Rees matrix semigroups

PROPOSITION 4.3. *Let S be a completely 0-simple semigroup. Then $S \simeq \mathcal{M}_0[G; I, \Lambda; P]$ for some group G, index sets I and Λ, and regular sandwich matrix P.*

Proof of 4.3. Let S be completely 0-simple. So S contains a primitive idempotent e.

LEMMA 4.4. $R_e = eS - \{0\}$.

Proof of 4.4. Every element of R_e must be a right multiple of e and cannot be 0. Hence $R_e \subseteq eS - \{0\}$.

Let $x \in eS - \{0\}$. So $x = es$ for some $s \in S - \{0\}$. Hence $ex = ees = es = x$. Since S is 0-simple, by Lemma 3.5 there exist $p, q \in S$ with $pxq = e$. Let $p' = epe$. Then $p'xq = epexq = epxq = ee = e$.

Let $f = xqp'$. Then $f^2 = xqp'xqp' = xqep' = xqeepe = xqepe = xqp' = f$. So f is idempotent. Furthermore, $ef = exqp' = xqp' = f$ and $fe = xqp'e = xqepee = xqepe = xqp' = f$. So $ef = fe = f$ and hence $f \leq e$. Suppose that $f = 0$; then $e = e^2 = p'xqp'xq = p'fxq = 0$, which is a contradiction. Hence $f \neq 0$. But e is primitive and therefore $\leq$-minimal among idempotents not equal to zero; thus $e = f = xqp'$. Since $x = es$, it follows that $x \mathcal{R} e$ and so $x \in R_e$. Hence $eS - \{0\} \subseteq R_e$. 4.4

LEMMA 4.5. *For any $x \in S - \{0\}$,*

a) $R_x = xS - \{0\}$,

b) $L_x = Sx - \{0\}$.

Proof of 4.5. We prove part a); a dual argument gives part b). As in the proof of Lemma 4.4, $R_x \subseteq xS - \{0\}$. So let $y \in xS - \{0\}$. Then $y = xs$ for some $s \in S - \{0\}$. Since S is 0-simple, by Lemma 3.5 there exist $p, q \in S$ with $peq = x$. So $y = peqs$. By Lemma 4.4, $eqs, eq \in R_e$. Since $\mathcal{R}$ is a left congruence, $y = peqs \mathcal{R} peq = x$. So $y \in R_x$ and hence $xS - \{0\} \subseteq R_x$. 4.5

LEMMA 4.6. a) *the $\mathcal{D}$-classes of S are 0 and $S - \{0\}$;*

b) *S is regular;*

c) *for all $x, y \in S - \{0\}$, if $L_x \cap R_y$ contains an idempotent, then $xy \in R_x \cap L_y$; otherwise, $xy = 0$.*

Proof of 4.6. Let $x, y \in S - \{0\}$. Suppose $xSy = \{0\}$. Then

$$S^2 = SxSSyS \subseteq S(xSy)S = S\{0\}S = \{0\},$$

which contradicts the fact that 0-simple semigroups are (by definition) not null. Hence xSy contains some non-zero element z. Now, $z \in xS - \{0\} = R_x$ and $z \in Sy - \{0\} = L_y$. Thus $x \mathcal{R} z \mathcal{L} y$ and so $x \mathcal{D} y$. So the $\mathcal{D}$-classes of S must be $S - \{0\}$ and $\{0\}$.

The primitive idempotent e lies in $S - \{0\}$ and so every element of $S - \{0\}$ is regular by Proposition 3.17. Since 0 is also regular, the semigroup S is regular.

If $xy \neq 0$, then $xy \in (xS - \{0\}) \cap (Sy - \{0\}) = R_x \cap L_y$. By Proposition 3.16, this is true if and only if $L_x \cap R_y$ contains an idempotent. 4.6

Let H be an $\mathcal{H}$-class of S contained in the $\mathcal{D}$-class $S - \{0\}$. Let $x, y \in H$. Then either $xy = 0$ or $xy \in R_x \cap L_y = H$.

Suppose first that $xy = 0$. Let $z, t \in H$. Since $z \mathcal{L} x$ and $r \mathcal{R} y$, we have $z = px$ and $t = yr$ for some $x, y \in S^1$. Then $zt = pxyr = p0r = 0$. Since $z, t \in H$ were arbitrary, $H^2 = \{0\}$.

On the other hand, suppose that $xy \in H$. Then H is a subgroup by Proposition 3.12. So we can divide the $\mathcal{H}$-classes in $S - \{0\}$ into *zero* $\mathcal{H}$-classes and *group* $\mathcal{H}$-classes.

Let I be the set of $\mathcal{R}$-classes and let Λ be the set of $\mathcal{L}$-classes in $S - \{0\}$. Write the $\mathcal{R}$- and $\mathcal{L}$-classes as $R^{(i)}$ and $L^{(\lambda)}$ for $i \in I$ and $\lambda \in \Lambda$, and write $H^{(i\lambda)}$ for $R^{(i)} \cap L^{(\lambda)}$. We will treat I and Λ as abstract index sets.

Since $S - \{0\}$ is a regular $\mathcal{D}$-class, every $\mathcal{R}$-class and every $\mathcal{L}$-class contains an idempotent and thus some group $\mathcal{H}$-class. Therefore assume without loss that there is some element $1 \in I \cap \Lambda$ such that $H^{(11)}$ is a group $\mathcal{H}$-class. For brevity, write H for $H^{(11)}$.

For each $i \in I$ and $\lambda \in \Lambda$, fix arbitrary elements $r_\lambda \in H^{(1\lambda)} \subseteq R^{(1)}$ and $q_i \in H^{(i1)} \subseteq L^{(1)}$. Since 1_H is idempotent, it is a left identity for $R^{(1)}$ and a right identity for $L^{(1)}$. So $1_H r_\lambda = r_\lambda$ and $q_i 1_H = q_i$. Therefore, by Lemma 3.10, $\rho_{r_\lambda}|_{L^{(1)}} : L^{(1)} \to L^{(\lambda)}$ restricts to a bijection between H and $H^{(i1)}$ and $\lambda_{q_i}|_{R^{(1)}} : R^{(1)} \to R^{(1)}$ restricts to a bijection between $H^{(i1)}$ and $H^{(i\lambda)}$ for each $\lambda \in \Lambda$. This there is a unique expression $q_i x r_\lambda$, where $x \in H$, for every element of $H^{(i\lambda)}$.

Therefore the map $\varphi : (I \times H \times \Lambda) \cup \{0\} \to S$ defined by $(i, x, \lambda)\varphi = q_i x r_\lambda$ and $0\varphi = 0$ is a bijection.

To turn $(I \times H \times \Lambda) \cup \{0\}$ into a $I \times \Lambda$ Rees matrix semigroup over H^0, it remains to define a sandwich matrix P. For each $i \in I$ and $\lambda \in \Lambda$, let $p_{\lambda i} = r_\lambda q_i$. Notice that $p_{\lambda i} = r_\lambda q_i \in R_{r_\lambda} \cap L_{q_i} = R^{(1)} \cap L^{(1)} = H$ if and only if $R_{q_i} \cap L_{r_\lambda}$ contains an idempotent and is thus a group $\mathcal{H}$-class; otherwise $p_{\lambda i} = 0$. Hence each $p_{\lambda i}$ lies in H^0.

So φ is now a bijection from $\mathcal{M}_0[H; I, \Lambda; P]$ to S. For any elements $(i, x, \lambda), (j, y, \mu) \in \mathcal{M}_0[H; I, \Lambda; P] - \{0\}$,

$$\begin{aligned}\big((i,x,\lambda)\varphi\big)\big((j,y,\mu)\varphi\big) &= (q_i x r_\lambda)(q_j y r_\mu) = q_i x (r_\lambda q_j) y r_\mu \\ &= q_i x p_{\lambda j} y r_\mu\end{aligned}$$

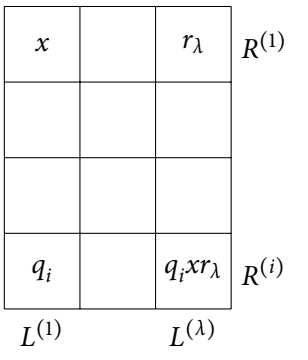


FIGURE 4.1
Choosing $r_\lambda \in H^{(1\lambda)}$ and $q_i \in H^{(i1)}$

$$= (i, xp_{\lambda j}y, \mu)\varphi$$
$$= \big((i, x, \lambda)(j, y, \mu)\big)\varphi.$$

Furthermore, $\big((i, x, \lambda)\varphi\big)(0\varphi) = q_i x r_\lambda 0 = 0 = \big((i, x, \lambda)0\big)\varphi$ and similarly for other multiplications involving 0. Hence the map φ is a homomorphism and hence an isomorphism between $\mathcal{M}_0[H; I, \Lambda; P]$ and S. 4.3

Combining Propositions 4.2 and 4.3, we get the following characterization of completely 0-simple semigroups:

Rees–Suschkewitsch theorem

THEOREM 4.7. *A semigroup S is completely 0-simple if and only if there exist a group G, index sets, I and Λ, and a $\Lambda \times I$ matrix P with entries from G^0 such that $S \simeq \mathcal{M}_0[G; I, \Lambda; P]$.* 4.7

IDEALS AND COMPLETELY 0-SIMPLE SEMIGROUPS

This section is devoted to a result characterizing the 0-simple semigroups that are also completely 0-simple. We require some definitions. A semigroup S is *group-bound* if every $x \in S$ has some power x^n lying in a subgroup of S. A semigroup *satisfies the condition* $\min_{\mathcal{L}}$ (respectively, $\min_{\mathcal{L}}$) if any subset of the partial order $S/\mathcal{L}$ (respectively, $S/\mathcal{R}$) has a minimal element.

Characterization of completely 0-simple semigroups

THEOREM 4.8. *Let S be 0-simple. The following are equivalent:*

a) *S is completely 0-simple;*

b) *S is group-bound;*

c) *S satisfies the conditions $\min_{\mathcal{L}}$ and $\min_{\mathcal{R}}$;*

d) *S contains a 0-minimal left ideal and a 0-minimal right ideal.*

Proof of 4.8. First part [a) ⇒ b)]. Suppose S is completely 0-simple. Let $x \in S$. Then either H_x is a subgroup and $x^2 \in H_x$, or else $x^2 = 0$. In either case, x^2 lies in a subgroup. Thus S is group-bound.

Second part [b) ⇒ c)]. Suppose S is group-bound. Let $x, y \in S - \{0\}$ be such that $L_x \leq L_y$. We are going to show that $L_x = L_y$. Then $x = py$ for some $p \in S$. Furthermore, $y = qxr$ for some $q, r \in S$ by Lemma 3.5. Then $y = qxr = qpyr$ and so $y = (qp)^n y r^n$ for all $n \in \mathbb{N}$. Fix n so that $g = (qp)^n$ lies in a subgroup G. Then $1_G y = 1_G g y r^n = g y r^n = y$ and so $y = g^{-1}gy = g^{-1}(qp)^n y = g^{-1}(qp)^{n-1}qpy = g^{-1}(qp)^{n-1}qx$. Hence $L_y \leq L_x$ and so $L_x = L_y$. Therefore $L_x \leq L_y \Rightarrow L_x = L_y$, and this certainly implies that any subset of $S/\mathcal{L}$ is has a minimal element. So S satisfies $\min_{\mathcal{L}}$. Similarly, $S/\mathcal{R}$ satisfies $\min_{\mathcal{R}}$.

Third part [c) ⇒ d)]. Suppose S satisfies $\min_{\mathcal{L}}$ and $\min_{\mathcal{R}}$. Then there among the $\mathcal{L}$-classes that are not equal to $\{0\}$ there is a minimal. Let L_x be such a minimal non-$\{0\}$ $\mathcal{L}$-class. Then Sx is a left ideal not equal to $\{0\}$. Suppose L is some left ideal contained in Sx and not equal to $\{0\}$. Pick $y \in L - \{0\}$. Then $Sy \subseteq Sx$ and so $L_y \subseteq L_x$. Since L_x is minimal among non-$\{0\}$ $\mathcal{L}$-classes, $L_x = L_y$ and so $Sx = Sy$. So Sx must be a 0-minimal left ideal. Similarly S must contain a 0-minimal right ideal.

Fourth part [d) ⇒ a)]. Suppose S contains a 0-minimal left ideal and a 0-minimal right ideal.

LEMMA 4.9. a) *If L is a 0-minimal non-null left ideal of S, then $L = Sx$ for any $x \in L - \{0\}$.*

b) *If R is a 0-minimal non-null right ideal of S, then $R = xS$ for any $x \in R - \{0\}$.*

Proof of 4.9. We prove part a); a dual argument gives part b).

Let $x \in L - \{0\}$. Then Sx is a left ideal of S and is contained in L. Since L is 0-minimal, either $Sx = L$ or $Sx = \{0\}$. Suppose, with the aim of obtaining a contradiction, that $Sx = \{0\}$. Then $\{0, x\}$ is a left ideal of S contained in L and not equal to $\{0\}$. Since L is 0-minimal, $L = \{x, 0\}$. But then L is null, which is a contradiction. So $L = Sx$. 4.9

LEMMA 4.10. a) *S is the union of its 0-minimal left ideals.*

b) *S is the union of its 0-minimal right ideals.*

Proof of 4.10. We prove part a); a dual argument gives part b).

Let L be a 0-minimal left ideal. Suppose $x \in S$ is such that $Lx \neq \{0\}$. Note that Lx is a left ideal. Suppose $K \neq \{0\}$ is a left ideal contained in Lx. Let $J = \{y \in L : yx \in K\}$. Then J is a left ideal and $J \subseteq L$. Since L is 0-minimal and $J \neq \{0\}$, we have $J = L$ and so $K = Jx = Ls$. Hence Lx is 0-minimal.

Now, LS is an ideal and so, since S is 0-simple, either $LS = \{0\}$ or $LS = S$. Suppose, with the aim of obtaining a contradiction, that $LS = \{0\}$. Then $LS \subseteq L$ and so L is an ideal. Since $L \neq \{0\}$, we have $L = S$. Hence $S^2 = LS = \{0\}$ and so S is null, which contradicts S being 0-simple. Therefore $LS = S$. So there exists $x \in S$ with $Lx \neq \{0\}$.

Let $M = \bigcup\{Lx : x \in S, Lx \neq \{0\}\}$. Then M is a union of 0-minimal left ideals and is thus itself a left ideal. By the preceding paragraph, $M \neq \{0\}$. Let $m \in M$ and $z \in S$. Then $m \in Lx$ for some $x \in S$ and so $mt \in Lxt \subseteq M$. Hence $MS \subseteq M$ and so M is also a right ideal. So M is an ideal and not equal to $\{0\}$. Since S is 0-simple, we have $M = S$. 4.10

Let L be a 0-minimal left ideal. For any 0-minimal right ideal R, the set LR is an ideal and hence, since S is 0-simple, either $LR = \{0\}$ or $LR = S$. By the proof of Lemma 4.10(a), there exists some $x \in S$ with $Lx \neq \{0\}$. By Lemma 4.10(b), x lies in some 0-minimal right ideal. Fix R containing x. Then $LR \neq \{0\}$ and so $LR = S$.

Notice that since R is a right ideal, $RL \subseteq R$. Similarly, $RL \subseteq L$. Let $x \in RL - \{0\} \subseteq R - \{0\}$. Then $R = xS$ by Lemma 4.9(b). Since $S = LR = LxS$, we have $Lx \neq \{0\}$ and so by the proof of Lemma 4.10(b), Lx is a 0-minimal left ideal. However, $Lx \subseteq L$ since $x \in RL \subseteq L$. Therefore, since L is 0-minimal and $Lx \neq \{0\}$, we have $Lx = L$ and so $RLx = RL$. Similarly $xRL = RL$. Hence RL is a group with a zero adjoined.

Let e be the identity of the group $RL - \{0\}$. Let f be a non-zero idempotent in S with $f \leq e$. Then $ef = fe = f$. Since $e \in RL \subseteq R \cap L$, it follows Lemma 4.9 that $R = eS$ and $L = Se$. Hence $f = efe \in eSe = eS^2e = (eS)(Se) = RL$. Since $RL - \{0\}$ is a group, $e = f$. So e is a primitive idempotent. Hence S is completely 0-simple. 4.8

COMPLETELY SIMPLE SEMIGROUPS

Completely simple

An idempotent of a semigroup without zero is *primitive* if it is minimal. A semigroup without zero is *completely simple* if it is simple and contains a primitive idempotent.

Define a new version of the Rees matrix construction as follows. Let G be a group, let I and Λ be abstract index sets, and let P be a $\Lambda \times I$ matrix with entries from G, with the (λ, i)-th entry of P being $p_{\lambda i}$. Let $\mathcal{M}[G; I, \Lambda; P]$ be the set $I \times G \times \Lambda$ with multiplication

$$(i, x, \lambda)(j, y, \mu) = (i, xp_{\lambda j}y, \mu).$$

Then we have the following characterization of completely simple semigroups, paralleling Theorem 4.7:

THEOREM 4.11. *A semigroup S is completely simple if and only if there exist a group G, index sets I and Λ, and a $\Lambda \times I$ matrix P with entries from G such that $S \simeq \mathcal{M}[G; I, \Lambda; P]$.* 4.11

Theorem 4.11, and many other properties of completely simple semigroups, are consequences of the following observations:

- S is simple if and only if S^0 is 0-simple;
- an idempotent is a primitive in S if and only if it is primitive in S^0;
- for any group G, index sets I and Λ, and $\Lambda \times I$ matrix P with entries from G, we have $(\mathcal{M}[G; I, \Lambda; P])^0 = \mathcal{M}_0[G; I, \Lambda; P]$.

Notice that in the second condition above, 'primitive' means 'minimal' in S and 'minimal and non-0' in S^0.

PROPOSITION 4.12. *A semigroup is completely simple if and only if it is regular and every idempotent is primitive.*

Proof of 4.12. Suppose S is completely simple. Then $S \simeq \mathcal{M}[G; I, \Lambda; P]$. Then S consists of a single $\mathcal{D}$-class. Furthermore, S contains idempotents, which are regular elements. Hence S is regular by Proposition 3.17. By following the reasoning in the proof of Proposition 4.2 (and ignoring mentions of the zero), every idempotent in S is primitive.

Now suppose that S is regular and every idempotent is primitive. We have to show that S is simple. Since S is regular, every $\mathcal{D}$-class contains an idempotent. So every $\mathcal{J}$-class contains an idempotent. Let J_e be a $\mathcal{J}$-class and let $J_f \leq J_e$, where e and f are idempotents. Then $f = peq$ for some $p, q \in S^1$. Let $g = eqfpe$. Then

$$\begin{aligned} g^2 &= eqfpeeqfpe && \text{[by definition of } g\text{]} \\ &= eqfpeqfpe && \text{[since } e \text{ is idempotent]} \\ &= eqfffpe && \text{[since } f = peq\text{]} \\ &= eqfpe && \text{[since } f \text{ is idempotent]} \\ &= g; && \text{[by definition of } g\text{]} \end{aligned}$$

thus g is idempotent. Furthermore $ge = eg = g$ and so $g \leq e$. Since e is primitive (since all idempotents are primitive), it follows that $g = e$.

Therefore $f = peq$ and $e = g = eqfpe$. Hence $J_e = J_f$. Since all $\mathcal{J}$-classes contain idempotents, S contains only one $\mathcal{J}$-class. Hence all elements $x \in S$ generates the same principal ideal, S^1xS^1, which must thus be the kernel of S. Hence $x \in K(S)$ for all $x \in S$. Therefore $K(S) = S$ and so S is simple. 4.12

COMPLETELY REGULAR SEMIGROUPS

Characterizing completely regular

PROPOSITION 4.13. *Let S be a semigroup. Then the following are equivalent:*

a) *S is completely regular;*

b) *every element of S lies in a subgroup of S;*

c) *every $\mathcal{H}$-class of S is a subgroup.*

Proof of 4.13. First part [a) ⇒ b)]. Suppose S is completely regular. Let $x \in S$. Then $e = xx^{-1} = x^{-1}x$ is an idempotent. By Proposition 3.16, $x \in R_e \cap L_e = H_e$, which is a subgroup. So every element of S lies in a subgroup.

Second part [b) ⇒ c)]. Suppose every element of S lies in a subgroup. Let $x \in S$. Then $x \in G$ for some subgroup G of S. Then $x \mathcal{H} 1_G$ and so $H_x = H_{1_G}$, which contains an idempotent and is thus a subgroup. So every $\mathcal{H}$-class of S is a subgroup.

Third part [c) ⇒ a)]. Suppose every $\mathcal{H}$-class of S is a subgroup. Define $^{-1}$ by letting x^{-1} (where $x \in S$) be the unique inverse of x in the subgroup

H_x. It is clear that $^{-1}$ satisfies the conditions (4.3) and S is thus completely regular. 4.13

The following result follows from Proposition 4.13 and Theorem 4.8:

Characterization of completely simple semigroups

THEOREM 4.14. *Let S be simple. The following are equivalent:*

a) *S is completely simple;*

b) *S is completely regular;*

c) *S satisfies the conditions $\min_{\mathcal{L}}$ and $\min_{\mathcal{R}}$;*

d) *S contains a minimal left ideal and a minimal right ideal.* 4.14

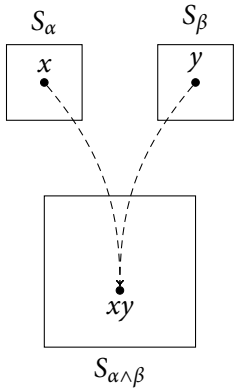


FIGURE 4.2
Multiplying in a semilattice of semigroups

A *semilattice of semigroups* is a semigroup S for which there exists a semilattice Y and a collection of disjoint subsemigroups S_α of S, where $\alpha \in Y$, such that $S = \bigcup_{\alpha\in Y} S_\alpha$ and $S_\alpha S_\beta \subseteq S_{\alpha\wedge\beta}$ (see Figure 4.2). A *semilattice of completely simple semigroups* is one in which every S_α is completely simple; a *semilattice of groups* is one in which every S_α is a group.

THEOREM 4.15. *Every completely regular semigroup is a semilattice of completely simple semigroups.*

Proof of 4.15. Let S be a completely regular semigroup.

By Proposition 4.13, each $\mathcal{H}$-class of S is a subgroup. So for any $x \in S$, we have $x^2 \mathcal{H} x$ and hence $x^2 \mathcal{J} x$. Hence for any $x, y \in S$, we have $J_{xy} = J_{(xy)^2} = J_{x(yx)y} \leq J_{yx}$. By symmetry, $J_{yx} \leq J_{xy}$ and so $J_{xy} = J_{yx}$.

Let $x \mathcal{J} y$. Then there exist $r, s \in S^1$ with $rys = x$. Let $z \in S$. Then

$$J_{zx} = J_{zrys} \leq J_{zry} = J_{ryz} \leq J_{yz} = J_{zy}.$$

By symmetry $J_{zy} \leq J_{zx}$ and hence $J_{zx} = J_{zy}$. So $zx \mathcal{J} zy$. Similarly $xz \mathcal{J} yz$. Therefore $\mathcal{J}$ is a congruence. The factor semigroup $S/\mathcal{J}$ is a commutative semigroup of idempotents since $x^2 \mathcal{J} x$ and $xy \mathcal{J} yx$ for all $x, y \in S$. Hence $S/\mathcal{J}$ is a semilattice by Theorem 1.18.

Since $\mathcal{J}$ is a congruence, $(J_x)^2 \subseteq J_{x^2} = J_x$ and so J_x is a subsemigroup. Furthermore, $J_x J_y \subseteq J_{xy}$.

The aim is to show $J_x y J_x = J_x$ for all $y \in J_x$, and deduced that J_x is simple. Let $z \in J_x$. Since $y \mathcal{J} z$, there exist $p, q, r, s \in S$ such that $pyq = z$ and $rzs = y$. [We cannot immediately deduce that $z \in J_x y J_x$, because p and q may not lie in J_x.] Write 1_y for the identity of H_y and 1_z for the identity of H_z. Since $y, z \in J_x$, it follows that $1_y, 1_z \in J_x$. Then $(1_z p)y(q1_z) = 1_z z 1_z = z$ and $(1_y r)z(s1_y) = 1_y y 1_y = y$. Furthermore, $J_{1_z p} \geq J_{(1_z p)y(q1_z)} = J_z = J_x$ and $J_{1_z p} \leq J_{1_z} = J_x$. Hence $1_z p \in J_x$. Similarly $q1_z, 1_z r, s1_z \in J_x$. Hence $z \in J_x y J_x$. Since $z \in J_x$ was arbitrary, $J_x = J_x y J_x$. Therefore J_x is simple.

Thus, since J_x is completely regular, it is completely simple by Theorem 4.14.

To see S is a semilattice of completely simple semigroups, let Y be the semilattice $S/\mathcal{J}$ and write S_α instead of $\alpha \in S/\mathcal{J}$. 4.15

EXERCISES

[See pages 152–157 for the solutions.]

✶4.1 Let S be a regular semigroup, T a semigroup (not necessarily regular), and let $\varphi : S \to T$ be a homomorphism. Prove that $\operatorname{im}\varphi$ is a regular semigroup. Prove further that if $e \in \operatorname{im}\varphi$ is idempotent, $f\varphi = e$, and $x \in S$ is an inverse of f^2, then fxf is idempotent and $(fxf)\varphi = e$.

4.2 Let G be a group, $I = \{1\}$ and $\Lambda = \{1\}$ index sets (each containing only one element), and P a matrix over G.

a) Prove that $\mathcal{M}[G; I, \Lambda; P] \simeq G$.

b) Give an example to show that if we replace G by a monoid M and construct $\mathcal{M}[M; I, \Lambda; P]$ using the same multiplication, we can have $\mathcal{M}[M; I, \Lambda; P] \not\simeq M$.

✶4.3 Let $S = \mathcal{M}[G; I, \Lambda; P]$. Prove that

a) the $\mathcal{L}$-classes of S are sets of the form $I \times G \times \{\lambda\}$;

b) the $\mathcal{R}$-classes of S are sets of the form $\{i\} \times G \times \Lambda$;

c) the $\mathcal{H}$-classes of S are sets of the form $\{i\} \times G \times \{\lambda\}$.

4.4 Prove that every completely simple semigroup is equidivisible.

4.5 Let S be a completely simple semigroup. Prove that

a) $\mathcal{L}$, $\mathcal{R}$, and $\mathcal{H}$ are congruences on S;

b) $S/\mathcal{L}$ is a right zero semigroup and $S/\mathcal{R}$ is a left zero semigroup;

c) $S/\mathcal{H}$ is isomorphic to the rectangular band $S/\mathcal{R} \times S/\mathcal{L}$.

4.6 Let S be a completely simple semigroup.

a) Suppose $|S| = p$, where p is a prime. Prove that S is [isomorphic to] either a right zero semigroup, a left zero semigroup, or a group.

b) Suppose $|S| = pq$, where p and q are primes. Prove that S is [isomorphic to] either a rectangular band, a right group, or a left group. (See Exercise 3.11 for the definition of a right group; the definition of a left group is dual.)

✶4.7 a) Let S and T be completely regular semigroups and $\varphi : S \to T$ a homomorphism. Show that $(z\varphi)^{-1} = z^{-1}\varphi$ for all $z \in S$.

b) Give an example of regular semigroups S and T, where S and T each have an operation $^{-1}$ satisfying

$$(x^{-1})^{-1} = x \text{ and } xx^{-1}x = x \text{ for all } x \in S,$$

(that is, satisfying the definition of completely regular semigroups except for the condition $xx^{-1} = x^{-1}x$) and a homomorphism $\varphi : S \to T$ such that $(z\varphi)^{-1} \neq z^{-1}\varphi$ for some $z \in S$.

✶4.8 Let G and H be groups, I, J, Λ, and M be index sets, P be a $\Lambda \times I$ regular matrix over G^0, and Q be a $J \times$ M regular matrix over H^0.

a) Suppose $\varphi : \mathcal{M}_0[G; I, \Lambda; P] \to \mathcal{M}_0[H; J, \mathrm{M}; Q]$ be an isomorphism.

i) Prove that there exist bijections $\alpha : I \to J$ and $\beta : \Lambda \to \mathrm{M}$ such that $(i, a, \lambda)\varphi \in \{i\alpha\} \times H \times \{\lambda\beta\}$ and such that $p_{\lambda i} = 0 \Leftrightarrow q_{(\lambda\beta)(i\alpha)} = 0$.

ii) Assume without loss that $1 \in I \cap \Lambda$. Define an isomorphism $\gamma : G \to \{1\} \times G \times \{1\} \subseteq \mathcal{M}_0[G; I, \Lambda; P]$ and an isomorphism $\eta : H \to \{1\alpha\} \times H \times \{1\beta\} \subseteq \mathcal{M}_0[H; J, \mathrm{M}; Q]$. Deduce that $\theta = \gamma\varphi\eta^{-1}$ is an isomorphism from G to H.

iii) Check that $(i, x, \lambda) = (i, 1_G, 1)(1, p_{11}^{-1}x, 1)(1, p_{11}^{-1}, \lambda)$. Let $u_i, v_\lambda \in H$ be such that

$$(i, 1_G, 1)\varphi = (i\alpha, u_i, 1\beta) \text{ and } (1, p_{11}^{-1}, \lambda)\varphi = (1\alpha, q_{(1\alpha)(1\beta)}^{-1} v_\lambda, \lambda\beta).$$

Using the fact that $(i, p_{\lambda i}, \lambda) = (i, 1_G, \lambda)(i, 1_G, \lambda)$, prove that

$$p_{\lambda i}\theta = v_\lambda q_{(\lambda\beta)(i\alpha)} u_i \tag{4.6}$$

for all $i \in I$ and $\lambda \in \Lambda$.

b) Suppose that there exists an isomorphism $\theta : G \to H$, bijections $\alpha : I \to J$ and $\beta : \Lambda \to \mathrm{M}$ and elements u_i and v_λ such that (4.6) holds for all $i \in I$ and $\lambda \in \Lambda$. Show that $\mathcal{M}_0[G; I, \Lambda; P] \simeq \mathcal{M}_0[H; J, \mathrm{M}; Q]$.

✶ 4.9 Let G be a group, I and Λ index sets, and let P be a matrix over G^0 that is not necessarily regular (that is, P can have rows or columns where all the entries are 0). Let $S = \mathcal{M}_0[G; I, \Lambda; P]$, where the multiplication is the same as in the usual Rees matrix semigroup. Prove that S is regular (as a semigroup) if and only if P is regular (as a matrix).

NOTES

The Rees–Suschkewitsch theorem (Theorem 4.7) was originally proved in Rees, 'On semi-groups'; the analogue for completely simple semigroups is the earlier version, having been essentially proved in Suschkewitsch, 'Über die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit'. The results on the structure of completely regular semigroups are due to Clifford, 'Semigroups admitting relative inverses'.

Inverse semigroups

5

Inverse semigroups

❁ Recall that an inverse semigroup is one equipped with an operation $^{-1}$ satisfying the four conditions in (4.4), namely that for all $x, y \in S$,

$$(x^{-1})^{-1} = x, \tag{5.1}$$
$$(xy)^{-1} = y^{-1}x^{-1}, \tag{5.2}$$
$$xx^{-1}x = x, \tag{5.3}$$
$$xx^{-1}yy^{-1} = yy^{-1}xx^{-1}. \tag{5.4}$$

Characterization of inverse semigroups

THEOREM 5.1. *The following are equivalent:*

a) *S is an inverse semigroup;*

b) *every element of S has a unique inverse;*

c) *S is regular and its idempotents commute;*

d) *every $\mathcal{L}$-class and every $\mathcal{R}$-class of S contains exactly one idempotent.*

Proof of 5.1. First part [a) ⇒ c)]. Suppose S is an inverse semigroup. Let $x \in S$. Then $xx^{-1}x = x$ by (5.3) and so S is regular. Let $e \in E(S)$. Then

$$\begin{aligned}
e^{-1} &= e^{-1}ee^{-1} && \text{[by (5.3)]}\\
&= e^{-1}eee^{-1} && \text{[since } e \text{ is idempotent]}\\
&= e^{-1}(e^{-1})^{-1}ee^{-1} && \text{[by (5.1)]}\\
&= ee^{-1}e^{-1}(e^{-1})^{-1} && \text{[by (5.4)]}\\
&= ee^{-1}e^{-1}e && \text{[by (5.1)]}\\
&= e(ee)^{-1}e && \text{[by (5.2)]}\\
&= ee^{-1}e && \text{[since } e \text{ is idempotent]}\\
&= e. && \text{[by (5.3)]}
\end{aligned}$$

Hence $ee^{-1} = e^{-1}e = e$ for any $e \in E(S)$. Now let $e, f \in E(S)$. Then $ef = ee^{-1}ff^{-1} = ff^{-1}ee^{-1} = fe$ by (5.4). Thus idempotents of S commute.

Second part [b) ⇒ c)]. Suppose every element of S has a unique inverse. Then S is clearly regular. Let $e, f \in E(S)$. Then

$$(ef)(f(ef)^{-1}e)(ef) = ef^2(ef)^{-1}e^2f = ef(ef)^{-1}ef = ef$$

and

$$(f(ef)^{-1}e)(ef)(f(ef)^{-1}e) = f(ef)^{-1}ef(ef)^{-1}e = f(ef)^{-1}e$$

and so $f(ef)^{-1}e$ is an inverse of ef. By the uniqueness of inverses, $(ef)^{-1} = f(ef)^{-1}e$. Hence

$$((ef)^{-1})^2 = f(ef)^{-1}ef(ef)^{-1}e = f(ef)^{-1}e = (ef)^{-1}$$

and so $(ef)^{-1}$ is idempotent. Thus, since $(ef)^{-1}(ef)^{-1}(ef)^{-1} = (ef)^{-1}$, the uniqueness of inverses implies that $ef = ((ef)^{-1})^{-1} = (ef)^{-1}$ and so ef is idempotent. A similar argument shows that fe is idempotent. Hence

$$(ef)(fe)(ef) = ef^2e^2f = efef = ef$$

and

$$(fe)(ef)(fe) = fe^2f^2e = fefe = fe.$$

Hence $fe = (ef)^{-1} = ef$. Thus idempotents of S commute.

Third part [c) ⇒ d)]. Suppose that S is regular and that its idempotents commute. Since S is regular, every $\mathcal{L}$-class contains at least one idempotent by Proposition 3.18. So suppose a particular $\mathcal{L}$-class contains idempotents e and f. Then both e and f are right identities for this $\mathcal{L}$-class by Proposition 3.15. So $ef = e$ and $fe = f$. Since idempotents commute, $ef = fe$ and so $e = f$. So each $\mathcal{L}$-class contains a unique idempotent. Similarly each $\mathcal{R}$-class contains a unique idempotent.

Fourth part [d) ⇒ b)]. Suppose every $\mathcal{L}$-class and every $\mathcal{R}$-class of S contains a unique idempotent. Let $x \in S$. By Proposition 3.19, the inverses of x are in one-to-one correspondence with pairs of idempotents $(e,f) \in R_x \times L_x$. Since R_x and L_x each contain a unique idempotent, x therefore has a unique inverse. So every element of S has a unique inverse.

Fifth part [b) ⇒ a)]. Suppose every element of S has a unique inverse. Then for any $x \in S$, we have $xx^{-1}x = x$; thus (5.3) holds. By the uniqueness of inverses, $(x^{-1})^{-1} = x$; thus (5.1) holds. Let $x, y \in S$. Then xx^{-1} and yy^{-1} are idempotents and so commute by the second and third parts of this proof; thus (5.4) holds. Therefore

$$xy(y^{-1}x^{-1})xy = x(yy^{-1})(x^{-1}x)y = xx^{-1}xyy^{-1}y = xy$$

and

$$(y^{-1}x^{-1})xy(y^{-1}x^{-1} = y^{-1}(x^{-1}x)(yy^{-1})x^{-1} = y^{-1}yy^{-1}x^{-1}xx^{-1} = y^{-1}x^{-1}.$$

Hence, by the uniqueness of inverses, $(xy)^{-1} = y^{-1}x^{-1}$; thus (5.2) holds. Thus S is an inverse semigroup. 5.1

Let S be an inverse semigroup. By Theorem 5.1, all elements of $E(S)$ commute. Hence, if $e,f \in E(S)$, then $(ef)^2 = efef = e^2f^2 = ef$ and so $ef \in E(S)$. So $E(S)$ is a subsemigroup of S; furthermore, $E(S)$ is a commutative semigroup of idempotents and hence a semilattice by Theorem 1.18.

PROPOSITION 5.2. *Let S be an inverse semigroup. Then S is a group if and only if S contains exactly one idempotent.*

Proof of 5.2. In one direction, this result is obvious: if S is a group, then 1_S is the unique idempotent in S.

So suppose S is an inverse semigroup and e is the unique idempotent in S. Let $x \in S$. Then xx^{-1} and $x^{-1}x$ are idemopotents and so $e = xx^{-1} = x^{-1}x$. Thus $ex = xx^{-1}x = x$ and $xe = xx^{-1}x = x$. So e is an identity for S. Furthemore, since $e = xx^{-1} = x^{-1}x$ for all $x \in S$, every element of x is right- and left-invertible and so S is a group. 5.2

LEMMA 5.3. *Let S be an inverse semigroup.*

a) *For any $e, f \in E(S)$, we have $Se = Sf \Rightarrow e = f$.*

b) *For any $e, f \in E(S)$, we have $Se \cap Sf = Sef$.*

c) *For any $x \in S$, we have $Sx = Sx^{-1}x$.*

d) *For $x \in S$ and $e \in E(S)$, the element $f = x^{-1}ex$ is idempotent and $ex = xf$.*

Proof of 5.3. a) Since $e = ee \in Se = Sf$, we deduce that $e = xf$ for some $x \in S$. Then $ef = xf^2 = xf = e$. Similarly $fe = f$. Since idempotents commute, $e = f$.

b) Obviously $Sef \subseteq Sf$ and, since idempotents commute, $Sef = Sfe \subseteq Se$. So $Sef \subseteq Se \cap Sf$. Let $x \in Se \cap Sf$. Then $x = ye$ and $x = zf$ for some $y, z \in S$. Then $x = zf = zf^2 = xf = yef \in Sef$. So $Se \cap Sf \subseteq Sef$ and hence $Se \cap Sf = Sef$.

c) Obviously $Sx^{-1}x \subseteq Sx$. But $Sx = Sxx^{-1}x \subseteq Sx^{-1}x$ and so $Sx = Sx^{-1}x$.

d) Since idempotents commute, $f^2 = x^{-1}exx^{-1}ex = x^{-1}xx^{-1}eex = x^{-1}ex = f$, so f is idempotent. Furthermore, $ex = exx^{-1}x = xx^{-1}ex = xf$. 5.3

VAGNER–PRESTON THEOREM

Theorem 1.19 showed that every semigroup embeds into $\mathcal{T}_X$ for some X. Cayley's Theorem shows that every group embeds into $\mathcal{S}_X$ for some X. The Vagner-Preston theorem, to which this section is devoted, is an analogue of these results for inverse semigroups.

Partial bijections

Let $\tau \in \mathcal{P}_X$. Recall from (1.3) that the domain of τ, denoted $\operatorname{dom}\tau$, is the subset of X on which τ is defined. If $\tau : \operatorname{dom}\tau \to \operatorname{im}\tau$ is a bijection, then τ is a *partial bijection*. The set of partial bijections on X is denoted $\mathcal{I}_X$. (The symbol $\mathcal{I}$ stands for 'injection'.) Notice that if $\tau, \sigma \in \mathcal{I}_X$, then

$$\begin{aligned}\operatorname{dom}(\tau\sigma) &= \{x \in X : (\exists y \in X)((x,y) \in \tau\sigma)\}\\ &= \{x \in X : (\exists y \in X)(\exists z \in X)((x,z) \in \tau \wedge (z,y) \in \sigma\}\\ &= \{x \in X : (\exists z \in X)((x,z) \in \tau \wedge z \in \operatorname{dom}\sigma\}\end{aligned}$$

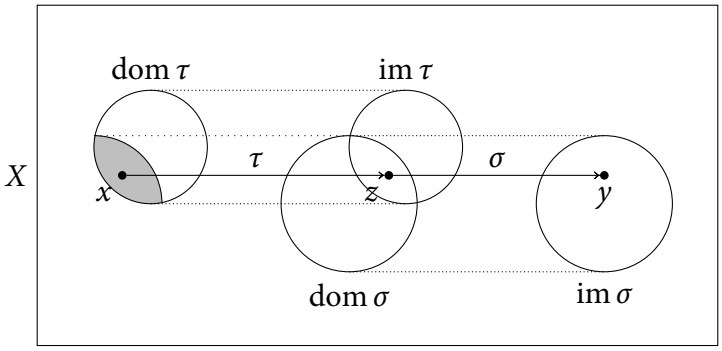


FIGURE 5.1
The domain of the composition of two partial bijections

$$
\begin{aligned}
&= \{x \in X : (x \in \operatorname{dom}\tau) \wedge (x\tau \in \operatorname{dom}\sigma)\} \\
&= \{x \in X : (x\tau \in \operatorname{im}\tau) \wedge (x\tau \in \operatorname{dom}\sigma)\} \\
&= \{x \in X : (x\tau \in \operatorname{im}\tau \cap \operatorname{dom}\sigma)\} \\
&= (\operatorname{im}\tau \cap \operatorname{dom}\sigma)\tau^{-1};
\end{aligned}
$$

see Figure 5.1. For $x, y \in \operatorname{dom}\tau\sigma$, we have $x, y \in \operatorname{dom}\tau$ and $x\tau, y\tau \in \operatorname{dom}\sigma$ and so

$$
\begin{aligned}
x\tau\sigma = y\tau\sigma &\Rightarrow x\tau = y\tau && \text{[since } \sigma \text{ is injective]} \\
&\Rightarrow x = y. && \text{[since } \tau \text{ is injective]}
\end{aligned}
$$

Hence $\tau\sigma$ is a bijection from $\operatorname{dom}(\tau\sigma)$ to $\operatorname{im}(\tau\sigma)$ and so $\tau\sigma \in \mathcal{I}_X$. Thus $\mathcal{I}_X$ is a subsemigroup of $\mathcal{P}_X$.

Inverses of partial bijections

For $\tau \in \mathcal{I}_X$, let τ^{-1} be the partial bijection with domain $\operatorname{im}\tau$ and image $\operatorname{dom}\tau$ defined by $(x\tau)\tau^{-1} = x$. (That is, τ is defined by inverting the bijection $\tau : \operatorname{dom}\tau \to \operatorname{im}\tau$.) Then $\tau\tau^{-1} = \mathrm{id}_{\operatorname{dom}\tau}$ and $\tau^{-1}\tau = \mathrm{id}_{\operatorname{im}\tau}$.

$\mathcal{I}_X$ is an inverse semigroup

PROPOSITION 5.4. *For any set X, the semigroup of partial bijections $\mathcal{I}_X$ is an inverse semigroup.*

Proof of 5.4. Let $\tau \in \mathcal{I}_X$. Since $\tau\tau^{-1} = \mathrm{id}_{\operatorname{dom}\tau}$ and $\tau^{-1}\tau = \mathrm{id}_{\operatorname{im}\tau}$, we have $\tau\tau^{-1}\tau = \tau$ and $\tau^{-1}\tau\tau^{-1}$. Hence τ^{-1} is an inverse of τ. Thus $\mathcal{I}_X$ is regular.

Suppose $\sigma \in \mathcal{I}_X$ is an inverse of τ. Then $\tau\sigma\tau = \tau$ and $\sigma\tau\sigma = \sigma$. From the first equality, $\operatorname{im}\tau \subseteq \operatorname{dom}\sigma$. From the second equality, $\operatorname{dom}\sigma \subseteq \operatorname{im}\tau$. Hence $\operatorname{dom}\sigma = \operatorname{im}\tau = \operatorname{dom}\tau^{-1}$. For any $x \in \operatorname{dom}\sigma$, we have $x \in \operatorname{im}\tau$ and so $x = y\tau$ for some $y \in X$. Hence $x\sigma = y\tau\sigma = y\tau\sigma\tau\tau^{-1} = y\tau\tau^{-1} = x\tau^{-1}$. Hence $\sigma = \tau^{-1}$. So τ^{-1} is the unique inverse of τ.

Since each element of $\mathcal{I}_X$ has a unique inverse, $\mathcal{I}_X$ is an inverse semigroup by Theorem 5.1. 5.4

Vagner–Preston representation theorem

THEOREM 5.5. *Let S be an inverse semigroup. Then there exists a set X and a monomorphism $\varphi : S \to \mathcal{I}_X$. Hence S is isomorphic to a subsemigroup of $\mathcal{I}_X$.*

Proof of 5.5. Let $X = S$. For each $x \in S$, let τ_x be the partial transformation with domain Sx^{-1} and defined by $y\tau_x = yx$. Thus τ_x is simply ρ_x restricted to Sx^{-1}.

Let us prove that $\tau_x \in \mathcal{I}_X$. Let $y, z \in Sx^{-1}$, with $y = px^{-1}$ and $z = qx^{-1}$. Then

$$\begin{aligned} y\tau_x = z\tau_x &\Rightarrow yx = zx \\ &\Rightarrow px^{-1}x = qx^{-1}x \\ &\Rightarrow px^{-1}xx^{-1} = qx^{-1}xx^{-1} \\ &\Rightarrow px^{-1} = qx^{-1} \\ &\Rightarrow y = z. \end{aligned}$$

So τ_x is a partial bijection and so $\tau_x \in \mathcal{I}_X$.

Define $\varphi : S \to \mathcal{I}_X$ by $x\varphi = \tau_x$. We first prove that φ is injective. Let $x, y \in S$. Then

$$\begin{aligned} x\varphi = y\varphi &\Rightarrow \tau_x = \tau_y && \text{[by definition of } \varphi\text{]} \\ &\Rightarrow \operatorname{dom}\tau_x = \operatorname{dom}\tau_y \\ &\Rightarrow Sx^{-1} = Sy^{-1} && \text{[by definition of } \tau_x \text{ and } \tau_y\text{]} \\ &\Rightarrow Sxx^{-1} = Syy^{-1} && \text{[by Lemma 5.3(c)]} \\ &\Rightarrow xx^{-1} = yy^{-1} && \text{[by Lemma 5.3(a)]} \\ &\Rightarrow xx^{-1}\tau_x = yy^{-1}\tau_y && \text{[since } \tau_x = \tau_y\text{]} \\ &\Rightarrow xx^{-1}x = yy^{-1}y && \text{[by definition of } \tau_x \text{ and } \tau_y\text{]} \\ &\Rightarrow x = y; \end{aligned}$$

thus φ is injective.

If $z \in \operatorname{dom}\tau_x = Sx^{-1}$, then $z\tau_x\tau_{x^{-1}}\tau_x = zxx^{-1}x = zx = z\tau_x$. If $z \in \operatorname{dom}\tau_{x^{-1}} = Sx$, then $z\tau_{x^{-1}}\tau_x\tau_{x^{-1}} = zx^{-1}xx^{-1} = zx^{-1} = z\tau_{x^{-1}}$. Furthermore, $\operatorname{dom}\tau_{x^{-1}} = Sx = \operatorname{im}\tau_x$ and $\operatorname{im}\tau_{x^{-1}} = Sx^{-1} = \operatorname{dom}\tau_x$. Hence $(\tau_x)^{-1} = \tau_{x^{-1}}$.

Let $x, y \in S$. Then

$$\begin{aligned} \operatorname{dom}(\tau_x\tau_y) &= \operatorname{dom}\tau_x \cap (\operatorname{dom}\tau_y)\tau_x^{-1} \\ &= (\operatorname{im}\tau_x \cap \operatorname{dom}\tau_y)\tau_x^{-1} \\ &= (Sx^{-1}x \cap Sy^{-1})\tau_x^{-1} && \text{[by definition of } \tau_x \text{ and } \tau_y\text{]} \\ &= (Sx^{-1}x \cap Syy^{-1})\tau_x^{-1} && \text{[by Lemma 5.3(c)]} \\ &= (Sx^{-1}xyy^{-1})\tau_x^{-1} && \text{[by Lemma 5.3(b)]} \\ &= (Sx^{-1}xyy^{-1})\tau_{x^{-1}} && \text{[since } \tau_x^{-1} = \tau_{x^{-1}}\text{]} \\ &= Sx^{-1}xyy^{-1}x^{-1} && \text{[by definition of } \tau_{x^{-1}}\text{]} \\ &= Sxx^{-1}xyy^{-1}x^{-1} && \text{[by Lemma 5.3(c)]} \\ &= Sxyy^{-1}x^{-1}xx^{-1} && \text{[since idempotents commute]} \\ &= Sxyy^{-1}x^{-1} \\ &= S(xy)(xy)^{-1} \\ &= S(xy)^{-1} && \text{[by Lemma 5.3(c)]} \\ &= \operatorname{dom}\tau_{xy}, && \text{[by definition of } \tau_{x^{-1}}\text{]} \end{aligned}$$

and for all $z \in \operatorname{dom} \tau_{xy}$, we have $z\tau_x\tau_y = zxy = z\tau_{xy}$. Hence $(x\varphi)(y\varphi) = \tau_x\tau_y = \tau_{xy} = (xy\varphi)$. Hence φ is a monomorphism. 5.5

Notice that the image of S in $\mathcal{I}_X$ is an *inverse* subsemigroup of $\mathcal{I}_X$. However, some subsemigroups of $\mathcal{I}_X$ are not inverse; see Exercise 5.1.

THE NATURAL PARTIAL ORDER

Elements of $\mathcal{I}_X$ are maps, and thus relations, and thus simply subsets of $X \times X$. Thus we can apply the partial order $\subseteq$ to $\mathcal{I}_X$. However, $\subseteq$ can be characterized using the algebraic structure of $\mathcal{I}_X$, since

$$\begin{aligned} \sigma \subseteq \tau &\Leftrightarrow \sigma = \tau|_{\operatorname{dom}\sigma} \\ &\Leftrightarrow \sigma = \mathrm{id}_{\operatorname{dom}\sigma}\,\tau \\ &\Leftrightarrow \sigma = \sigma\sigma^{-1}\tau. \end{aligned}$$

Since every inverse monoid embeds into $\mathcal{I}_X$ for some X by Theorem 5.5, we can transfer this algebraic definition to arbitrary inverse semigroups by defining $x \preceq y \Leftrightarrow x = xx^{-1}y$.

LEMMA 5.6.

For $x, y \in S$, the following are equivalent:

a) $x \preceq y$;

b) $x = ey$ *for some* $e \in E(S)$;

c) $x = yf$ *for some* $f \in E(S)$;

d) $x = yx^{-1}x$.

Proof of 5.6. First part [a) $\Rightarrow$ b)]. Suppose $x \preceq y$. Then $x = xx^{-1}y$, and $e = xx^{-1}$ is an idempotent.

Second part [b) $\Rightarrow$ c)]. Suppose $x = ey$. Let $f = y^{-1}ey$. Then $f^2 = y^{-1}eyy^{-1}ey = y^{-1}yy^{-1}e^2y = y^{-1}ey = f$; thus f is idempotent. Furthermore, $yf = yy^{-1}ey = eyy^{-1}y = ey = x$.

Third part [c) $\Rightarrow$ d)]. Suppose $x = yf$. Then $xf = xf^2 = xf = x$ and so $x^{-1}xf = x^{-1}x$ Hence $yx^{-1}x = yx^{-1}xf = yfx^{-1}x = xx^{-1}x = x$.

Fourth part [d) $\Rightarrow$ a)]. Suppose $x = yx^{-1}x$. Then $x = yy^{-1}yx^{-1}x = yx^{-1}xy^{-1}y$. Let $e = yx^{-1}xy^{-1}$. Then $e^2 = yx^{-1}xy^{-1}yx^{-1}xy^{-1} = yx^{-1}xx^{-1}xy^{-1}yy^{-1} = yx^{-1}xy^{-1} = e$, so e is idempotent. Furthermore, $ex = e^2y = ey = x$, so $exx^{-1} = xx^{-1}$. Hence $xx^-y = exx^{-1}y = xx^{-1}ey = xx^{-1}x = x$ and so $x \preceq y$ 5.6

PROPOSITION 5.7. *The relation $\preceq$ is a partial order.*

Proof of 5.7. Since $x = xx^{-1}x$, we have $x \leq x$ for any $x \in S$ thus x is reflexive. If $x \leq y$ and $y \leq x$, then by $x = xx^{-1}y$ and $y = yy^{-1}x$. Hence $x = xx^{-1}yy^{-1}x = yy^{-1}xx^{-1}x = yy^{-1}x = y$; thus $\leq$ is anti-symmetric. If $x \leq y$ and $y \leq z$, then $x = ey$ and $y = fz$ for some $e, f \in E(S)$, whence $x = (ef)z$ and so $x \leq z$ since ef is in the subsemigroup $E(S)$; thus $\leq$ is transitive. 5.7

Proposition 5.7 justifies the choice of the symbol $\leq$. Notice that if x and y are idempotents, then by the commutativity of idempotents this agrees with the definition of the natural partial order for idempotents (see Proposition 1.16). We are therefore justified in using the same symbol $\leq$ for both relations.

PROPOSITION 5.8. *Let S be an inverse semigroup. For all $x \in S$ and $e \in E(S)$, we have $x \leq e \Rightarrow x \in E(S)$.*

Proof of 5.8. For $x \in S$ and $e \in E(S)$,

$$\begin{aligned}
x \leq e &\Rightarrow x = xx^{-1}e && \text{[by definition of } \leq\text{]}\\
&\Rightarrow x^2 = xx^{-1}exx^{-1}e\\
&\Rightarrow x^2 = xx^{-1}xx^{-1}ee && \text{[since idempotents commute in } S\text{]}\\
&\Rightarrow x^2 = xx^{-1}e && \text{[since } xx^{-1} \text{ and } e \text{ are idempotents]}\\
&\Rightarrow x^2 = x && \text{[since } x = xx^{-1}e\text{]}\\
&\Rightarrow x \in E(S). && 5.8
\end{aligned}$$

PROPOSITION 5.9. a) *The relation $\leq$ is compatible (with multiplication); that is, $x \leq y \wedge z \leq t \Rightarrow xz \leq yt$ for all $x, y, z, t \in S$.*

b) *The relation $\leq$ is compatible with inversion; that is, $x \leq y \Rightarrow x^{-1} \leq y^{-1}$ for all $x, y \in S$.*

Proof of 5.9. a) Let $x, y, z, t \in S$. Then

$$\begin{aligned}
&x \leq y \wedge z \leq t\\
&\Rightarrow (\exists e, f \in E(S))(x = ey \wedge z = tf) && \text{[by Lemma 5.6]}\\
&\Rightarrow (\exists e, f \in E(S))(xz = eyz \wedge yz = ytf)\\
&\Rightarrow (\exists e, f \in E(S))(xz \leq yz \wedge yz \leq yt) && \text{[by Lemma 5.6]}\\
&\Rightarrow (\exists e, f \in E(S))(xz \leq yt). && \text{[since } \leq \text{ is transitive]}
\end{aligned}$$

b) Let $x, y \in S$. Then

$$\begin{aligned}
&x \leq y\\
&\Rightarrow (\exists e \in E(S))(x = ey) && \text{[by Lemma 5.6]}\\
&\Rightarrow (\exists e \in E(S))(x^{-1} = y^{-1}e)\\
&\Rightarrow (\exists e \in E(S))(x^{-1} = y^{-1}yy^{-1}e)\\
&\Rightarrow (\exists e \in E(S))(x^{-1} = y^{-1}eyy^{-1})
\end{aligned}$$

$\Rightarrow (\exists f \in E(S))(x^{-1} = fy^{-1})$ [since $y^{-1}ey \in E(S)$ by Lemma 5.3(d)]
$\Rightarrow x^{-1} \le y^{-1}$. [by Lemma 5.6]

5.9

The natural partial order is a measure of how close an inverse semigroup is to being a group:

PROPOSITION 5.10. *Let S be an inverse semigroup. Then S is a group if and only if $\le$ is the equality relation on S.*

Proof of 5.10. Suppose S is a group. Then

$$x \le y \Leftrightarrow x = xx^{-1}y \Leftrightarrow x = 1_S y \Leftrightarrow x = y;$$

thus $\le$ is the equality relation.

Now suppose that $\le$ is the equality relation. Let $e, f \in E(S)$. Then $ef \le e$ and $ef \le f$; hence $e = ef = f$. Thus S contains a unique idempotent and so S is a group by Proposition 5.2. 5.10

CLIFFORD SEMIGROUPS

Recall that a semigroup S is a *Clifford semigroup* if it satisfies the conditions in (4.5). Thus S is a Clifford semigroup if it is completely regular and for all $x, y \in S$

$$xx^{-1}yy^{-1} = yy^{-1}xx^{-1}. \tag{5.5}$$

We are going to prove a structure theorem for Clifford semigroups, but first we need to strengthen the notion of a semilattice of semigroups, which we introduced in the previous chapter. When we know that S is a semilattice of semigroups S_α, we know something of the coarse structure of S: we know that if $x \in S_\alpha$ and $y \in S_\beta$, then $xy \in S_{\alpha\wedge\beta}$; see Figure 4.2.

One way to strengthen this notion is as follows. Suppose that we have a semilattice Y, disjoint semigroups S_α for each $\alpha \in Y$, and, for all $\alpha \ge \beta$, homomorphisms $\varphi_{\alpha,\beta} : S_\alpha \to S_\beta$ satisfying the conditions

$$(\forall \alpha \in Y)(\varphi_{\alpha,\alpha} = \mathrm{id}_\alpha) \tag{5.6}$$
$$(\forall \alpha, \beta, \gamma \in Y)\big((\alpha \ge \beta \ge \gamma) \Rightarrow (\varphi_{\alpha,\beta}\varphi_{\beta,\gamma} = \varphi_{\alpha,\gamma})\big) \tag{5.7}$$

Then we can define a multiplication on $S = \bigcup_{\alpha\in Y} S_\alpha$ as follows: for each $x \in S_\alpha$ and $y \in S_\beta$, the product xy is defined to be $(x\varphi_{\alpha,\alpha\wedge\beta})(y\varphi_{\beta,\alpha\wedge\beta})$. That is, we use the homomorphisms to map x and y 'down' into $S_{\alpha\wedge\beta}$ and multiply them there; see Figure 5.2. For any $x \in S_\alpha$, $y \in S_\beta$, $z \in S_\gamma$,

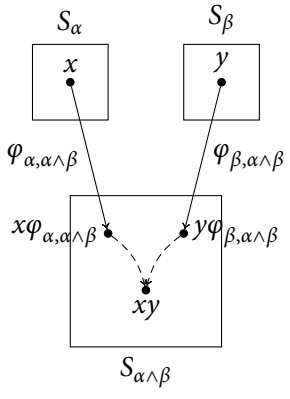


FIGURE 5.2
Multiplying in a strong semilattice of semigroups

$$
\begin{aligned}
& x(yz) \\
&= x\big((y\varphi_{\beta,\beta\wedge\gamma})(z\varphi_{\gamma,\beta\wedge\gamma})\big) && \text{[by definition of multiplication]} \\
&= (x\varphi_{\alpha,\alpha\wedge\beta\wedge\gamma})\big((y\varphi_{\beta,\beta\wedge\gamma})(z\varphi_{\gamma,\beta\wedge\gamma})\big)\varphi_{\beta\wedge\gamma,\alpha\wedge\beta\wedge\gamma} \\
& && \text{[by definition of multiplication]} \\
&= (x\varphi_{\alpha,\alpha\wedge\beta\wedge\gamma})(y\varphi_{\beta,\beta\wedge\gamma}\varphi_{\beta\wedge\gamma,\alpha\wedge\beta\wedge\gamma})(z\varphi_{\gamma,\beta\wedge\gamma}\varphi_{\beta\wedge\gamma,\alpha\wedge\beta\wedge\gamma}) \\
& && \text{[since } \varphi_{\beta\wedge\gamma,\alpha\wedge\beta\wedge\gamma} \text{ is a homomorphism]} \\
&= (x\varphi_{\alpha,\alpha\wedge\beta\wedge\gamma})\big((y\varphi_{\beta,\alpha\wedge\beta\wedge\gamma})(z\varphi_{\gamma,\alpha\wedge\beta\wedge\gamma})\big) && \text{[by (5.7)]} \\
&= \big((x\varphi_{\alpha,\alpha\wedge\beta\wedge\gamma})(y\varphi_{\beta,\alpha\wedge\beta\wedge\gamma})\big)(z\varphi_{\gamma,\alpha\wedge\beta\wedge\gamma}) && \text{[by associativity in } S_{\alpha\wedge\beta\wedge\gamma}] \\
&= (xy)z, && \text{[by similar reasoning]}
\end{aligned}
$$

and so this multiplication is associative. This semigroup S is a *strong semilattice of semigroups* and is denoted $\mathcal{S}[Y; S_\alpha; \varphi_{\alpha,\beta}]$. If every S_α is a group, it is a *strong semilattice of groups*.

THEOREM 5.11. *The following are equivalent:*

a) *S is a Clifford semigroup;*

b) *S is a semilattice of groups;*

c) *S is a strong semilattice of groups;*

d) *S is regular, and the idempotents of S are central;*

e) *S is regular, and every $\mathcal{D}$-class of S contains a unique idempotent.*

Proof of 5.11. First part [a) $\Rightarrow$ b)]. Let S be a Clifford semigroup. Then S is completely regular and so is a semilattice of completely simple semigroups S_α by Theorem 4.15. Let e, f be idempotents. Then $e = ee^{-1}$ and $f = ff^{-1}$ and so $ef = fe$ by (5.5). So all idempotents of S commute. Now, S_α is completely simple and so $S_\alpha \simeq \mathcal{M}[G; I, \Lambda; P]$ for some group G, index sets I and Λ, and matrix P over G. Let $e, f \in S_\alpha$ be idempontents. Then $e = (i, p_{\lambda i}^{-1}, \lambda)$ and $f = (j, p_{\mu j}^{-1}, \mu)$, and $(i, p_{\lambda i}^{-1} p_{\lambda j} p_{\mu j}^{-1}, \mu) = ef = fe = (j, p_{\mu j}^{-1} p_{\mu i} p_{\lambda i}^{-1}, \lambda)$. Hence $i = j$ and $\lambda = \mu$ and so $e = f$. Since there is at least one idempotent in every $\mathcal{R}$-class and every $\mathcal{L}$-class, it follows that there can be only one $\mathcal{R}$-class and one $\mathcal{L}$-class in S_α. So S_α is a group by Exercise 4.2(a). Therefore S is a semilattice of groups.

Second part [b) $\Rightarrow$ c)]. Let S be a semilattices of groups S_α, where $\alpha \in Y$. Write 1_α for the identity of the group S_α. Then if $\alpha \geq \beta$, for any $x \in S_\alpha$, we have $1_\beta x \in S_\beta$. Hence we can define $\varphi_{\alpha,\beta} : S_\alpha \to S_\beta$ by $x\varphi_{\alpha,\beta} = 1_\beta x$. Clearly $\varphi_{\alpha,\alpha} = \mathrm{id}_{S_\alpha}$, so (5.6) holds. Furthermore, for $x, y \in S_\alpha$,

$$
\begin{aligned}
(x\varphi_{\alpha,\beta})(y\varphi_{\alpha,\beta}) &= 1_\beta x 1_\beta y && \text{[by definition of } \varphi_{\alpha,\beta}] \\
&= 1_\beta xy && \text{[since } 1_\beta x \in S_\beta \text{ and thus } (1_\beta x)1_\beta = 1_\beta x] \\
&= (xy)\varphi_{\alpha,\beta}; && \text{[by definition of } \varphi_{\alpha,\beta}]
\end{aligned}
$$

hence $\varphi_{\alpha,\beta}$ is a homomorphism. Finally, for $\alpha \geq \beta \geq \gamma$, for any $x \in S_\alpha$

$$\begin{aligned}
& x\varphi_{\alpha,\beta}\varphi_{\beta,\gamma} \\
&= (1_\beta x)\varphi_{\beta,\gamma} && \text{[by definition of } \varphi_{\alpha,\beta}\text{]} \\
&= 1_\gamma 1_\beta x && \text{[by definition of } \varphi_{\beta,\gamma}\text{]} \\
&= (1_\beta \varphi_{\beta,\gamma})x && \text{[by definition of } \varphi_{\beta,\gamma}\text{]} \\
&= 1_\gamma x && \text{[since } \varphi_{\beta,\gamma} \text{ is a (group) homomorphism]} \\
&= x\varphi_{\alpha,\gamma}; && \text{[by definition of } \varphi_{\alpha,\gamma}\text{]}
\end{aligned}$$

hence (5.7) holds. Finally, for any $x \in S_\alpha$ and $y \in S_\beta$,

$$\begin{aligned}
xy &= 1_{\alpha\wedge\beta}xy && \text{[since } xy \in S_{\alpha\wedge\beta}\text{]} \\
&= 1_{\alpha\wedge\beta}x1_{\alpha\wedge\beta}y && \text{[since } 1_{\alpha\wedge\beta}x \in S_{\alpha\wedge\beta}\text{]} \\
&= (x\varphi_{\alpha,\alpha\wedge\beta})(y\varphi_{\beta,\alpha\wedge\beta}). && \text{[by definition of } \varphi_{\alpha,\alpha\wedge\beta} \text{ and } \varphi_{\alpha,\alpha\wedge\beta}\text{]}
\end{aligned}$$

Therefore S is isomorphic to $\mathcal{S}[Y; S_\alpha; \varphi_{\alpha,\beta}]$.

Third part [c) ⇒ d)]. A strong semilattice of groups $S = \mathcal{S}[Y; S_\alpha; \varphi_{\alpha,\beta}]$ is certainly regular: for each $x \in S_\alpha$, let x^{-1} be the inverse of x in the group S_α. The idempotents of S are the identities of the groups S_α. Write 1_α for the identity of S_α. Then for any $x \in S_\beta$,

$$\begin{aligned}
1_\alpha x = (1_\alpha \varphi_{\alpha,\alpha\wedge\beta})(x\varphi_{\beta,\alpha\wedge\beta}) &= 1_{\alpha\wedge\beta}(x\varphi_{\beta,\alpha\wedge\beta}) \\
= (x\varphi_{\beta,\alpha\wedge\beta}) = (x\varphi_{\beta,\alpha\wedge\beta})1_{\alpha\wedge\beta} &= (x\varphi_{\beta,\alpha\wedge\beta})(1_\alpha\varphi_{\alpha,\alpha\wedge\beta}) = x1_\alpha.
\end{aligned}$$

Thus every idempotent of S is central.

Fourth part [d) ⇒ e)] Each $\mathcal{D}$-class D_x contains at least one idempotent, namely xx^{-1}. Suppose e and f are idempotent and $e\,\mathcal{D}\,f$. Then by Proposition 3.19(b) there exists an element x and inverse x' such that $xx' = e$ and $x'x = f$. Therefore

$$\begin{aligned}
e &= e^2 \\
&= xx'xx' && \text{[since } xx' = e\text{]} \\
&= xfx' && \text{[since } x'x = f\text{]} \\
&= xx'f && \text{[since } f \text{ is central]} \\
&= xx'x'x && \text{[since } f = x'x\text{]} \\
&= ex'x && \text{[since } xx' = e\text{]} \\
&= x'ex && \text{[since } e \text{ is central]} \\
&= x'xx'x && \text{[since } e = xx'\text{]} \\
&= f^2 = f. && \text{[since } f = x'x\text{]}
\end{aligned}$$

Hence every $\mathcal{D}$-class of D contains a unique idempotent.

Fifth part [e) ⇒ a)]. Since every $\mathcal{D}$-class contains a single idempotent, every $\mathcal{D}$-class is a group and so $\mathcal{D} = \mathcal{H}$. So every element of S lies in a subgroup and so S is completely regular by Proposition 4.13. Thus by Theorem 4.15 is a semilattice of completely simple semigroups S_α. Every element of a completely simple semigroup is $\mathcal{D}$-related, and so every S_α is contained within a single $\mathcal{D}$-class and is thus a group. So S is a semilattice of groups $\mathcal{S}[Y; S_\alpha; \varphi_{\alpha,\beta}]$. Hence for $x \in S_\alpha$ and $y \in S_\beta$, we have $xx^{-1}yy^{-1} = 1_\alpha 1_\beta = 1_{\alpha\wedge\beta} = 1_\beta 1_\alpha = yy^{-1}xx^{-1}$. 5.11

In particular, Theorem 5.11(d) implies that in a Clifford semigroup, idempotents commute; hence, by Theorem 5.1, Clifford semigroups are inverse semigroups. Notice that this is not obvious from the conditions (4.5) and (4.4).

Let S be a Clifford semigroup. By Theorem 5.11, S is isomorphic to a strong semilattice of groups $\mathcal{S}[Y; G_\alpha; \varphi_{\alpha,\beta}]$. Let $x \in G_\alpha$ and $y \in G_\beta$. Then

$$\begin{aligned} x \le y &\Leftrightarrow x = (xx^{-1})y \\ &\Leftrightarrow x = 1_\alpha y \\ &\Leftrightarrow x = (1_\alpha \varphi_{\alpha,\alpha\wedge\beta})(y\varphi_{\beta,\alpha\wedge\beta}) \\ &\Leftrightarrow x = (1_\alpha \varphi_{\alpha,\alpha})(y\varphi_{\beta,\alpha}) \wedge (\alpha \wedge \beta = \beta) \\ &\Leftrightarrow x = y\varphi_{\beta,\alpha\wedge\beta} \wedge (\alpha \le \beta). \end{aligned}$$

Thus the natural partial order $\le$ precisely corresponds to the homomorphisms $\varphi_{\alpha,\beta}$ and the order of the semilattice $(Y, \le)$. In particular, we have

$$1_\alpha \le 1_\beta \Leftrightarrow 1_\alpha = 1_\beta \varphi_{\beta,\alpha} \wedge (\alpha \le \beta) \Leftrightarrow \alpha \le \beta.$$

Since the identities of the groups G_α are precisely the idempotents of S, we see that $(E(S), \le)$ and $(Y, \le)$ are isomorphic.

In particular, every semilattice $(Y, \le)$ is a Clifford semigroup $\mathcal{S}[Y; G_\alpha, \varphi_{\alpha,\beta}]$ where the groups G_α are all trivial.

BRUCK–REILLY EXTENSIONS

Bruck–Reilly extensions

Let M be a monoid presented by $\langle A \mid \rho\rangle$. Let $\varphi : M \to M$ be an endomorphism. The *Bruck–Reilly extension of M with respect to φ*, denoted $\mathrm{BR}(M, \varphi)$, is the monoid presented by

$$\langle A \cup \{b, c\} \mid \rho \cup \{(bc, \varepsilon), (ba, (a\varphi)b), (ac, c(a\varphi)) : a \in A\}\rangle, \qquad (5.8)$$

where the we view $a\varphi$ in the defining relations as some word in A^* representing that element of M.

Characterizing words equal in $\mathrm{BR}(M,\varphi)$

PROPOSITION 5.12. *Every element of $BR(M,\varphi)$ is represented by a word of the form $c^\gamma w b^\beta$, where $\gamma,\beta \in \mathbb{N}\cup\{0\}$ and $w \in A^*$. Furthermore, $c^\gamma w b^\beta$ and $c^{\gamma'} w' b^{\beta'}$ represent the same element of $BR(M,\varphi)$ if and only if $\gamma=\gamma'$, $\beta=\beta'$, and $w =_M w'$.*

Proof of 5.12. Since $\mathrm{BR}(M,\varphi)$ is generated by $A\cup\{b,c\}$, every element is represented by some word $u \in (A\cup\{b,c\})^*$. Using the defining relations (bc,ε), we can delete any subword bc. Then, using defining relations of the form $(ba,(a\varphi)b)$, we can replace any subword ba by $(a\varphi)b$ and any subword ac by $c(a\varphi)$. Iterating this process, we eventually find a word v containing no subwords bc, ba or ac: that is, $v = c^\gamma w b^\beta$ for some $\gamma,\beta \in \mathbb{N}\cup\{0\}$ and $w \in A^*$.

For the second part, suppose that $\gamma=\gamma'$, $\beta=\beta'$, and $w =_M w'$. Then there is a sequence of elementary ρ-transitions from w to w'. Since ρ is a subset of the defining relations in (5.8), w and w' represent the same element of $\mathrm{BR}(M,\varphi)$. Hence $c^\gamma w b^\beta$ and $c^\gamma w' b^\beta$ represent the same element of $\mathrm{BR}(M,\varphi)$.

For the converse, we will represent $\mathrm{BR}(M,\varphi)$ as a transformation semigroup. Let

$$X = (\mathbb{N}\cup\{0\}) \times M \times (\mathbb{N}\cup\{0\}) = \{(\gamma,w,\beta) : \gamma,\beta \in \mathbb{N}\cup\{0\}, w \in M\}.$$

Define

$$\begin{aligned}
(\gamma,w,\beta)\tau_a &= (\gamma, w(a\varphi^\beta), \beta) && \text{for each } a \in A\\
(\gamma,w,\beta)\tau_b &= (\gamma, w, \beta+1)\\
(\gamma,w,\beta)\tau_c &= \begin{cases} (\gamma+1, w\varphi, 0) & \text{if } \beta = 0\\ (\gamma, w, \beta-1) & \text{if } \beta > 0.\end{cases}
\end{aligned}$$

Let $\psi : \mathrm{BR}(M,\varphi) \to \mathcal{T}_X$ be the homomorphism extending $x \mapsto \tau_x$ for all $x \in A\cup\{b,c\}$. It is easy to prove that for all defining relations (u,v) in (5.8), we have $u\psi = v\psi$ and so ψ is well-defined.

Suppose now that $c^\gamma w b^\beta$ and $c^{\gamma'} w' b^{\beta'}$ represent the same element of $\mathrm{BR}(M,\varphi)$. Then $(c^\gamma w b^\beta)\psi = (c^{\gamma'} w' b^{\beta'})\psi$. Thus

$$(\gamma,w,\beta) = (0,1_M,0)\big((c^\gamma w b^\beta)\psi\big) = (0,1_M,0)\big((c^{\gamma'} w' b^{\beta'})\psi\big) = (\gamma,w',\beta),$$

and so $\gamma=\gamma'$ and $\beta=\beta'$. 5.12

Notice that if M is the trivial monoid and $\varphi : M \to M$ the identity map, then $\mathrm{BR}(M,\varphi)$ is the bicyclic monoid.

$\mathrm{BR}(M,\varphi)$ is independent of $\langle A \mid \rho\rangle$

In the proof of Proposition 5.12, the map ψ is an isomorphism between $\mathrm{BR}(M,\varphi)$ and a submonoid $\operatorname{im}\psi$ of $\mathcal{T}_X$. Since this submonoid does not depend on the presentation $\langle A \mid \rho\rangle$ for M, we see that the definition of $\mathrm{BR}(M,\varphi)$ is independent of the choice of presentation for M.

PROPOSITION 5.13. *Let G be a group and let $\varphi : G \to G$ be an endomorphism. Then $BR(G, \varphi)$ is an inverse semigroup.*

Bruck–Reilly presentation of a group is inverse

Proof of 5.13. Let $S = \mathrm{BR}(G, \varphi)$ and let $x = c^\gamma w b^\beta \in S$ (where $w \in G$) be arbitrary. Let $y = c^\beta w^{-1} b^\gamma$. Then

$$xyx = c^\gamma w b^\beta c^\beta w^{-1} b^\gamma c^\gamma w b^\beta =_S c^\gamma w w^{-1} w b^\beta = c^\gamma w b^\beta = x.$$

So x is regular. Since $x \in S$ was arbitrary, we see that S is regular. The idempotents of S are elements of the form $c^\gamma b^\gamma$ by Exercise 5.7(c). Thus, given two idempotents $e = c^\gamma b^\gamma$ and $f = c^\beta b^\beta$, we see that if $\gamma \geq \beta$,

$$ef = c^\gamma b^\gamma c^\beta b^\beta =_S c^\gamma b^{\gamma-\beta} b^\beta =_S c^\gamma c^\gamma =_S c^\beta c^{\gamma-\beta} b^\gamma =_S c^\beta b^\beta c^\gamma b^\gamma = fe$$

and similarly $ef = fe$ if $\gamma \leq \beta$. So S is a regular semigroup whose idempotents commute and so is inverse by Theorem 5.1. 5.13

Therefore, in particular, the bicyclic monoid is an inverse monoid.

PROPOSITION 5.14. *Let M be a monoid and let $\varphi : M \to M$ be defined by $x\varphi = 1$ for all $x \in M$. Then $BR(M, \varphi)$ is simple.*

Proof of 5.14. Let $S = \mathrm{BR}(M, \varphi)$. We aim to show that $SxS = S$ for all $x \in S$. Suppose $x = c^\gamma w b^\beta$, where $w \in M$. Let $c^\delta u b^\zeta$ be an arbitrary element of S. Let $p = c^\delta u b^{\gamma+1}$ and $q = c^{\beta+1} b^\zeta$. Then

$$\begin{aligned} pxq &= c^\delta u b^{\gamma+1} c^\gamma w b^\beta c^{\beta+1} b^\zeta \\ &=_S c^\delta u b w c b^\zeta \\ &=_S c^\delta u b c (w\varphi) b^\zeta \\ &=_S c^\delta u b c b^\zeta \\ &=_S c^\delta u b^\zeta. \end{aligned}$$

So $c^\delta u b^\zeta = pxq \in SxS$. Since $c^\delta u b^\zeta \in S$ was arbitrary, $S = SxS$. Hence any ideal of S must be S itself. So S is simple. 5.14

Notice that $\mathrm{BR}(M, \varphi)$ contains an isomorphic copy of M: these elements are represented by words over A; that is, by words of the form $c^0 w b^0$. Thus M embeds into $\mathrm{BR}(M, \varphi)$. So Proposition 5.14 has the following consequence:

COROLLARY 5.15. *Every semigroup embeds into a simple monoid.*

Embedding monoids in simple monoids

EXERCISES

[See pages 157–159 for the solutions.]

∗5.1 Let $X = \{1, 2\}$. Find a subsemigroup of $\mathcal{I}_X$ that contains only two elements and which is not an inverse subsemigroup.

∗5.2 Let S be an inverse semigroup, T a semigroup (not necessarily inverse), and let $\varphi : S \to T$ be a homomorphism. Prove that $\operatorname{im}\varphi$ is an inverse semigroup, and that φ is an inverse semigroup homomorphism, in the sense that $x^{-1}\varphi = (x\varphi)^{-1}$.

5.3 Prove that a Clifford semigroup is an inverse semigroup.

5.4 A semigroup is *orthodox* if it is regular and its set of idempotents form a subsemigroup.

a) Prove that a Clifford semigroup is orthodox.

b) Prove that a semigroup is completely simple and orthodox if and only if it is isomorphic to the direct product of a rectangular band and a group.

∗5.5 Prove that a completely 0-simple semigroup is inverse if and only if it is isomorphic to $\mathcal{M}_0[G; I, I; P]$ where P is a diagonal $I \times I$ matrix.

Partial right translation

∗5.6 Let S be a cancellative semigroup. Then for each $x \in S$, the map $\rho_x : S^1 \to S^1$ (where $t\rho_x = tx$) is injective and so lies in $\mathcal{I}_{S^1}$. An element τ of $\mathcal{I}_{S^1}$ is a *partial right translation* if $\operatorname{dom}\tau$ is a left ideal of S^1 and for any $x \in \operatorname{dom}\tau$ and $y \in S^1$, we have $(yx)\tau = y(x\tau)$.

a) Prove that if $\tau \in \mathcal{I}_{S^1}$ is a partial right translation, then $\operatorname{im}\tau$ is a left ideal of S^1.

b) Let $\varphi : S \to \mathcal{I}_S$ be the homomorphism defined by $x \mapsto \rho_x$. Let T be the inverse subsemigroup of $\mathcal{I}_{S^1}$ generated by $\operatorname{im}\varphi$. Prove that the set of partial right translations in $\mathcal{I}_{S^1}$ is an inverse subsemigroup of of $\mathcal{I}_{S^1}$ and contains T.

5.7 Let G be a group and $\varphi : G \to G$ an endomorphism. Let $S = \mathrm{BR}(G, \varphi)$.

a) Prove that in S, we have

$$c^\gamma w b^\beta \mathrel{\mathcal{R}} c^\delta u b^\zeta \Leftrightarrow \gamma = \delta;$$
$$c^\gamma w b^\beta \mathrel{\mathcal{L}} c^\delta u b^\zeta \Leftrightarrow \beta = \zeta;$$

and deduce that

$$c^\gamma w b^\beta \mathrel{\mathcal{H}} c^\delta u b^\zeta \Leftrightarrow \gamma = \delta \wedge \beta = \zeta.$$

b) Prove that in S, we have $\mathcal{D} = \mathcal{J} = S \times S$.

c) Prove that the idempotents of S are elements of the form $c^\gamma b^\gamma$.

NOTES

The Vagner–Preston representation theorem (Theorem 5.5) and much of the basic theory of inverse semigroups, is found in Vagner, 'Generalized groups' and Preston, 'Inverse semi-groups with minimal right ideals'; Preston, 'Representations of inverse semi-groups'. The structure theorem for Clifford semigroups is due to Clifford, 'Semigroups admitting relative inverses', though the terminology is later.

Commutative semigroups

6

❁ Abelian groups (that is, commutative groups) have a simpler structure and are better understood than general groups. It is therefore unsurprising that commutative semigroups are also relatively well-understood. However, in commutative semigroups the Green's relations $\mathcal{H}$, $\mathcal{L}$, $\mathcal{R}$, $\mathcal{D}$, and $\mathcal{J}$ all coincide, and are therefore less useful than usual. Thus we use different tools. As we shall see, commutative semigroups admit a decomposition into 'archimedean components'; finitely generated commutative semigroups are finitely presented by Rédei's theorem (Theorem 6.6); and commutative cancellative semigroups are group-embeddable (Proposition 6.7).

ARCHIMEDEAN DECOMPOSITION

Define a binary relation $\sqsubseteq$ on S by $x \sqsubseteq y \Leftrightarrow J_x \leq J_y$. Equivalently, $x \sqsubseteq y \Leftrightarrow R_x \leq R_y$, and so $x \sqsubseteq y \Leftrightarrow (\exists q \in S^1)(x = yq)$ for some $q \in S^1$. So $x \sqsubseteq y$ if and only if y is a factor of x. Notice that $xy \sqsubseteq x$ for all $x, y \in S$. Furthermore, $x \sqsubseteq y$ implies $zx \sqsubseteq zy$; hence, by commutativity, $\sqsubseteq$ is both left and right compatible.

Let S be a semigroup and let

$$\nu = \{(x^2, x), (xy, yx) : x, y \in X\}.$$

Let $\mathcal{N} = \nu^\#$. For any $[x]_\mathcal{N}, [y]_\mathcal{N} \in S/\mathcal{N}$,

$$[x]_\mathcal{N}[x]_\mathcal{N} = [x^2]_\mathcal{N} = [x]_\mathcal{N} \text{ and } [x]_\mathcal{N}[y]_\mathcal{N} = [xy]_\mathcal{N} = [yx]_\mathcal{N} = [y]_\mathcal{N}[x]_\mathcal{N}$$

since $(x^2, x), (xy, yx) \in \nu \subseteq \mathcal{N}$. So $S/\mathcal{N}$ is a commutative semigroup of idempotents and therefore a semilattice by Theorem 1.18. Indeed, if σ is a congruence on S such that S/σ is a semilattice, then $\nu \subseteq \sigma$. So $\mathcal{N}$ is the smallest congruence on S such that $S/\mathcal{N}$ is a semilattice.

Furthermore, notice that the $\mathcal{N}$-classes are subsemigroups of S, since if $x \mathcal{N} y$ implies $xy \mathcal{N} x^2 \mathcal{N} x$.

We can define a relation $\leq_\mathcal{N}$ on S by $x \leq_\mathcal{N} y \Leftrightarrow [x]_\mathcal{N} \leq [y]_\mathcal{N}$, where $\leq$ is the partial order on $S/\mathcal{N}$. The relation $\leq_\mathcal{N}$ is a quasi-order but is not in general a partial order. Note that $x \mathcal{N} y \Leftrightarrow x \leq_\mathcal{N} y \wedge y \leq_\mathcal{N} x$. When S is commutative, $\leq_\mathcal{N}$ admits the following elegant description:

PROPOSITION 6.1. *Let S be a commutative semigroup. Then:*

a) $x \leq_{\mathcal{N}} y \Leftrightarrow (\exists k \in \mathbb{N})(x^k \sqsubseteq y)$;
b) $x \mathcal{N} y \Leftrightarrow (\exists k, \ell \in \mathbb{N})(x^k \sqsubseteq y \wedge y^m \sqsubseteq x)$.

Proof of 6.1. Define a binary relation σ on S by $x \sigma y \Leftrightarrow (\exists k, \ell \in \mathbb{N})(x^k \sqsubseteq y \wedge y^m \sqsubseteq x)$

First,

$$\begin{aligned} x^k \sqsubseteq y &\Rightarrow [x^k]_{\mathcal{N}} \leq [y]_{\mathcal{N}} \\ &\Rightarrow [x]_{\mathcal{N}} \leq [y]_{\mathcal{N}} && \text{[since } (x^2, x) \in \mathcal{N}\text{]} \\ &\Rightarrow x \leq_{\mathcal{N}} y; \end{aligned}$$

this proves the reverse implication of part a). Furthermore,

$$x^k \sqsubseteq y \wedge y^k \sqsubseteq x \Rightarrow x \leq_{\mathcal{N}} y \wedge y \leq_{\mathcal{N}} x \Rightarrow x \mathcal{N} y$$

and so $\sigma \subseteq \mathcal{N}$. On the other hand, it is easy to see that σ is an equivalence relation; since $\sqsubseteq$ is left and right compatible, so is σ. So σ is a congruence. Furthermore, $x^2 \ \sigma \ x$ for all $x \in S$. Therefore, since S is commutative, S/σ is a congruence. Since $\mathcal{N}$ is the smallest congruence on S such that the corresponding factor semigroup is a congruence, $\mathcal{N} \subseteq \sigma$. Hence $\mathcal{N} = \sigma$. This proves part b).

Finally,

$$\begin{aligned} x \leq_{\mathcal{N}} y &\Rightarrow [x]_{\mathcal{N}} \leq [y]_{\mathcal{N}} \\ &\Rightarrow [x]_{\mathcal{N}} = [x]_{\mathcal{N}}[y]_{\mathcal{N}} && \text{[by Theorem 1.18]} \\ &\Rightarrow [x]_{\mathcal{N}} = [xy]_{\mathcal{N}} \\ &\Rightarrow x \ \sigma \ xy && \text{[since } \sigma = \mathcal{N}\text{]} \\ &\Rightarrow x^k \ \sigma \ xy && \text{[since } x^k \ \sigma \ x\text{]} \\ &\Rightarrow x^k \sqsubseteq xy && \text{[by definition of } \sigma\text{]} \\ &\Rightarrow x^k \sqsubseteq y. && \text{[since } xy \subseteq y\text{]} \end{aligned}$$

This proves the forward implication of part a). 6.1

Archimedean semigroups

Let S be a semigroup. Then S is *archimedean* if S is commutative and for all $x, y \in S$ there exists $k \in \mathbb{N}$ such that $x^k \sqsubseteq y$. As an immediate consequence of Proposition 6.1, we have the following result:

THEOREM 6.2. *Every commutative semigroup is a semilattice of archimedean semigroups.* 6.2

As a consequence of Theorem 6.2, a full understanding of the structure of commutative semigroups relies on an understanding of archimedean semigroups and a knowledge of how to reconstruct a semigroup from the semilattice and the various archimedean semigroups. Both of these problems are difficult, although a full structure theorem for archimedean semigroups is known. We limit ourselves to the easy case of the structure of archimedean semigroups that contain an idempotent:

PROPOSITION 6.3. *Let S be a semigroup. Then S archimedean if and only if either*

a) *S is a group, or*

b) *S is an ideal extension of a group by a nilsemigroup.*

Proof of 6.3. Let S be archimedean and let $e \in S$ be idempotent. Then for any $x \in S$, we have $e^k \sqsubseteq x$ for some $k \in \mathbb{N}$; since $e = e^k$, we have $e \sqsubseteq x$. Hence $e \sqsubseteq ex \sqsubseteq e$ and so $ex \mathcal{H} e$. Therefore $eS = H_e$. Thus (by commutativity), H_e is an ideal of S. If $S = H_e$, the proof is complete since a) holds. Otherwise, since S is archimedean, for any $x \in S$, there exists $k \in \mathbb{N}$ such that $x^k \sqsubseteq e$; hence $x^k \mathcal{H} e$ and $x^k \in H_e$. Hence every element of the factor semigroup S/H_e has a power equal to $0_{S/H_e}$; hence S/H_e is a nilsemigroup and b) holds. 6.3

COROLLARY 6.4. *An archimedean semigroup contains at most one idempotent.* 6.4

RÉDEI'S THEOREM

Let F_n be the free commutative monoid of rank n; thus $F_n = \prod_{i=1}^{n} \mathbb{N} \cup \{0\}$. Define a partial order $\leq$ on F_n as follows: on F_n by

$$(x_1, \ldots, x_n) \leq (y_1, \ldots, y_n) \Leftrightarrow (\forall i \in \{1, \ldots, n\})(x_i \leq y_i).$$

Notice that there are no infinite $\leq$-descreasing sequences in F_n.

THEOREM 6.5. *Every antichain in F_n is finite.* Dickson's theorem

Proof of 6.5. Let $Y \subseteq F_n$ be an antichain. The proof is by induction on n. If $n = 1$, then Y is a subset of $F_1 = \mathbb{N} \cup \{0\}$. Since $\leq$ is a total order on $\mathbb{N} \cup \{0\}$, every pair of elements is comparable and thus Y contains at most one element.

Now suppose the result holds for all $k < n$. For each $t \in \mathbb{N} \cup \{0\}$, the set

$$\{(x_1, \ldots, x_{n-1}) : (x_1, \ldots, x_{n-1}, t) \in Y\} \tag{6.1}$$

is an anti-chain of F_{n-1} and therefore finite. Fix some $y \in Y$. Let $x \in Y - \{y\}$. Since Y is an antichain, it is impossible that $y_i \leq x_i$ for all $i \in \{1, \ldots, n\}$; thus $x_i < y_i$ for some $i \in \{1, \ldots, n\}$. Hence

$$\begin{aligned} Y &= \{y\} \cup \bigcup_{i=1}^{n} \{x \in Y : x_i < y_i\} \\ &= \{y\} \cup \bigcup_{i=1}^{n} \bigcup_{j=0}^{y_i - 1} \{x \in Y : x_i = j\}. \end{aligned}$$

Each set in this union is of the form (6.1) and thus finite; hence Y itself is finite. This proves the induction step. 6.5

Rédei's theorem

THEOREM 6.6. *Every finitely generated commutative semigroup is finitely presented.*

Proof of 6.6. Let σ be a congruence on F_n. Define the lexicographic order $\preceq$ on F_n by

$$(x_1,\dots,x_n) \prec (y_1,\dots,y_n) \Leftrightarrow (\exists k \in \{1,\dots,n\})\big(x_k < y_k \wedge (\forall j < k)(x_j = y_k)\big).$$

Then $\preceq$ is a total order on F_n and is compatible: $x \preceq y$ implies $xz \preceq yz$ for all $z \in F_n$. Furthermore, $\preceq$ is a well-order (that is, every non-empty subset of F_n has a $\preceq$-minimum element). In particular, every σ-class $[x]_\sigma$ has a $\preceq$-minimum element q_x. Let

$$Q = \{q_x : x \in F_n\} = \{y \in F_n : (\forall x \in F_n)(y\ \sigma\ x \Rightarrow y \preceq x)\}.$$

Let P be the complement of Q in F_n; that is,

$$P = \{x : q_x \prec x\} = \{x \in F_n : (\exists y \in F_n)(y\ \sigma\ x \wedge y \prec x\}.$$

Then P consists of the non-$\preceq$-minimal elements of all the σ-classes and

$$x \in P \Rightarrow q_x \prec x \Rightarrow q_x z \prec xz \Rightarrow xz \in P;$$

hence P is an ideal of F_n. Let M be the set of $\preceq$-minimal elements of P. Then M is an antichain and so finite by Theorem 6.5. Let $\rho = \{(q_m, m) : m \in M\}$; since M is finite, so is ρ.

The aim is now to show that $\rho^\# = \sigma$. Since $q_m\ \sigma\ m$ for each $m \in M$, it is immediate that $\rho \subseteq \sigma$ and so $\rho^\# \subseteq \sigma$.

To establish the opposite inclusion, the first step is to prove that $q_x\ \rho^\#\ x$ for all $x \in F_n$. Suppose, with the aim of obtaining a contradiction, that $(q_x, x) \notin \rho^\#$ for some $x \in F_n$. Then, since $\preceq$ is a well-order, there is a $\preceq$-minimum such $s \in F_n$ with $(q_s, s) \notin \rho^\#$. By definition of ρ, the element s cannot be in Q (since otherwise $q_s = s$ and so $(q_s, s) \in \rho^\#$) and cannot be in M (since otherwise $(q_s, s) \in \rho \subseteq \rho^\#$). Hence $s \in P$ and $s > m$ for some $m \in M$. Thus $s = mt$ for some $t \in F_n$. Let $u = q_m t$. Since $(q_m, m) \in \rho^\#$ and $(q_m, m) \in \sigma$, multiply by t to see that $(u, s) \in \rho^\#$ and $(u, s) \in \sigma$. Notice that $(u, s) \in \sigma$ implies $q_u = q_s$. Since $q_m \prec m$ and $\prec$ is compatible, $u \prec s$. Since s is $\prec$-minimum with $(q_s, s) \notin \rho^\#$, it follows that $(q_u, u) \in \rho^\#$. Hence $s\ \rho^\#\ u\ \rho^\#\ q_x = q_s$. Thus, $(q_s, s) \in \rho^\#$, which is a contradiction. Therefore $q_x\ \rho^\#\ x$ for all $x \in F_n$.

Finally, let $(x, y) \in \sigma$. Then $q_x = q_y$. By the previous paragraph, (q_x, x) and (q_y, y) are in $\rho^\#$. Thus $x\ \rho^\#\ q_x = q_y\ \rho^\#\ y$; hence $(x, y) \in \rho^\#$. That is, $\sigma \subseteq \rho^\#$, and therefore $\sigma = \rho^\#$. 6.6

CANCELLATIVE COMMUTATIVE SEMIGROUPS

We can prove that commutative cancellative semigroups are group-embeddable using an construction similar to that used to embed an integral domain in a field:

PROPOSITION 6.7. *Every cancellative commutative semigroup is group-embeddable.*

Proof of 6.7. Let S be a commutative cancellative semigroup. Define a relation σ on $S \times S$ by $(x,y)\ \sigma\ (z,t) \Leftrightarrow xt = zy$. It is easy to see that σ is an equivalence relation, and

$$\begin{aligned}
&(x,y)\ \sigma\ (z,t) \wedge (x',y')\ \sigma\ (z',t') \\
&\Rightarrow xt = zy \wedge x't' = z'y' \\
&\Rightarrow xtx't' = zyz'y' \\
&\Rightarrow xx'tt' = zz'yy' && \text{[since } S \text{ is commutative]} \\
&\Rightarrow (xx',yy')\ \sigma\ (zz',tt').
\end{aligned}$$

Thus σ is a congruence. Let $G = (S \times S)/\sigma$.

Fix some element $z \in S$. We will show that $[(z,z)]_\sigma$ is an identity for G. Let $[(x,y)]_\sigma \in G$; then $(zx)y = (zy)x$ since S is commutative. Hence $(zx,zy) \sim (x,y)$ and so $[(z,z)]_\sigma[(x,y)]_\sigma = [(zx,zy)]_\sigma = [(x,y)]_\sigma$ and similarly $[(x,y)]_\sigma[(z,z)]_\sigma = [(x,y)]_\sigma$. So G is a monoid with identity $[(z,z)]_\sigma$.

Furthermore, $(xy)z = z(yx)$, since S is commutative and so $(xy,yx) \sim (z,z)$. Hence $[(x,y)]_\sigma[(y,x)]_\sigma = [(xy,yx)]_\sigma = [(z,z)]_\sigma$ and similarly $[(y,x)]_\sigma[(x,y)]_\sigma = [(z,z)]_\sigma$. Thus $[(y,x)]_\sigma$ is a left and right inverse for $[(x,y)]_\sigma$. So G is a group.

Finally, let $\varphi : S \to G$ be defined by $s\varphi = [(sz,z)]_\sigma$; then φ is injective since

$$\begin{aligned}
&s\varphi = t\varphi \\
&\Rightarrow [(sz,z)]_\sigma = [(tz,z)]_\sigma \\
&\Rightarrow (sz,z)\ \sigma\ (tz,z) \\
&\Rightarrow sz^2 = tz^2 \\
&\Rightarrow s = t.
\end{aligned}$$

Therefore S is group-embeddable. 6.7

Proposition 6.7 is actually a special case of Ore's theorem, which we shall state shortly after some necessary definitions.

Right- and left-reversibility

A semigroup S is *right-reversible* if any two principal left ideals of S intersect; that is, if $Sx \cap Sy \neq \varnothing$ for any $x, y \in S$, or, equivalently, if every two elements of S have a common left multiple. Similarly, S is *left-reversible*

if any two principal right ideals of S intersect; that is, if $xS \cap yS \neq \varnothing$ for any $x, y \in S$, or, equivalently, if every two elements of S have a common right multiple. Notice that any commutative semigroup is right- and left-reversible, for any two elements x and y have common left and right multiple $xy = yx$.

Ore's theorem

THEOREM 6.8. *Every cancellative right-reversible semigroup is group-embeddable.*

Proof of 6.8. [See Exercise 6.2.] 6.8

EXERCISES

[See pages 159–161 for the solutions.]

✶6.1 Let S be commutative, let I be an ideal of S, and let G be an abelian group. Let $\varphi : I \to G$ be a homomorphism. Prove that there is a unique extension of φ to a homomorphism $\hat{\varphi} : S \to G$.

6.2 Let S be a cancellative right-reversible semigroup. Let $\varphi : S \to \mathcal{I}_S$ be the homomorphism defined by $x \mapsto \rho_x$. Let T be the inverse subsemigroup of $\mathcal{I}_S$ generated by $\operatorname{im}\varphi$. By Exercise 5.6(b), every element of T is a partial right translation. Define a relation $\sim$ on T by

$$\alpha \sim \beta \Leftrightarrow (\exists \delta \in T)\big((\delta \subseteq \alpha) \wedge (\delta \subseteq \beta)\big)$$

for all $\alpha, \beta \in T$. Notice that

$$\delta \subseteq \alpha \Leftrightarrow \big((\operatorname{dom}\delta \subseteq \operatorname{dom}\alpha) \wedge (\forall x \in \operatorname{dom}\delta)(x\delta = x\alpha)\big).$$

a) Prove that $\sim$ is an congruence.

b) Let $G = T/\sim$. Prove that G is a group.

c) Let $\alpha, \beta \in T$. Prove that $\alpha \circ \beta$ is not the empty relation, and so deduce that T does not contain the empty relation.

d) Let $\psi = \varphi\circ\, \sim^\natural$ (that is, $x\psi = [x\varphi]_\sim$). Prove that ψ is a monomorphism and so deduce that S is group-embeddable.

✶6.3 Let $S = (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\})$ and define a multiplication on S by

$$(m, n)(p, q) = (m + p, 2^p n + q)$$

Check that this multiplication is associative, so that S is a semigroup. Prove that S is left reversible but not right reversible.

NOTES

The decomposition of a commuative semigroup as a semilattice of archimedean semigroups is due to Tamura & Kimura, 'On decompositions of a commutative semigroup'. Rédei's theorem (Theorem 6.6) was first proved by Rédei, *Theorie der Endlich Erzeugbaren Kommutativen Halbgruppen*; the proof given here is from Grillet, 'A short proof of Rédei's theorem'. Ore's theorem (Theorem 6.8) is contained in a theorem about rings proved, using different terminology, in Ore, 'Linear equations in non-commutative fields'; the proof in Exercise 6.2 is due to Rees, 'On the group of a set of partial transformations'.

Finite semigroups

7

In this chapter, we begin the study of finite semigroups. Although Green's relations will play a role, other techniques are used to understand finite semigroups. In particular we will introduce the notion of divisibility, where one semigroup is a homomorphic image of a subsemigroup of another. The goal is to prove the Krohn–Rhodes theorem, which says that all finite semigroups divide a wreath product of finite groups and finite aperiodic semigroups, which, as we shall see, are finite semigroups where all subgroups are trivial.

GREEN'S RELATIONS

As a consequence of Proposition 3.2, we know that $\mathcal{D}$ and $\mathcal{J}$ coincide for finite semigroups.

PROPOSITION 7.1. *Let M be a finite monoid with identity 1. Then $H_1 = L_1 = R_1 = D_1 = J_1$. Furthermore, $M - H_1$ is an ideal of M.*

Proof of 7.1. Let $x \in R_1$. Then there exists $y \in M^1 = M$ such that $xy = 1$. Suppose, with the aim of obtaining a contradiction, that $yx \neq 1$. We will obtain a contradiction by showing that x is not periodic. To prove this, suppose that $x^{m+k} = x^m$ for some $m, k \in \mathbb{N}$. Then $x^k = x^{m+k}y^m = x^m y^m = 1$, and so $y = 1y = x^k y = x^{k-1}$ and $yx = x^k = 1$. This contradicts $yx \neq 1$, and so proves that x is not periodic; that is, all powers of x are distinct. This contradicts the fact that M is finite, and so proves that $yx = 1$. Hence $x \mathcal{H} 1$. Therefore $R_1 \subseteq H_1$. The opposite inclusion is obvious, so $R_1 = H_1$. Similarly $L_1 = H_1$. So D_1 contains only one $\mathcal{L}$-class and only one $\mathcal{R}$-class and so $D_1 = H_1$. Finally, $J_1 = H_1$ since $\mathcal{D} = \mathcal{J}$. 7.1

PROPOSITION 7.2. *Let S and S' be finite semigroups and let $\varphi : S \to S'$ be an epimorphism. Let G' be a maximal subgroup of S'. Then there is a maximal subgroup G of S such that $G\varphi = G'$.*

Proof of 7.2. Let G' be a maximal subgroup of S'. Then $T = G'\varphi^{-1}$ is a subsemigroup of S and $T\varphi = G'$. Since T is finite, it has a kernel; let $K = K(S)$, which is a simple ideal of T. Since φ is surjective, $K\varphi$ is an ideal of the group G' and so $K\varphi = G'$. Since K is finite it is also completely simple by a result analogous to Proposition 4.1. So, by Theorem

4.11, $K \simeq \mathcal{M}[G; I, \Lambda; P]$ for some group G, index sets I and Λ, and matrix P over G. View $\varphi|_K$ as an epimorphism from $\mathcal{M}[G; I, \Lambda; P]$ to G'. For each $i \in I$ and $\lambda \in \Lambda$, let $G_{i\lambda}$ be the subset $\{i\} \times G \times \{\lambda\}$ of $\mathcal{M}[G; I, \Lambda; P]$. Then $\mathcal{M}[G; I, \Lambda; P]$ is the union of the various $G_{i\lambda}$, and $G_{i\lambda}G_{j\mu} \subseteq G_{i\mu}$. In particular, every $G_{i\lambda}$ is a subgroup of G.

Let $G'_{i\lambda} = G_{i\lambda}\varphi$. Then each $G'_{i\lambda}$ is a subgroup of G, and $G'_{i\lambda}G'_{j\mu} \subseteq G'_{i\mu}$. In particular, $G'_{i\lambda}G'_{j\lambda} \subseteq G'_{i\lambda}$, which implies $G'_{j\lambda} = 1_{G'}G'_{j\lambda} \subseteq G'_{i\lambda}$. Similarly $G'_{i\lambda} \subseteq G'_{i\mu}$. Thus all the $G'_{i\lambda}$ are equal. Since φ is surjective, G' is the union of the $G'_{i\lambda}$ and thus equal to any one of the $G'_{i\lambda}$. Hence $G' = G_{i\lambda}\varphi$ for any $i \in I$ and $\lambda \in \Lambda$. 7.2

PROPOSITION 7.3. *Let S be a finite semigroup and let $x, y \in S$. If $x \mathcal{H} y$, then $y \in xG$ for some subgroup G of S.*

Proof of 7.3. Let H be an $\mathcal{H}$-class of S. Apply Proposition 7.2 to the natural epimorphism $\sigma_H^\natural : \mathrm{Stab}(H) \to \Gamma(H)$ to see that $H = G\sigma_H^\natural$ for some subgroup G of $\mathrm{Stab}(H)$. By Proposition 3.22, we see that $y \in x \cdot \Gamma(H) = xG$ for all $x, y \in H$. 7.3

Aperiodic semigroups

A semigroup S is *aperiodic* if for every $x \in S$, there exists $n \in \mathbb{N}$ such that $x^n = x^{n+1}$.

Notice that aperiodic semigroup are actually periodic. For example, any semigroup of idempotents, such as a semilattice or right zero semigroup, satisfies $x = x^2$ and so is aperiodic.

PROPOSITION 7.4. *Let S be a finite semigroup. The following are equivalent:*

a) $\mathcal{H} = \mathrm{id}_S$;

b) *all subgroups of S are trivial;*

c) *S is aperiodic.*

Proof of 7.4. First part [a) ⇒ b)]. Suppose $\mathcal{H} = \mathrm{id}_S$. By Proposition 3.13, maximal subgroups of S are $\mathcal{H}$-classes. So all subgroups of S are trivial.

Second part [b) ⇒ a)]. Suppose that all subgroups of S are trivial. Let H be an $\mathcal{H}$-class of S. Then $\Gamma(H)$, which is a homomorphic image of a subgroup of $\mathrm{Stab}(H)$, is trivial. Since $|H| = |\Gamma(H)|$, it follows that H is trivial by Proposition 7.3. Hence $\mathcal{H} = \mathrm{id}_S$.

Third part [b) ⇒ c)]. Suppose that all subgroups of S are trivial. Let $x \in S$. Since S is finite, $x^m = x^{m+k}$ for some $m, k \in \mathbb{N}$. The set of elements $\{x^m, x^{m+1}, \ldots, x^{m+k-1}\}$ is a subgroup and so is trivial, which implies $k = 1$. Hence $x^m = x^{m+1}$. Thus S is aperiodic.

Fourth part [c) ⇒ b)]. Suppose S is aperiodic. Let G be a subgroup of S and let $x \in G$. Then $x^m = x^{m+1}$ for some $m \in \mathbb{N}$. Hence $x = 1_G$ by cancellativity in G. So G is trivial. Thus all subgroups of S are trivial. 7.4

SEMIDIRECT AND WREATH PRODUCTS

Semidirect product

Let S and T be semigroups and let T act on S from the left by endomorphisms; let $\varphi : T \to \mathrm{End}(S)$ be the anti-homomorphism corresponding to this left action. To avoid having to write extra brackets, we will write ${}^{t}s$ instead of $t \cdot s$. The *semidirect product of S and T with respect to φ* is denoted $S \rtimes_\varphi T$ and is the cartesian product $S \times T$ with multiplication defined by

$$(s_1, t_1)(s_2, t_2) = (s_1 {}^{t_1}s_2, t_1 t_2). \tag{7.1}$$

This multiplication is associative (see Exercise 7.5) and so $S \rtimes_\varphi T$ is a semigroup. Notice that $S \rtimes_\varphi T$ has cardinality $|S||T|$.

Notice that for any semigroups S and T, we can take the trivial left action, where $t \cdot s = {}^{t}s = s$ for $t \in T$ and $s \in S$; this corresponds to the trivial anti-homomorphism $\varphi : T \to \mathrm{End}(S)$ $y\varphi = \mathrm{id}_S$ for all $y \in T$. In this case, $(s_1, t_1)(s_2, t_2) = (s_1 s_2, t_1 t_2)$. Thus the direct product is a special case of the semidirect product.

Wreath product

Define a left action of T on S^T by letting $y \cdot f = {}^{y}f$ be such that $(x)\,{}^{y}f = (xy)f$. This satisfies the definition of a left action since

$$(x)\big(z \cdot (y \cdot f)\big) = (x)\,{}^{z}({}^{y}f) = (xz)\,{}^{y}f = (xzy)f = (x)\,{}^{zy}f = zy \cdot f.$$

Let φ be the anti-homomorphism corresponding to this action. The *wreath product of S and T*, denoted $S \wr T$, is the semidirect product $S^T \rtimes_\varphi T$. Thus the product in $S \wr T$ is

$$(f_1, t_1)(f_2, t_2) = (f_1 {}^{t_2}f_2, t_1 t_2).$$

Since this multiplication is derived from the multiplication in direct and semidirect products, we know it is associative. Hence $S \wr T$ is a semigroup. Notice that $S \wr T$ has cardinality $|S|^{|T|}|T|$.

Let S, T, U be finite semigroups. Then

$$\big|(S \wr T) \wr U\big| = |S \wr T|^{|U|}|U| = \big(|S|^{|T|}|T|\big)^{|U|}|U| = |S|^{|T||U|}|T|^{|U|}|U|$$

and

$$\big|S \wr (T \wr U)\big| = |S|^{|T \wr U|}|T \wr U| = |S|^{|T|^{|U|}|U|}|T|^{|U|}|U|.$$

Therefore the wreath product, as an operation on semigroups, is not associative.

DIVISION

Division

A semigroup S *divides* a semigroup T, denoted $S \prec T$, if S is a homomorphic image of a subsemigroup of T. Notice that divisibility is a reflexive relation.

PROPOSITION 7.5. *The divisibility relation $\prec$ is transitive.*

Proof of 7.5. Let S, T, U be semigroups with $S \prec T$ and $T \prec U$. Then there are subsemigroups T' of T and U' of U and epimorphisms $\varphi : T' \to S$ and $\psi : U' \to T$. Let $U'' = T'\psi^{-1}$. Since T' is a subsemigroup of T, it follows that U'' is a subsemigroup of U' and thus of U. Furthermore, $\psi|_{U''} \circ \varphi : U'' \to S$ is an epimorphism. So $S \prec U$. 7.5

The relation of divisibility is closely related to the connection between finite automata and semigroups, which we will look at in Chapter 9.

PROPOSITION 7.6. *Let S and T be semigroups. Then S, T, and $S \times T$ divide $S \wr T$.*

Proof of 7.6. Since S and T are homomorphic images of $S \times T$ under the projection maps $\pi_S : S \times T \to S$ and $\pi_T : S \times T \to T$, we have $S \prec S \times T$ and $T \prec S \times T$. Since $\prec$ is transitive (by Proposition 7.5), it suffices to prove that $S \times T \prec S \wr T$.

For each $s \in T$, let $f_s \in S^T$ have all components equal to s. Define a map $\psi : S \times T \to S \wr T$ by $(s,t)\psi = (f_s, t)$. Then

$$\begin{aligned}
&\big((s,t)\psi\big)\big((s',t')\psi\big)\psi \\
&= (f_s, t)(f_{s'}, t') \\
&= (f_s\, {}^t f_{s'}, tt') \\
&= (f_{ss'}, tt') \qquad [\text{since } (x)(f_s\, {}^t f_{s'}) = (x)f_s(xt')f_{s'} = ss' = (x)f_{ss'}] \\
&= (ss', tt')\psi \\
&= \big((s,t)(s',t')\big)\psi.
\end{aligned}$$

So ψ is a homomorphism. Furthermore,

$$(s,t)\psi = (s',t')\psi \Rightarrow (f_s, t) = (f_{s'}, t') \Rightarrow s = s' \wedge t = t' \Rightarrow (s,t) = (s',t');$$

thus ψ is injective. Thus $\psi : S \times T \to \operatorname{im}\psi \subseteq S \wr T$ is an isomorphism, and so ψ^{-1} is an epimorphism from the subsemigroup $\operatorname{im}\psi$ of $S \wr T$ onto the subsemigroup $S \times T$. So $S \times T \prec S \wr T$. 7.6

PROPOSITION 7.7. *Let M be a monoid and let E be an ideal extension of M by T. Then $E \prec T \wr M$.*

Proof of 7.7. By Proposition 1.31, E is a subdirect product of T and M. That is, E is a subsemigroup of $T \times M$ and hence E divides $T \times M$. The result follows from Propositions 7.6 and 7.5. 7.7

PROPOSITION 7.8. *If $S' \prec S$ and $T' \prec T$, then $S' \wr T' \prec S \wr T$.*

Proof of 7.8. The strategy is to prove this in two cases: when S' and T' are subsemigroups of S and T, and when S' and T' are homomorphic images of S and T. The general result follows immediately.

a) Suppose S' and T' are subsemigroups of S and T. Let

$$U = \{(f,t) \in S \wr T : T'f \subseteq S' \wedge t \in T'\}.$$

If $(f_1,t_1),(f_2,t_2) \in U$, then $(f_1,t_1)(f_2,t_2) = (f_1\,{}^{t_1}f_2, t_1t_2)$. Now, $t_1t_2 \in T'$ since T' is a subsemigroup of T. Furthermore, for $x \in T'$, we have $(x)(f_1\,{}^{t_1}f_2) = ((x)f_1)((xt_1)f_2) \in (T'f)(T'f) \subseteq S'$ since S' is a subsemigroup of S. So U is a subsemigroup of $S \wr T$.

Define $\varphi : U \to S' \wr T'$ by $(f,t)\varphi = (f|_{T'}, t)$. Then φ is a surjective homomorphism and so $S' \wr T' \prec S \wr T$.

b) Suppose $\varphi : S \to S'$ and $\psi : T \to T'$ are epimorphisms. Let

$$U = \{(f,t) \in S \wr T : \ker\psi \subseteq \ker(f\varphi)\}.$$

Suppose $(f_1,t_1),(f_2,t_2) \in U$. Let $x,y \in T$ with $x\psi = y\psi$. Then $(x)f_2\varphi = (y)f_2\varphi$ since $\ker\psi \subseteq \ker(f_2\varphi)$. Furthermore, $(xt_1)\psi = (x\psi)(t_1\psi) = (y\psi)(t_1\psi) = (yt_1)\psi$ and so $(xt_1)f_2\varphi = (yt_2)f_2\varphi$ since $\ker\psi \subseteq \ker(f_2\varphi)$. Hence

$$(x)f_1f_2^{t_1}\varphi = (x)f_1\varphi(xt_1)f_2\varphi = (y)f_1\varphi(yt_1)f_2\varphi = (y)f_1\,{}^{t_1}f_2\varphi.$$

Thus $\ker\psi \subseteq \ker f_1\,{}^{t_1}f_2\varphi$, and so $(f_1,t_1),(f_2,t_2) = (f_1f_2^{t_1}, t_1t_2) \in U$. So U is a subsemigroup of $S \wr T$.

For any map $f : T \to S$ such that $\ker\psi \subseteq \ker(f\varphi)$, there is a unique map $f' : T' \to S'$ such that $\psi f' = f\varphi$. Define $\vartheta : U \to S' \wr T'$ by $(f,t)\vartheta = (f', t\psi)$. Notice that since ψ is surjective, for any map $f' \in S'^{T'}$ there is a map $f \in S^T$ with $\psi f' = f\varphi$; hence ϑ is surjective. Let $(f_1,t_1),(f_2,t_2) \in U$, then $(f_1,t_1)(f_2,t_2) = (f_1\,{}^{t_1}f_2, t_1t_2)$. Further, $(f_1,t_1)\vartheta(f_2,t_2)\vartheta = (f_1',t_1\psi)(f_2',t_2\psi) = (f_1'\,{}^{t_1\psi}f_2', (t_1t_2)\psi)$. Now

$$\begin{aligned}
& y\psi f_1'\,{}^{t_1\psi}f_2' \\
&= (y\psi)f_1'((y\psi)(t_1\psi))f_2' && \text{[by definition of the product and action]} \\
&= (y\psi)f_1'(yt_1)\psi f_2' && \text{[since } \psi \text{ is a homomorphism]} \\
&= (y)f_1\varphi(yt_1)f_2\varphi && \text{[by definition of } f_1' \text{ and } f_2'\text{]} \\
&= \big((y)f_1(yt_1)f_2\big)\varphi && \text{[since } \varphi \text{ is a homomorphism]} \\
&= \big((y)f_1f_2^{t_1}\big)\varphi, && \text{[by definition of the product and action]}
\end{aligned}$$

and so

$$(f_1f_2^{t_1}, t_1t_2)\vartheta = (f_1'\,{}^{t_1\psi}f_2', (t_1t_2)\psi). \tag{7.2}$$

Hence

$$\begin{aligned}
& \big((f_1,t_1)(f_2,t_2)\big)\vartheta \\
&= (f_1f_2^{t_1}, t_1t_2)\vartheta && \text{[multiplication in } S \wr T\text{]} \\
&= (f_1'\,{}^{t_1\psi}f_2', (t_1t_2)\psi) && \text{[by (7.2)]}
\end{aligned}$$

$$= (f_1', t_1\psi)(f_2', t_2\psi) \qquad \text{[factoring in } S' \wr T'\text{]}$$
$$= (f_1, t_1)\vartheta(f_2, t_2)\vartheta;$$

therefore ϑ is a homomorphism and so an epimorphism. Hence $S' \wr T' \prec S \wr T$. 7.8

Constant extension

Let S be a semigroup. Let S' be a set in bijection with S under $x \mapsto x'$. Define a multiplication on $S \cup S'$ as follows: multiplication in S is as before (so that S is a subsemigroup of $S \cup S'$), and for all $x, y \in S$,

$$xy' = x'y' = y', \qquad x'y = (xy)'. \tag{7.3}$$

It is easy but tedious to prove that this multiplication is associative; the set $S \cup S'$ is thus a semigroup, called the *constant extension* of S and denoted $C(S)$.

PROPOSITION 7.9. *If $S \prec T$, then $C(S) \prec C(T)$.*

Proof of 7.9. If S is a subsemigroup of T, then $C(S)$ is a subsemigroup of $C(T)$.

Suppose S is a homomorphic image of T. Then there exists some epimorphism $\varphi : T \to S$. Define $\hat{\varphi} : C(T) \to C(S)$ by $x\hat{\varphi} = x\varphi$ and $x'\hat{\varphi} = (x\varphi)'$. Then $\hat{\varphi}$ is an epimorphism, and so $C(S)$ is a homomorphic image of $C(T)$.

Hence $S \prec T$ implies $C(S) \prec C(T)$. 7.9

PROPOSITION 7.10. *Let M be a monoid and S a semigroup. Then $C(S \wr M) \prec C(S)^M \wr C(M)$.*

Proof of 7.10. Define a map $\psi : S \wr M \to C(S)^M \wr C(M)$ by

$$\begin{aligned}
(f, m)\psi &= (f_{\text{ext}}, m), && \text{where } (y)f_{\text{ext}} \in C(S)^M \text{ is defined by} \\
& && (x)[(y)f_{\text{ext}}] = (xy)f \text{ for all } y \in C(M); \\
(f, m)'\psi &= (f_{\text{con}}, m'), && \text{where } (y)f_{\text{con}} \in C(S)^M \text{ is defined by} \\
& && (x)[(y)f_{\text{con}}] = ((x)f)' \text{ for all } y \in C(M).
\end{aligned}$$

Notice that $(x)[(y)f_{\text{con}}]$ does not depend on y. Hence f_{con} is a constant map from $C(M)$ to $C(S)^M$.

The maps f_{ext} and f_{con} are maps from $C(M)$ to $C(S)^M$. That is, $(y)f_{\text{ext}}$ and $(y)f_{\text{con}}$ are maps from M to $C(S)$. Notice that although f_{con} is a constant map from $C(M)$ to $C(S)^M$, the maps $(y)f_{\text{con}}$ are *not* constant.

We are going to prove that ψ is a monomorphism. Let us first prove that ψ is injective. To begin, observe that $(f, m)\psi = (g, n)'\psi$ implies $(f_{\text{ext}}, m) = (h_{\text{con}}, n')$, which can never happen since $m \in M$ and $n' \in M'$. Thus to prove that ψ is injective ψ is injective, we only have to check that no two distinct elements of $S \wr M$ are mapped to the same element and that no two distinct elements $(S \wr M)'$ are mapped to the same element:

a) Suppose $(f,m)\psi = (g,m)\psi$. Then $f_{\mathrm{ext}} = g_{\mathrm{ext}}$ and $m = n$, and hence $(y)f_{\mathrm{ext}} = (y)f_{\mathrm{ext}}$ for all $y \in M$, or, equivalently, $(xy)f = (xy)g$ for all $x, y \in M$. In particular, putting $x = 1$ shows that $(y)f = (y)g$ for all $y \in M$ and so $f = g$; hence $(f,m) = (g,m)$.

b) Suppose $(f,m)'\psi = (g,n)'\psi$. Then $(f_{\mathrm{con}}, m') = (g_{\mathrm{con}}, n')$ and so $f_{\mathrm{con}} = g_{\mathrm{con}}$ and $m' = n'$. Hence $((x)f)' = (x)[(y)f_{\mathrm{con}}] = (x)[(y)g_{\mathrm{con}}] = ((x)g)'$, and so $(x)f = (x)g$ for all $x \in M$. Hence $f = g$ and so $(f,m)' = (g,n)'$.

Therefore ψ is injective.

Next, we have to prove that ψ is injective. There are four cases to consider, where we form a product of two elements of $S \wr M$ or $(S \wr M)'$. We explain one case in full here and outline the others; the details are left to Exercise 7.10.

a) Let $(f,m), (g,n) \in S \wr M$. We first have to prove:

$$(f^m g)_{\mathrm{ext}} = f_{\mathrm{ext}}\, {}^m g_{\mathrm{ext}}. \tag{7.4}$$

Since both sides of (7.4) are maps from $C(M)$ to $C(S)^M$, we must prove that $(y)(fg^m)_{\mathrm{ext}} = (y)f_{\mathrm{ext}}\, {}^m g_{\mathrm{ext}}$ for all $y \in C(M)$; since both sides of this equality are maps from M to $C(S)$, we must prove that $(x)[(y)(f^m g)_{\mathrm{ext}}] = (x)[(y)f_{\mathrm{ext}}\, {}^m g_{\mathrm{ext}}]$ for all $x \in M$ and $y \in C(M)$. We proceed as follows:

$$\begin{aligned}
&(x)[(y)(f^m g)_{\mathrm{ext}}] \\
&= (xy)f^m g && \text{[by definition of } {}_{\mathrm{ext}}\text{]} \\
&= (xy)f(xym)g && \text{[by definition of the product and action]} \\
&= (x)[(y)f_{\mathrm{ext}}](x)[(y)\,{}^m g_{\mathrm{ext}}] && \text{[by definition of } {}_{\mathrm{ext}}\text{]} \\
&= (x)[(y)f_{\mathrm{ext}}(y)\,{}^m g_{\mathrm{ext}}], && \text{[by multiplication in } C(S)^M\text{]} \\
&= (x)[(y)f_{\mathrm{ext}}\, {}^m g_{\mathrm{ext}}]; && \text{[by multiplication in } (C(S)^M)^{C(M)}\text{]}
\end{aligned}$$

this proves (7.4). Now we have:

$$\begin{aligned}
\big((f,m)(g,n)\big)\psi &= (f^m g, mn)\psi \\
&= ((f^m g)_{\mathrm{ext}}, mn) \\
&= (f_{\mathrm{ext}}\, {}^m g_{\mathrm{ext}}, mn) && \text{[by (7.4)]} \\
&= (f_{\mathrm{ext}}, m)(g_{\mathrm{ext}}, n) \\
&= (f,m)\psi(g,n)\psi.
\end{aligned}$$

b) Let $(f,m)' \in (S \wr M)'$ and $(g,n) \in S \wr M$. By Exercise 7.10,

$$(f^m g)_{\mathrm{con}} = f_{\mathrm{con}}\, {}^{m'} g_{\mathrm{ext}}. \tag{7.5}$$

Now we have:

$$\begin{aligned}
\big((f,m)'(g,n)\big)\psi &= (f^m g, mn)'\psi \\
&= ((f^m g)_{\mathrm{con}}, (mn)')
\end{aligned}$$

$$
\begin{aligned}
&= (f_{\mathrm{con}}\ {}^{m'}g_{\mathrm{ext}}, m'n) && \text{[by (7.4)]}\\
&= (f_{\mathrm{con}}, m')(g', n)\\
&= (f, m)'\psi(g, n)\psi.
\end{aligned}
$$

c) Let $(f, m) \in S \wr M$ and $(g, n)' \in (S \wr M)'$. By Exercise 7.10,

$$g_{\mathrm{con}} = f_{\mathrm{ext}}\ {}^{m}g_{\mathrm{con}}. \tag{7.6}$$

Now we have:

$$
\begin{aligned}
\big((f, m)(g, n)'\big)\psi &= (g, n)'\psi\\
&= (g_{\mathrm{con}}, n')\\
&= (f_{\mathrm{ext}}\ {}^{m}g_{\mathrm{con}}, mn') && \text{[by (7.6)]}\\
&= (f_{\mathrm{ext}}, m)(g_{\mathrm{con}}, n')\\
&= (f, m)\psi(g, n)'\psi.
\end{aligned}
$$

d) Let $(f, m)', (g, n)' \in (S \wr M)'$. By Exercise 7.10,

$$g_{\mathrm{con}} = f_{\mathrm{con}}\ {}^{m}g_{\mathrm{con}}. \tag{7.7}$$

Now we have:

$$
\begin{aligned}
\big((f, m)'(g, n)'\big)\psi &= (g, n)'\psi\\
&= (g_{\mathrm{con}}, n')\\
&= (f_{\mathrm{con}}\ {}^{m}g_{\mathrm{con}}, m'n') && \text{[by (7.7)]}\\
&= (f_{\mathrm{con}}, m')(g_{\mathrm{con}}, n')\\
&= (f, m)'\psi(g, n)'\psi.
\end{aligned}
$$

Hence ψ is a homomorphism and thus a monomorphism. Therefore ψ^{-1} is a homomorphism from the subsemigroup $\operatorname{im}\psi$ of $C(S)^M \wr C(M)$ onto $C(S \wr M)$, and so $C(S \wr M) \prec C(S)^M \wr C(M)$. 7.10

COROLLARY 7.11. *Let M be a finite monoid and S a semigroup. Then $C(S \wr M)$ divides a wreath product of copies of $C(S)$ and $C(M)$.*

Proof of 7.11. By Proposition 7.10, let M be a monoid and S a semigroup. Then $C(S \wr M) \prec C(S)^M \wr C(M)$. But $C(S)^M$ is a direct product of $|M|$ copies of $C(S)$ and so $C(S)^M \wr C(M)$ divides a wreath product of copies of $C(S)$ and $C(M)$ by Propositions 7.6 and 7.8. The result follows by the transitivity of $\prec$. 7.11

KROHN–RHODES DECOMPOSITION THEOREM

Let U_3 be the monoid obtained by adjoining an identity to a two-element right zero semigroup $\{a, b\}$. So U_3 has elements $\{1, a, b\}$ and is multiplication table is as shown in Figure 7.1. Notice that in U_3, the Green's relation $\mathcal{H}$ is the identity relation and so U_3 is aperiodic by Proposition 7.4.

	1	a	b
1	1	a	b
a	a	a	b
b	b	a	b

TABLE 7.1
Multiplication table of U_3.

To prove the Krohn–Rhodes theorem, we will prove that every finite semigroup divides a wreath product of its own subgroups and copies of U_3. We first of all note that it suffices to prove the theorem for monoids since $S \prec S^1$. The proof is by induction on the number of elements in the monoid. The core of the induction is Lemma 7.13, which shows that a monoid S is either a group, a left simple semigroup with an identity adjoined, monogenic, or can be decomposed as $S = L \cup T$, where L is a left ideal and T is a submonoid and L^1 and T have fewer elements than S. The theorem is trivial for groups, and we will prove it for left simple semigroups with identities adjoined (Lemma 7.15) and for monogenic semigroups (Lemma 7.16); these cases form the base of the induction. The fourth possibility, of decomposition as $S = L \cup T$, supplies the induction step.

We need the following auxiliary result before we prove Lemma 7.13:

LEMMA 7.12. *Let S be a finite semigroup. Then one of the following is true:*

a) *S is trivial;*
b) *S is left simple;*
c) *S is monogenic;*
d) *$S = L \cup T$, where L is a proper left ideal of S and T is a proper subsemigroup of S.*

Proof of 7.12. Suppose that none of a), b), or c) is true; we aim to prove d). Since S is not left simple, it contains proper left ideals. Since it is finite, it has a maximal proper left ideal K. Let $x \in S - K$. Then $K \cup S^1x$ is a left ideal that strictly contains K. Since K is maximal, $K \cup S^1x = S$. If $S^1x \neq S$, then let $L = K$ and $T = S^1x$ and the proof is complete.

So assume $S^1x = S$. Then $S = Sx \cup \langle x \rangle$. If $S \neq Sx$, then let $L = Sx$ and $T = \langle x \rangle$ and the proof is complete since $T \neq S$ because S is not monogenic.

So assume $S = Sx$. Let $M = \{y \in S : yx \in K\}$. Then M non-empty (since $Ma = L$) and is a left ideal of S. Furthermore, it is a proper left ideal because K is a proper left ideal and $Sx = S$. If $M \nsubseteq K$, then $M \cup K$ is a left ideal of S strictly containing the maximal left ideal K and so $M \cup K = S$; set $L = M$ and $T = K$ and the proof is complete.

So assume $M \subseteq K$; that is

$$yx \in K \Rightarrow y \in K. \tag{7.8}$$

Repeat the reasoning above for all $x \in S - K$. Either some such x allows us to complete the proof, or (7.8) holds for all $x \in S - K$. In the former case, the proof is finished. In the latter case, take the converse to see that $y \in S - K \Rightarrow yx \in S - K$ for all $x \in S - K$. Therefore $S - K$ is a subsemigroup. So let $L = K$ and $T = S - K$; the proof is complete. 7.12

LEMMA 7.13. *Let S be a finite monoid. Then one of the following is true:*

a) *S is a group;*

b) *S is a left simple with an identity adjoined;*

c) *S is monogenic;*

d) *$S = L \cup T$, where L is a left ideal of S and T is a submonoid of S, and L^1 and T both have fewer elements than S.*

Proof of 7.13. Suppose that none of a), b), and c) is true; we aim to prove d). Let G be the group of units of S. Consider two cases:

- G is trivial. Then $S - G = S - \{1\}$ is an ideal and thus a subsemigroup of S. Since S is not left simple with an identity adjoined, we know that $S - \{1\}$ is not left simple. Apply Lemma 7.12 to $S - \{1\}$ to see that $S - \{1\} = L \cup Q$, where K is a proper left ideal of $S - \{1\}$ and Q is a proper subsemigroup of $S - \{1\}$. Since $L \neq S - \{1\}$, we know that $L \cup \{1\} \neq S$. Let $T = Q \cup \{1\}$; then T is a proper submonoid of S and $S = L \cup T$.
- G is non-trivial. Then let $L = S - G$ and let $T = G$. Then $S = L \cup T$. Since G is non-trivial, $L \cup \{1\} \neq S$, and since S is not a group, $T \neq S$.

In both cases, $S = L \cup T$, where L is a left ideal of S and T is a submonoid of S. Furthermore, in both cases L^1 and T both have fewer elements than S. 7.13

Now we turn to proving the cases forming the base of the induction; that is, monoids consisting of a left simple semigroup with an identity adjoined, and monogenic monoids. To prove the former case in Lemma 7.15, we will need the following lemma, which essentially shows that the theorem holds for left zero semigroups:

LEMMA 7.14. *Every finite left zero semigroup divides a wreath product of copies of U_3.*

Proof of 7.14. Let L_n be the left zero semigroup with n elements. The strategy is to proceed by induction and show that $L_n^1 \prec L_{n-1}^1 \wr L_1^1$. The base of the induction is proved by observing that the semigroup $L_1^1 = \{0,1\}$ is a homomorphic image of U_3.

For each $x \in L_{n-1}^1$, define $f_x : L_1^1 \to L_{n-1}^1$ by $(1)f_x = x$ and $(0)f_x = 1$. Notice that there are n elements in L_{n-1}^1 and so n elements $(f_x, 0)$ of $L_{n-1}^1 \wr L_1^1$. Furthermore, $(f_x, 0)(f_y, 0) = (f_x {}^0f_y, 0) = (f_x, 0)$, since $(z)f_x {}^0f_y = (z)f_x(z0)f_y = (z)f_x(0)f_y = (z)f_x 1 = (z)f_x$. So the set $K = \{(0, f_x) : x \in L_{n-1}^1\}$

forms a left zero subsemigroup of $L^1_{n-1} \wr L^1_1$. So $K \cup \{1\}$ is a subsemigroup isomorphic to L^1_n. (The wreath product $L^1_{n-1} \wr L^1_1$ is a monoid by Exercise 7.6(a).) Hence $L^1_n \prec L^1_{n-1} \wr L^1_1$.

By Proposition 7.8, L^1_n and so L_n divide a wreath product of n copies of U_3. 7.14

LEMMA 7.15. *Let S be a finite left simple semigroup. Then S^1 divides the wreath product of a subgroup of S and copies of U_3.*

Proof of 7.15. Since S is finite, it contains an idempotent. By Exercise 3.11(b) (but for a left simple semigroup), we see that S is isomorphic to $G \times E$, where G is a subgroup of S and E is a left zero semigroup. By Lemma 7.14, E divides a wreath product of copies of U_3. So by Propositions 7.6 and 7.8, $G \times E$ divides a wreath product of G and copies of U_3. 7.15

Next we prove the remaining case for the base of the induction, namely monogenic monoids:

LEMMA 7.16. *Let S be a finite monogenic monoid. Then S divides the wreath product of a subgroup of S and copies of U_3.*

Proof of 7.16. The monogenic monoid $S = \{1, x, \ldots, x^k, \ldots, x^{k+m-1}\}$ (with $x^{k+m} = x^k$) is an ideal extension of the subgroup $G = \{x^k, \ldots, x^{k+m-1}\}$ by the monogenic monoid $C_k = \{1, x, \ldots, x^k\}$ (with $x^k = x^k + 1$).

We proceed by induction on k and show that C_k divides a subsemigroup of $C_{k-1} \wr C_1$. The base case of the induction is proven by observing that $C_1 = \{1, x\}$ (with $x^2 = x$) divides U_3.

Define $f_i : C_1 \to C_{k-1}$ by $(1)f_i = x^{i-1}$ and $(0)f_i = x^i$. Then $(f_i, 0)(f_1, 0) = (f_i {}^0 f_1, 0) = (f_{i+1}, 0)$ since

$$(0)f_i {}^0 f_1 = (0)f_i(0)f_1 = x^i x = x^{i+1} = (0)f_{i+1},$$
$$(1)f_i {}^0 f_1 = (1)f_i(0)f_1 = x^{i-1}x = (1)f_{i+1}.$$

Hence $(f_1, 0)^{k+1} = (f_1, 0)^k \neq (f_1, 0)^{k-1}$ and so the monogenic submonoid of $C_{k-1} \wr C_1$ generated by $(f_1, 0)$ is isomorphic to C_k. Hence $C_k \prec C_{k-1} \wr C_1$.

Thus every C_k divides a wreath product of U_3 by Propositions 7.6 and 7.8. So S, being an ideal extension of G and C_k, divides a wreath product of G and copies of U_3 by Proposition 7.7. 7.16

Finally, we are ready to being proving the induction step, in the case where the monoid has been decomposed as the union of a left ideal and a subsemigroup. We require the following four lemmata, and then we can quickly prove the theorem.

LEMMA 7.17. *Let S be a semigroup and suppose $S = L \cup T$, where L is a left ideal of S and T is a subsemigroup of S. Then $S \prec L^1 \wr C(T^1)$.*

Proof of 7.17. Let $i : C(T^1) \to L^1$ be the constant mapping defined by $(t)i = (t')i = 1$ for all $t \in T^1$. For each $x \in L$, let $f_x : C(T^1) \to L^1$ be the right translation defined by $(t)f_x = (t')f_x = tx$ for all $t \in T^1$. Notice that $tx \in L$ since L is a left ideal.

Let

$$V = \{(i,t) : t \in T^1\} \cup \{(f_x, t') : x \in L, t \in T^1\}.$$

We aim to show V is a subsemigroup of $L^1 \wr C(T^1)$ and that S is a homomorphic image of V. We have four cases to consider:

a) Let $(i,t),(i,u) \in V$. Then $(i,t)(i,u) = (i^t i, tu) = (i,tu)$ since $(s)i^t i = (s)i(st)i = 1 = (s)i$ and $(s')i^t i = (s')i(s't)i = 1 = (s')i$ for all $s \in T^1$.

b) Let $(i,t),(f_y,u') \in V$. Then $(i,t)(f_y,u') = (i^t f_y, tu') = (f_{ty}, u')$, since $(s)i^t f_y = (s)i(st)f_y = 1sty = (s)f_{ty}$ and $(s')i^t f_y = (s')i(s't)f_y = 1s'ty = (s')f_{ty}$ for all $s \in T^1$.

c) Let $(f_x,t'),(i,u) \in V$. Then $(f_x,t')(i,u) = ({f_x}^{t'} i, t'u) = (f_x,(tu)')$ since $(s){f_x}^{t'} i = (s)f_x(st')i = (s)f_x 1 = (s)f_x$ and $(s'){f_x}^{t'} i = (s')f_x(s't')i = (s')f_x 1 = (s')f_x$ for all $s \in T^1$.

d) Let $(f_x,t'),(f_y,u') \in V$. Then $(f_x,t')(f_y,u') = ({f_x}^{t'} f_y, t'u') = (f_{xty}, u')$, since $(s){f_x}^{t'} f_y = (s)f_x(st')f_y = (s)f_x(t')f_y = sxty = (s)f_{xty}$ and $(s'){f_x}^{t'} f_y = (s')f_x(s't')f_y = (s')f_x(t')f_y = sxty = (s')f_{xty}$ for all $s \in T^1$.

Hence V is a subsemigroup of $L^1 \wr C(T^1)$. Define a map $\varphi : V \to S$ by $(i,t)\varphi = t$ and $(f_x,t')\varphi = xt$. Then, using the four cases above,

$$\begin{aligned}
\big((i,t)(i,u)\big)\varphi &= (i,tu)\varphi = tu = (i,t)\varphi(i,u)\varphi,\\
\big((i,t)(f_y,u')\big)\varphi &= (f_{ty},u')\varphi = tyu = (i,t)\varphi(f_y,u')\varphi,\\
\big((f_x,t')(i,u)\big)\varphi &= (f_x,(tu)')\varphi = xtu = (f_x,t')\varphi(i,u)\varphi,\\
\big((f_x,t')(f_y,u')\big)\varphi &= (f_{xty},u')\varphi = xtyu = (f_x,t')\varphi(f_y,u')\varphi;
\end{aligned}$$

hence φ is a homomorphism. Finally, note that $T \subseteq \operatorname{im}\varphi$ since $(i,t)\varphi = t$ for all $t \in T$ and $L \subseteq \operatorname{im}\varphi$ since $(f_x,1)\varphi = x$ for all $x \in L$. Hence $S = L \cup T = \operatorname{im}\varphi$ and so φ is an epimorphism. Thus $S \prec L^1 \wr C(T^1)$. 7.17

The following result is essentially a more precise version of Lemma 7.17 that holds when we decompose a monoid into the union of its group of units and the set of remaining elements:

LEMMA 7.18. *Let S be a monoid and let G be its group of units. Then $I = S - G$ is an ideal of S and $S \prec I^1 \wr G$.*

Proof of 7.18. First, notice that $S-G$ is an ideal by Proposition 7.1. For each $x \in I^1$, define a map $f_x : G \to I^1$ by $(g)f_x = gxg^{-1}$ for all $g \in G$. Notice that $(g)f_1 = gg^{-1} = 1$ for all $g \in G$. Let $V = \{(f_x, g) : x \in I^1, g \in G\}$.

Let $(f_x,g),(f_y,h) \in V$. Then for any $k \in G$,

$$(k)f_x\, {}^g f_y = (k)f_x(kg)f_y = kxk^{-1}kgyg^{-1}k^{-1} = k(xgyg^{-1})k^{-1} = (k)f_{xgyg^{-1}}. \quad (7.9)$$

Therefore $(f_x, g)(f_y, h) = (f_x {}^g f_y, gh) = (f_{xgyg^{-1}}, gh)$. Notice that $xgyg^{-1} \in I^1$ since x is in I^1 and I is an ideal. Thus V is a subsemigroup of $I^1 \wr G$.

Define a map $\varphi : V \to S$ by $(f_x, g)\varphi = xg$. This map φ is well-defined since $f_x = f_y \Rightarrow (1)f_x = (1)f_y \Rightarrow x = y$. Furthermore,

$$\begin{aligned}\big((f_x, g)(f_y, h)\big)\varphi &= (f_x {}^g f_y, gh)\varphi \\ &= (f_{xgyg^{-1}}, gh)\varphi && \text{[by (7.9)]} \\ &= xgyg^{-1}gh \\ &= xgyh \\ &= (f_x, g)\varphi(f_y, h)\varphi.\end{aligned}$$

So φ is a homomorphism. Finally, $G \subseteq \operatorname{im}\varphi$ since $(f_1, g)\varphi = g$ for all $g \in G$ and $I^1 \subseteq \operatorname{im}\varphi$ since $(f_x, 1)\varphi = x$ for all $x \in S$. So φ is an epimorphism and so $S \prec I^1 \wr G$. 7.18

The following lemma shows that the result holds for right zero semigroups, but we only use it to prove the next lemma.

LEMMA 7.19. *Every finite right zero semigroup, and every finite right zero semigroup with an identity adjoined, divides a wreath product of copies of* U_3.

Proof of 7.19. Let R_k denote the right zero semigroup with k elements. Notice that R_k is a subsemigroup of R_ℓ and R_k^1 is a submonoid of R_ℓ^1 for $k \leq \ell$. The direct product of n copies of U_3 contains subsemigroups isomorphic to R_{2^n} and $R_{2^n}^1$, so for any k the direct product of sufficiently many copies of U_3 contains R_k and R_k^1. So R_k and R_k^1 divide a wreath product of copies of U_3 by Proposition 7.6. 7.19

LEMMA 7.20. *Let S be a semigroup. Suppose S divides a wreath product of groups and copies of U_3. Then $C(S)$ divides a wreath product of copies of those same groups and copies of U_3.*

Proof of 7.20. Supppose S divides a wreath product of groups G_i and copies of U_3. By Propositions 7.8, 7.9, and 7.11, $C(S)$ divides a wreath product of the monoids $C(G_i)$ and copies of $C(U_3)$. The semigroup $C(U_3)$ is a right zero semigroup with an identity adjoined, which divides a wreath product of copies of U_3 by Lemma 7.19. The group of units of $C(G_i)$ is G_i and $L = C(G_i) - G_i$ is an ideal of $C(G_i)$ by Proposition 7.1 and a right zero semigroup. So $C(G_i)$ divides $L^1 \wr G_i$ by Lemma 7.18. Since L^1 is a right zero semigroup with an identity adjoined, it divides the wreath product of copies of U_3 by Lemma 7.19. So $L^1 \wr G_i$ divides a wreath product of G_i and copies of U_3 by Proposition 7.8. So S divides a wreath product the groups G_i and copies of U_3. 7.20

Finally, equipped with these lemmata, the proof of the Krohn–Rhodes theorem is now quite straightforward. To keep track of the roles of the various lemmata, see Figure 7.1.

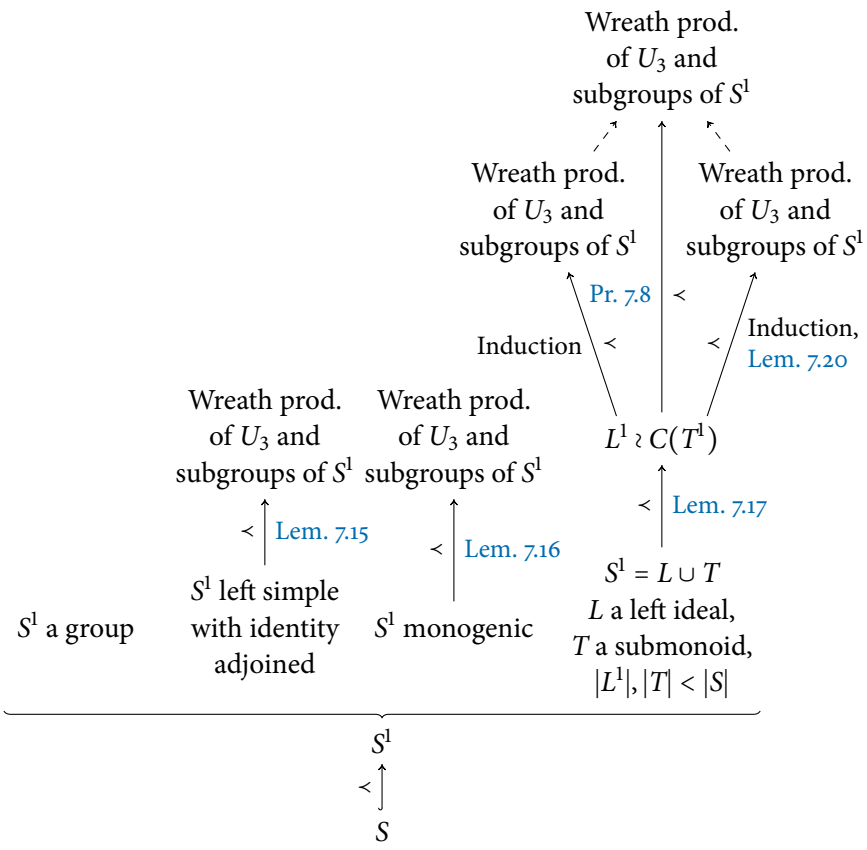


FIGURE 7.1
Diagram showing how the various lemmata are used to prove the Krohn–Rhodes theorem.

Krohn–Rhodes decomposition theorem

THEOREM 7.21. *Let S be a finite semigroup. Then S divides a wreath product of subgroups of S and copies of U_3.*

Proof of 7.21. Let S be a semigroup; we will show that S divides a wreath product of its subgroups and copies of U_3. Since $S \prec S^1$, we can assume S is a monoid.

The strategy is induction on the number of elements in S. The base case of the induction is when S has one element. In this case, S is trivial, and so S is a group and the result hold immediately.

So assume the result holds for all monoids with fewer elements than S. As already noted, the result clearly holds if S is a group and in particular if S is trivial. It also holds by Lemma 7.15 if S is a left simple semigroup with an identity adjoined, and if S is monogenic by Lemma 7.16.

So assume S is not trivial, not a group, not a left simple semigroup with an identity adjoined, and not monogenic. By Lemma 7.13, $S = L \cup T$, where L is a left ideal and T is a submonoid of S and both L^1 and T have fewer elements than S. So by the induction hypothesis, L^1 divides a wreath product of subgroups of L^1 (which are also subgroups of S) and copies of U_3, and similarly T divides a wreath product of subgroups of T (which are also subgroups of S) and copies of U_3. By Lemma 7.20, $C(T)$ also divides a wreath product of subgroups of S and copies of U_3. By

Proposition 7.8, S thus divides a wreath product of subgroups of S and copies of U_3.

Thus, by induction, the result holds for all monoids S. 7.21

EXERCISES

[See pages 161–165 for the solutions.]

7.1 Let S be a finite semigroup. Let J_x be a nontrivial $\mathcal{J}$-class of S. Prove that there is a regular $\mathcal{J}$-class J_y such that $J_x \leq J_y$.

*7.2 a) Prove that a finite nilsemigroup is nilpotent.

b) Give an example of an infinite nilsemigroup that is not nilpotent.

7.3 Let S and S' be finite semigroups and let $\varphi : S \to S'$ be an epimorphism.

a) Let J be a $\mathcal{J}$-class of S. Prove that there is a $\mathcal{J}$-class J' of S' such that $J\varphi \subseteq J'$.

b) Let J' be a $\mathcal{J}$-class of S'. Prove that there is a $\mathcal{J}$-class J of S such that $J\varphi \subseteq J'$. If J is minimal such that $J\varphi \subseteq J'$, then $J\varphi = J'$.

*7.4 Prove that if S is a finite semigroup in which $\mathcal{H}$ is the equality relation and $T \prec S$, then in T the relation $\mathcal{H}$ is also the equality relation. Give an example to show that this is may not be true when S is infinite.

*7.5 Prove that the multiplication (7.1) is associative.

*7.6 a) Prove that if M and N are monoids, $M \wr N$ is a monoid.

b) Prove that if M and N are groups, $M \wr N$ is a group.

7.7 Suppose that S and T are cancellative semigroups. Must $S \wr T$ be cancellative?

*7.8 Prove that the product defined by (7.3) for the constant extension is associative.

7.9 Let M be a non-trivial monoid. For each $x \in M$, let $\rho_x \in \mathcal{T}_M$ and $\tau_x \in \mathcal{T}_M$ be defined by $y\rho_x = yx$ and $y\tau_x = x$. Prove that $C(M)$ is isomorphic to the subset $\{\rho_x, \tau_x : x \in M\}$ of $\mathcal{T}_M$.

*7.10 Using a technique similar to the proof of (7.4), prove (7.5), (7.6), (7.7)

NOTES

The Krohn–Rhodes theorem was first stated and proved for automata in Krohn & Rhodes, 'Algebraic theory of machines I. Prime decomposition theorem for finite semigroups and machines'. The proof

in this chapter is due to Lallement, *Semigroups and Combinatorial Applications*, including the correction published in Lallement, 'Augmentations and wreath products of monoids'.

Varieties & pseudovarieties

8

❁ The aim of this chapter is to introduce varieties and pseudovarieties, which are, essentially, well-behaved classes of semigroups. For instance, the class of all commutative semigroups forms a variety, and the class of all *finite* commutative semigroups forms a pseudovariety. We will see how varieties and pseudovarieties can be defined and manipulated.

The concepts of varieties and pseudovarieties are actually broader than semigroups: varieties make sense for any type of algebraic structure, and the pseudovarieties make sense for any type of finite algebraic structure. Thus a large part of this chapter will be expressed in terms of universal algebra.

VARIETIES

Algebras and operations

An *algebra* is a set S equipped with some operations $\{f_i : i \in I\}$. An *operation* f_i on S is simply a map $f_i : S^{f_i\alpha} \to S$ for some $f_i\alpha \in \mathbb{N} \cup \{0\}$. This $f_i\alpha$ is called the *arity* of f_i. For instance, if S is a semigroup, the multiplication operation $\circ$ is a map $\circ : S^2 \to S$ and so has arity 2. If S is a inverse semigroup, the inverse operation $^{-1}$ is a map $^{-1} : S \to S$ and so has arity 1. If S is a monoid, we can view the identity element 1_S as an operation, or as a map $1_S : S^0 \to S$; the operation 1_S has arity 0. Operations of arity 1 are called *unary*; operations of arity 2 are called *binary*; operations of arity 0 are called *constants*. Notice that we have a map $\alpha : \{f_i : i \in I\} \to \mathbb{N} \cup \{0\}$.

Arity of an operation

Types

A *type* $\mathcal{T}$ of an algebra is a set of operations symbols $\{f_i : i \in I\}$ and a map $\alpha : \{f_i : i \in I\} \to \mathbb{N} \cup \{0\}$ determining the arity of each operations. We can write the type simply by listing the pairs in the map α (viewed as a set). A semigroup has type $\{(\circ, 2)\}$ and a lattice has type $\{(\wedge, 2), (\vee, 2)\}$. An algebra of type $\mathcal{T}$ is called a *$\mathcal{T}$-algebra*.

Notice that some structures can be viewed as algebras in more than one way, and thus have more than one type. Let G be a group. Then G, viewed as a group, is a $\{(\circ, 2), (1_G, 0), (^{-1}, 1)\}$-algebra; G, viewed as a monoid, is a $\{(\circ, 2), (1_G, 0)\}$-algebra; G, viewed as a semigroup, is a $\{(\circ, 2)\}$-algebra.

Strictly speaking, we should distinguish a symbol f_i from the operation f_i: for instance, we use the same symbol $\circ$ to refer to the different multiplications in different semigroups. We will want to discuss operations of the same type.

Let $\mathcal{T} = \{(f_i, f_i\alpha) : i \in I\}$ be a type. We are now going to give the definition of subalgebras, homomorphisms, congruences, and direct products of $\mathcal{T}$-algebras. These definitions are straightforward generalizations of the definitions for semigroups.

Subalgebras

Let S be a $\mathcal{T}$-algebra. A subset S' of S is a *subalgebra* of S if S' is closed under all the operations in $\mathcal{T}$: that is, for each $i \in I$, we have

$$x_1, \ldots, x_{f_i\alpha} \in S' \Rightarrow (x_1, \ldots, x_{f_i\alpha})f_i \in S'.$$

Let $X \subseteq S$. The subalgebra generated by X is defined to be the intersection of all subalgebras that contain X. It is easy to prove (cf. Proposition 1.9) that the subalgebra generated by X consists of all elements that can be obtained by starting from X and applying the operations f_i.

Homomorphisms

Let S and T be $\mathcal{T}$-algebras. Then $\varphi : S \to T$ is a *homomorphism* if for each $i \in I$, we have

$$\big((x_1, \ldots, x_{f_i\alpha})f_i\big)\varphi = (x_1\varphi, \ldots, x_{f_i\alpha}\varphi)f_i. \tag{8.1}$$

(Notice that on the left-hand side of (8.1), f_i is an operation on S, while on the right-hand side, it is an operation on T.) An injective homomorphism is a *monomorphism*, a surjective homomorphism is an *epimorphism*, and a bijective homomorphism is an *isomorphism*. If $\varphi : S \to T$ is an epimorphism, T is a *homomorphic image* of S.

Congruences

Let S be a $\mathcal{T}$-algebra. A binary relation ρ on S is a *congruence* if for each $i \in I$,

$$(\forall x_1, y_1, \ldots, x_{f_i\alpha}, y_{f_i\alpha})\big(x_1 \,\rho\, y_1 \wedge \ldots \wedge x_{f_i\alpha} \,\rho\, x_{f_i\alpha} \Rightarrow (x_1, \ldots, x_{f_i\alpha})f_i \,\rho\, (y_1, \ldots, y_{f_i\alpha})f_i\big).$$

Direct products

Let $\mathcal{S} = \{S_j : j \in J\}$ be a collection of $\mathcal{T}$-algebras. The *direct product* of the $\mathcal{T}$-algebras in $\mathcal{S}$ is their cartesian product $\prod^{\times}_{j\in J} S_j$ with the operations performed componentwise. To state this formally, view an element $s \in \prod^{\times}_{j\in J} S_j$ as a map $s : J \to \bigcup_{j\in J} S_j$ such that $(j)s \in S_j$ for all $j \in J$; then

$$(j)(s_1, \ldots, s_{f_i\alpha})f_i = \big((j)s_1, \ldots, (j)s_{f_i}\big)f_i.$$

Free $\mathcal{T}$-algebras

Let A be a non-empty set and let $F_{\mathcal{T}}(A)$ be the smallest set of all formal expressions (that is, words) over $A \cup \{f_i : i \in I\} \cup \{(\} \cup \{)\} \cup \{,\}$ satisfying the following:

1. $A \subseteq F_{\mathcal{T}}(A)$;
2. if $u_1, \ldots, u_{f_i\alpha} \in F_{\mathcal{T}}(A)$, then $(u_1, \ldots, u_{f_i\alpha})f_i \in F_{\mathcal{T}}(A)$.

For instance, if $\mathcal{T}$ is $\{(f,2),(\ '\ ,1)\}$ and $A = \{a,b,c\}$, then the words $(a,(((c,b)f)',c)f)f$ and $(((b)',((b,a)f,(c)')f)f$ are examples of elements of $F_{\mathcal{T}}(A)$. The set $F_{\mathcal{T}}(A)$ is obviously a $\mathcal{T}$-algebra and is called the *free $\mathcal{T}$-algebra* or *absolutely free-$\mathcal{T}$ algebra*. Notice that $F_{\mathcal{T}}(A)$ is generated by A.

Let $\iota : A \to F_{\mathcal{T}}(A)$ be the inclusion map. For any $\mathcal{T}$-algebra S and map $\varphi : A \to S$, there is a unique extenion of φ to a homomorphism $\hat{\varphi} : F_{\mathcal{T}}(A) \to S$. That is, $\iota\hat{\varphi} = \varphi$, or, equivalently, the following diagram commutes:

$$\begin{array}{ccc} A & \xhookrightarrow{\iota} & F_{\mathcal{T}}(A) \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \hat{\varphi}} \\ & & S \end{array} \tag{8.2}$$

This property is reminiscent of the definition of a free semigroup, and we shall say more about it later.

Let $\mathcal{X}$ be a non-empty class of $\mathcal{T}$-algebras. Let $\operatorname{Hom}\mathcal{X}$ denote the class of all $\mathcal{T}$-algebras that are homomorphic images of the algebras in $\mathcal{X}$. Let $\operatorname{Sub}\mathcal{X}$ denote the class of all $\mathcal{T}$-algebras that are subalgebras of algebras in $\mathcal{X}$. Let $\operatorname{Prod}\mathcal{X}$ denote the class of all $\mathcal{T}$-algebras that are direct products of the $\mathcal{T}$-algebras in $\mathcal{X}$. That is,

$$\begin{aligned} \operatorname{Hom}\mathcal{X} &= \big\{S : (\exists T \in \mathcal{X})(S \text{ is a homomorphic image of } T)\big\}; \\ \operatorname{Sub}\mathcal{X} &= \big\{S : (\exists T \in \mathcal{X})(S \text{ is a subsemigroup of } T)\big\}; \\ \operatorname{Prod}\mathcal{X} &= \Big\{S : (\exists \{T_i : i \in I\} \subseteq \mathcal{X})\Big(S = \prod_{i\in I}^{\times} T_i\Big)\Big\}. \end{aligned}$$

Thus Hom, Sub, and Prod are unary operators on classes of algebras. Notice that $\mathcal{X}$ is contained in $\operatorname{Hom}\mathcal{X}$, $\operatorname{Sub}\mathcal{X}$, and $\operatorname{Prod}\mathcal{X}$.

A non-empty class of $\mathcal{T}$-algebras is a *variety* of $\mathcal{T}$-algebras if it is closed under the operations Hom, Sub, and Prod. That is, $\mathcal{X}$ is a variety if $\operatorname{Hom}\mathcal{X} \cup \operatorname{Sub}\mathcal{X} \cup \operatorname{Prod}\mathcal{X} \subseteq \mathcal{X}$.

EXAMPLES 8.1. a) Let 1 consist only of the trivial semigroup $E = \{e\}$. Then 1 is a variety, since the only subsemigroup of E is E itself, the only homomorphic image of E is E itself, and any direct product of copies of E is isomorphic to E.

b) Let Com consist of all commutative semigroups (viewed as $\{(\circ,2)\}$-algebras) Since any subalgebra or homomorphic image of a commutative semigroup is itself a commutative semigroup, and a direct product of commutative semigroups is commutative, C is a variety.

c) Let G consist of all groups, viewed as $\{(\circ,2),(1_G,0),(^{-1},1)\}$-algebras. Then subalgebras are closed under taking inverses; thus subalgebras are subgroups. Since any subalgebra or homomorphic image of a group is also a group, and any direct product of groups is also a group, G is a variety.

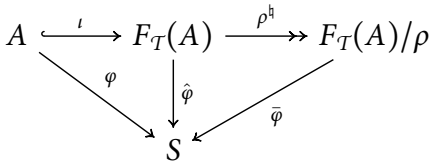
Notice that the class of all groups $\mathcal{G}$ viewed as $\{(\circ, 2)\}$ algebras is *not* a variety, because in this case subalgebras are subsemigroups and so $\mathcal{G}$ is not closed under taking subalgebras; for example, $\mathcal{G}$ contains $\mathbb{Z}$ but not its subsemigroup $\mathbb{N}$.

d) Let I consist of all inverse semigroups, viewed as a $\{(\circ, 2), ({}^{-1}, 1)\}$-algebra. Then I is a variety.

Let V be a variety of $\mathcal{T}$-algebras and let A be a non-empty set. Let $S \in \mathsf{V}$. Let S^A denote the set of maps from A to S, and let $\varphi \in S^A$. We know there is a unique extension of φ to a homomorphism $\hat{\varphi} : F_{\mathcal{T}}(A) \to S$. Now, $\operatorname{im}\hat{\varphi}$ is a subalgebra of S and so $\operatorname{im}\hat{\varphi} \in \mathsf{V}$ since V is closed under forming subalgebras. Let

$$\rho = \bigcap \{\ker \hat{\varphi} : \varphi \in S^A, S \in \mathsf{V}\}.$$

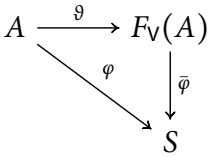
Then ρ, being an intersection of congruences on $F_{\mathcal{T}}(A)$, is also a congruence. Furthermore, $\rho \subseteq \ker\hat{\varphi}$ for any $\varphi \in S^A$. Hence for each $S \in \mathsf{V}$, there exists a unique homomorphism $\bar{\varphi} : F_{\mathcal{T}}(A)/\rho \to S$ such that $\rho^\natural\bar{\varphi} = \hat{\varphi}$. Thus $\bar{\varphi} : F_{\mathcal{T}}(A)/\rho \to S$ is the unique homomorphism such that $\varphi = \iota\hat{\varphi} = \iota\rho^\natural\bar{\varphi}$, and the following diagram commutes:



By a result for $\mathcal{T}$-algebras analogous to Proposition 1.30, $F_{\mathcal{T}}(A)/\rho$ is a subdirect product of $\{F_{\mathcal{T}}(A)/\ker\hat{\varphi} : \varphi \in S^A, S \in \mathsf{V}\}$. Now, each algebra $F_{\mathcal{T}}(A)/\ker\hat{\varphi}$ is a subalgebra of an element of V and therefore is itself a member of V (since $\operatorname{Sub}\mathsf{V} = \mathsf{V}$). Hence $F_{\mathcal{T}}(A)/\rho \in \operatorname{Sub}\operatorname{Prod}\mathsf{V} = \mathsf{V}$.

V-free algebras

The $\mathcal{T}$-algebra $F_{\mathcal{T}}(A)/\rho$ is called the V-*free algebra*, and is denoted $F_{\mathsf{V}}(A)$. Notice that there is a map $\vartheta : A \to F_{\mathsf{V}}(A)$ given by $x\vartheta = x\iota\rho^\natural = [x]_\rho$ such that the *universal mapping property* holds: for any $S \in \mathsf{V}$ and map $\varphi : A \to S$, there is a unique homomorphism $\bar{\varphi} : F_{\mathsf{V}}(A) \to S$ such that the following diagram commutes:



Notice that if V is the variety of all $\mathcal{T}$-algebras, $F_{\mathsf{V}}(A) = F_{\mathcal{T}}(A)$ and we recover diagram (8.2).

So for any variety V of $\mathcal{T}$-algebras we have (for each set A) a $\mathcal{T}$-algebra $F_{\mathsf{V}}(A) \in \mathsf{V}$ and a map $\vartheta : A \to F_{\mathsf{V}}(A)$ with the universal mapping property. This indicates that varieties are well-behaved collections of algebras

(and, in, particular, semigroups). But varieties have another, very useful property: they are precisely those collections of algebras that can be defined using sets of equations called laws.

Laws

For $\mathcal{T}$-algebras, a *law* over an alphabet A (sometimes called an *identity* or *identical relation* over A, but we will avoid this confusing terminology) is a pair of elements u and v of $F_{\mathcal{T}}(A)$, normally written as a formal equality $u = v$. A $\mathcal{T}$-algebra S *satisfies* the law $u = v$ if, for every map $\varphi : A \to S$, we have $u\hat{\varphi} = v\hat{\varphi}$ (where $\hat{\varphi}$ is the homomorphism in diagram (8.2)). Informally, S satisfies $u = v$ if we every possible substitution of elements of S for letters of A in the words u and v gives elements that are equal. For instance, commutative semigroups, viewed as $\{(\circ, 2)\}$-algebras, satisfy the law $x \circ y = y \circ x$. Semigroups of idempotents satisfy the law $x \circ x = x$.

Equational classes

Let $\mathcal{E}$ be a class of $\mathcal{T}$-algebras. Suppose there is a set L of laws over an alphabet A such that $S \in \mathcal{E}$ if and only if S satisfies every law in L. Then $\mathcal{E}$ is the *equational class* defined by L.

Birkhoff's theorem

THEOREM 8.2. *Let $\mathcal{T}$ be a type. Then a class of $\mathcal{T}$-algebras is a variety if and only if it is an equational class.*

Proof of 8.2. First part. Suppose $\mathcal{X}$ is an equational class. Then there is a set of laws L over an alphabet A such that $S \in \mathcal{X}$ if and only if S satisfies every law in L. To prove that $\mathcal{X}$ is a variety, we must show that it is closed under Hom, Sub, and Prod.

Let $S \in \mathcal{X}$, and let T be a $\mathcal{T}$-algebra and $\psi : S \to T$ an epimorphism. Let $u = v$ be a law in L. Let $\varphi : A \to T$ be a homomorphism. Define a map $\theta : A \to S$ by letting $a\theta \in S$ be such that $a\theta\psi = a\varphi$ (such an $a\theta$ exists because ψ is surjective). Notice that $\hat{\theta}\psi$ and $\hat{\varphi}$ are homomorphisms from $F_{\mathcal{T}}(A)$ to S extending $\theta\psi = \varphi$ and so, by the uniqueness of such homomorphisms, $\hat{\theta}\psi = \hat{\varphi}$. Since S satisfies L, we have $u\hat{\theta} = v\hat{\theta}$; hence $u\hat{\varphi} = u\hat{\theta}\psi = v\hat{\theta}\psi = v\hat{\psi}$. So T satisfies $u = v$. Hence T satisfies every law in L and so $T \in \mathcal{X}$. Thus $\mathcal{X}$ is closed under Hom.

Let $S \in \mathcal{X}$ and let T be a subalgebra of S. Let $u = v$ be a law in L. Then if $\varphi : A \to T$, then φ is also a map from A to S and so $u\hat{\varphi} = v\hat{\varphi}$ since S satisfies $u = v$. Hence T also satisfies $u = v$. So T satisfies every law in L and so $T \in \mathcal{X}$. Thus $\mathcal{X}$ is closed under Sub.

Let $\{S_j : j \in J\} \subseteq \mathcal{X}$ and suppose T is the direct product of $\{S_j : j \in J\}$. Let $u = v$ be a law in L. Let $\varphi : A \to T$ be a map. For each $j \in J$, let $\varphi_j = \varphi\pi_j$, where $\pi_j : T \to S_j$ is the projection homomorphism. So φ_j is a map from A to S_j, and S_j satisfies $u = v$, and thus $u\hat{\varphi}_j = v\hat{\varphi}_j$. The map $\psi : F_{\mathcal{T}}(A) \to T$ with $(j)(x\psi) = x\hat{\varphi}_j$ is a homomorphism extending φ, so, by the uniqueness condition, $\psi = \hat{\varphi}$. Since $u\hat{\varphi}_j = v\hat{\varphi}_j$ for each j, we have $u\hat{\varphi} = u\psi = v\psi = v\hat{\varphi}$; hence T satisfies $u = v$. So T satisfies every law in L and so $T \in \mathcal{X}$. Thus $\mathcal{X}$ is closed under Prod.

So $\mathcal{X}$ is closed under Hom, Sub, and Prod, and so is a variety.

Second part. Suppose now that V is a variety. Let A be an infinite alphabet. Recall that $F_{\mathsf{V}}(A) = F_{\mathcal{T}}(A)/\rho$, where

$$\rho = \bigcap \{\ker \hat{\varphi} : \varphi \in S^A, S \in \mathsf{V}\}.$$

We aim to show that V is the equational class defined by ρ, viewing pairs $\rho \subseteq F_{\mathcal{T}}(A) \times F_{\mathcal{T}}(A)$ as a set of laws.

Let $S \in \mathsf{V}$. Let $(u, v) \in \rho$; notice that $u, v \in F_{\mathcal{T}}(A)$. Then $(u, v) \in \ker \hat{\varphi}$ and thus $u\hat{\varphi} = v\hat{\varphi}$ for any $\varphi \in S^A$. So S satisfies the law $u = v$. Thus every $S \in \mathsf{V}$ satisfies the law $u = v$ for any $(u, v) \in \rho$.

Conversely, suppose that S satisfies the law $u = v$ for every $(u, v) \in \rho$. Let B be an alphabet with cardinality greater than or equal to both S and A. Let $F_{\mathsf{V}}(B)$ be the V-free algebra generated by B; then $F_{\mathsf{V}}(B) = F_{\mathcal{T}}(B)/\pi$ for some congruence π on $F_{\mathcal{T}}(B)$.

Let $\psi : F_{\mathcal{T}}(B) \to S$ be a homomorphism. Let $(u, v) \in \pi$. Let B_0 be the subset of B containing the letters that appear in u or v; notice that B_0 is finite. Let A_0 be a finite subset of A such that there is a bijection $\xi_0 : A_0 \to B_0$. Since B has cardinality greater than or equal to A, there is an injection $\xi : A \to B$ extending ξ_0. Since ξ is injective, there is a right inverse $\eta : B \to A$ of ξ (that is, $\xi\eta = \mathrm{id}_A$). Then ξ extends to a monomorphism $\hat{\xi} : F_{\mathcal{T}}(A) \to F_{\mathcal{T}}(B)$, and η extends to a homomorphism $\hat{\eta} : F_{\mathcal{T}}(B) \to F_{\mathcal{T}}(A)$. Since $\hat{\xi}$ is injective, there are uniquely determined $u_0, v_0 \in F_{\mathcal{T}}(A)$ such that $u_0\hat{\xi} = u$ and $v_0\hat{\xi} = v$. Notice that $u\eta = u_0$ and $v\eta = v_0$.

Consider the map $\eta\rho^\natural : F_{\mathcal{T}}(B) \to F_{\mathsf{V}}(A)$. Since $F_{\mathsf{V}}(B)$ lies in the variety V, we must have $\pi \subseteq \eta\rho^\natural$. In particular, $u\eta\rho^\natural = v\eta\rho^\natural$ and so $(u_0, v_0) \in \rho$. Thus S satisfies the law $u_0 = v_0$. Therefore, since $\eta\psi : F_{\mathcal{T}}(B) \to S$ is a homomorphism, $u_0\eta\psi = v_0\eta\psi$ and so $u\psi = v\psi$.

Hence $\pi \subseteq \ker \psi$ and so we have a well-defined homomorphism $\theta : F_{\mathsf{V}}(B) \to S$ with $[x]_\pi\theta = x\psi$. Therefore S is a homomorphic image of $F_{\mathsf{V}}(B) \in \mathsf{V}$ and so lies in the variety V

Thus we have proved that $S \in \mathsf{V}$ if and only if S satisfies every law $u = v$ in ρ. Therefore V is an equational class. 8.2

Theorem 8.2 shows that every variety can be defined by a set of laws, but in general, an infinite set of laws is required. This is true even for varieties of semigroups. However, in some cases, a finite set of laws suffice. Such varieties are said to be *finitely based*.

Let $\mathcal{T}$ be the type $\{(\circ, 2)\}$. The variety of all semigroups is defined by the law $x \circ (y \circ z) = (x \circ y) \circ z$. All semigroups satisfy this law, so when working with varieties of semigroups we will always implicitly assume it and write xy for $x \circ y$.

Now let $\mathcal{T}$ be the type $\{(\circ, 2), (^{-1}, 1)\}$. Again, when working with semigroups, we will assume the law $(xy)z = x(yz)$; we will also assume $xx^{-1}x = x$ and $(x^{-1})^{-1} = x$.

Some example varieties of semigroups are listed in Table 8.1.

Variety	*Symbol*	*Defining laws*
Trivial semigroup	1	$x = y$
Null semigroups	Z	$xy = zt$
Left zero semigroups	LZ	$xy = x$
Right zero semigroups	RZ	$xy = y$
Commutative semigroups	Com	$xy = yx$
Semilattices	Sl	$\begin{cases} x^2 = x, \\ xy = yx \end{cases}$
Completely regular sgrps	CR	$xx^{-1} = x^{-1}x$
Inverse semigroups	I	$\begin{cases} (xy)^{-1} = y^{-1}x^{-1}, \\ xx^{-1}yy^{-1} = yy^{-1}xx^{-1} \end{cases}$
Clifford semigroups	Cl	$\begin{cases} xx^{-1} = x^{-1}x, \\ xx^{-1}yy^{-1} = yy^{-1}xx^{-1} \end{cases}$
Groups	G	$xx^{-1} = yy^{-1}$
Semigroups	S	—

TABLE 8.1
Some varieties of semigroups. The laws $x(yz) = (xy)z$, $xx^{-1}x = x$, and $(x^{-1})^{-1} = x$ are implicitly assumed.

Another way to define a variety of $\mathcal{T}$-algebras is to use a specified set of $\mathcal{T}$-algebras to generate a variety. Let $\mathcal{X}$ be a set of $\mathcal{T}$-algebras. The intersection of all varieties of $\mathcal{T}$-algebras containing $\mathcal{X}$ is itself a variety, called the *variety of $\mathcal{T}$-algebras generated by $\mathcal{X}$*, or simply the *variety generated by $\mathcal{X}$*. It is easy to prove that the variety generated by $\mathcal{X}$ consists of all $\mathcal{X}$-algebras that can be obtained from $\mathcal{X}$ by repeatedly forming subsemigroups, homomorphic images, and direct products. That is, the variety generated by $\mathcal{X}$ is

$$\left\{\mathrm{O}_1\,\mathrm{O}_2\cdots\mathrm{O}_n\,\mathcal{X} : n \in \mathbb{N}, \mathrm{O}_i \in \{\mathrm{Hom}, \mathrm{Sub}, \mathrm{Prod}\}\right\}. \tag{8.3}$$

LEMMA 8.3. *For any non-empty class of $\mathcal{T}$-algebras $\mathcal{X}$, we have*

$$\mathrm{Sub}\,\mathrm{Hom}\,\mathcal{X} \subseteq \mathrm{Hom}\,\mathrm{Sub}\,\mathcal{X}$$
$$\mathrm{Prod}\,\mathrm{Hom}\,\mathcal{X} \subseteq \mathrm{Hom}\,\mathrm{Prod}\,\mathcal{X}$$
$$\mathrm{Prod}\,\mathrm{Sub}\,\mathcal{X} \subseteq \mathrm{Sub}\,\mathrm{Prod}\,\mathcal{X}$$

Proof of 8.3. Let $S \in \mathrm{Sub}\,\mathrm{Hom}\,\mathcal{X}$. Then there is $\mathcal{T}$-algebra $T \in \mathcal{X}$ and a epimorphism $\varphi : T \to U$ such that S is a subalgebra of U. Let $T' = S\varphi^{-1} = \{t \in T : t\varphi \in S\}$. Then T' is a subalgebra of T and $\varphi|_{T'} : T' \to S$ is an epimorphism. So $S \in \mathrm{Hom}\,\mathrm{Sub}\,\mathcal{X}$.

Let $S \in \mathrm{Prod}\,\mathrm{Hom}\,\mathcal{X}$. Then there is a collection of $\mathcal{T}$-algebras $\{T_i : i \in I\} \subseteq \mathcal{X}$ and a collection of epimorphisms $\Phi = \{\varphi_i : T_i \to U_i : i \in I\}$ such that $S = \prod^{\times}_{i\in I} U_i$. Define a homomorphism $\psi : \prod^{\times}_{i\in I} T_i \to S$ by $(i)(x\psi) = ((i)x)\varphi_i$. Then ψ is an epimorphism since each φ_i is an epimorphism. So $S \in \mathrm{Hom}\,\mathrm{Prod}\,\mathcal{X}$.

Let $S \in \operatorname{Prod}\operatorname{Sub}\mathcal{X}$. Then there is a collection of $\mathcal{T}$-algebras $\{T_i : i \in I\} \subseteq \mathcal{X}$ and a subalgebras U_i of T_i such that $S = \prod_{i\in I}^{\times} U_i$. Then S is a subalgebra of $\prod_{i\in I}^{\times} T_i$. So $S \in \operatorname{Sub}\operatorname{Prod}\mathcal{X}$. 8.3

As an immediate consequence of Lemma 8.3 and (8.3), and the fact that the operators Hom, Sub, and Prod are idempotent, we obtain the following result:

PROPOSITION 8.4. *Let $\mathcal{X}$ be a class of $\mathcal{T}$-algebras. The variety generated by $\mathcal{X}$ is* $\operatorname{Hom}\operatorname{Sub}\operatorname{Prod}\mathcal{X}$. 8.4

PSEUDOVARIETIES

Varieties are not useful for studying and classifying finite algebras, for the simple reason that every non-trivial variety contains infinite algebras: if a variety contains an algebra S with two elements, then it contains the direct product of infinitely many copies of S, which is of course infinite.

Clearly, if we take a class $\mathcal{X}$ of finite $\mathcal{T}$-algebras, then $\operatorname{Hom}\mathcal{X}$ and $\operatorname{Sub}\mathcal{X}$ also contain only finite $\mathcal{T}$-algebras. The problem, therefore, is with the operator Prod. To modify the notion of variety in order to study finite algebras, we therefore introduce a new operator on classes of $\mathcal{T}$-algebras.

Let $\operatorname{Prod}_{\text{fin}}\mathcal{X}$ denote the class of all $\mathcal{T}$ algebras that are finitary direct products of the algebras in $\mathcal{X}$. That is,

$$\operatorname{Prod}_{\text{fin}}\mathcal{X} = \Big\{S : (\exists\{T_1,\dots,T_n\} \subseteq \mathcal{X})\big(S = T_1 \times T_2 \times \dots \times T_n\big)\Big\}.$$

A non-empty class of finite $\mathcal{T}$-algebras is a *pseudovariety* of $\mathcal{T}$-algebras if it is closed under the operations Hom, Sub, and $\operatorname{Prod}_{\text{fin}}$. That is, $\mathcal{X}$ is a variety if $\operatorname{Hom}\mathcal{X} \cup \operatorname{Sub}\mathcal{X} \cup \operatorname{Prod}_{\text{fin}}\mathcal{X} \subseteq \mathcal{X}$.

EXAMPLES 8.5. a) Let 1 consist only of the trivial semigroup $E = \{e\}$. Then 1 is a pseudovariety, since the only subsemigroup of E is E itself, the only homomorphic image of E is E itself, and any finitary direct product of copies of E is isomorphic to E.

b) Let Com consist of all finite commutative semigroups (viewed as $\{(\circ,2)\}$-algebras). Then C is a pseudovariety.

c) Let G consist of all finite groups, viewed as $\{(\circ,2),(1_G,0),({}^{-1},1)\}$-algebras; then G is a pseudovariety.

Notice that the class of all finite groups viewed as $\{(\circ,2)\}$ algebras *is* a pseudovariety, because in this case subalgebras are subgroups (since if $x^n = 1_G$ then $x^{-1} = x^{n-1}$).

d) Let I consist of all finite inverse semigroups, viewed as $\{(\circ,2),({}^{-1},1)\}$-algebras. Then I is a pseudovariety.

e) Let N consist of all finite nilpotent semigroups. Then N is a pseudovariety.

f) Let A consist of all finite aperiodic semigroups. Then A is a pseudovariety. Notice that $\mathsf{N} \subseteq \mathsf{A}$.

g) Let S consist of all finite semigroups. Then S is a pseudovariety.

Notice that we are using the same symbols for certain varieties and pseudovarieties: for instance, Com denotes both the variety of commutative semigroups and the pseudovariety of finite commutative semigroups. This will not cause confusion, because from now on we will only use them to denote pseudovarieties.

Just as with varieties, we have the idea of generating a pseudovariety of finite $\mathcal{T}$-algebras. Let $\mathcal{X}$ be a set of finite $\mathcal{T}$-algebras. The intersection of all pseudovarieties of $\mathcal{T}$-algebras containing $\mathcal{X}$ is itself a pseudovariety, called the *pseudovariety of finite $\mathcal{T}$-algebras generated by $\mathcal{X}$*, or simply the *pseudovariety generated by $\mathcal{X}$*. It is easy to prove that the pseudovariety generated by $\mathcal{X}$ consists of all (necessarily finite) $\mathcal{X}$-algebras that can be obtained from $\mathcal{X}$ by repeatedly forming subsemigroups, homomorphic images, and finitary direct products. That is, the variety generated by $\mathcal{X}$ is

$$\left\{\mathrm{O}_1 \mathrm{O}_2 \cdots \mathrm{O}_n \mathcal{X} : n \in \mathbb{N}, \mathrm{O}_i \in \left\{\mathrm{Hom}, \mathrm{Sub}, \mathrm{Prod}_{\mathrm{fin}}\right\}\right\}. \tag{8.4}$$

We have the following analogy of Proposition 8.4:

PROPOSITION 8.6. *Let $\mathcal{X}$ be a class of $\mathcal{T}$-algebras. The pseudovariety generated by $\mathcal{X}$ is* $\mathrm{Hom}\,\mathrm{Sub}\,\mathrm{Prod}_{\mathrm{fin}}\,\mathcal{X}$.

Proof of 8.6. For any non-empty class of $\mathcal{T}$-algebras $\mathcal{X}$, we have

$$\mathrm{Prod}_{\mathrm{fin}}\,\mathrm{Hom}\,\mathcal{X} \subseteq \mathrm{Hom}\,\mathrm{Prod}_{\mathrm{fin}}\,\mathcal{X}$$
$$\mathrm{Prod}_{\mathrm{fin}}\,\mathrm{Sub}\,\mathcal{X} \subseteq \mathrm{Sub}\,\mathrm{Prod}_{\mathrm{fin}}\,\mathcal{X};$$

to see this, follow the reasoning in the proof of Lemma 8.3, restricting the index sets I to be finite. The result follows immediately. 8.6

PSEUDOVARIETIES OF SEMIGROUPS

From this point onwards, we will deal only with pseudovarieties of semigroups. All pseudovarieties will have type $\{(\circ, 2)\}$.

Notice that pseudovarieties are closed under division: if V is a pseudovariety, $T \in \mathsf{V}$, and $S \prec V$, then by definition there is an epimorphism $\varphi : T' \to S$, where T' is a subsemigroup of T; hence $S \in \mathrm{Hom}\,\mathrm{Sub}\,\mathsf{V} = \mathsf{V}$.

Semidirect product of pseudovarieties

The *semidirect product* of two pseudovarieties V and W, denoted $\mathsf{V} \rtimes \mathsf{W}$, is the pseudovariety generated by all semidirect products $S \rtimes_\varphi T$, where

$S \in \mathsf{V}$, $T \in \mathsf{W}$, and $\varphi : T \to \mathrm{End}(S)$ is a homomorphism. Our goal is to show that $\rtimes$ is an associative operation on the class of pseudovarieties; this contrasts the fact that $\rtimes$ is not associative on the class of semigroups.

Transformation semigroups

In order to prove this, we need to introduce some new concepts. A *transformation semigroup* is a pair (P, S) where P is a set and S embeds into $\mathcal{T}_P$ via a monomorphism $\alpha : S \to \mathcal{T}_P$. Let (P, S) and (Q, T) be transformation semigroups with embedding maps $\alpha : S \to \mathcal{T}_P$ and $\beta : T \to \mathcal{T}_Q$. The *wreath product of transformation semigroups* (P, S) and (Q, T), denoted $(P, S) \wr (Q, T)$, is the transformation semigroup $(P \times Q, S^Q \rtimes_\varphi T)$, where $\varphi : T \to \mathrm{End}(S^Q)$ is defined by $(q)f^t = (q(t\beta))f$, where, as with the wreath product of semigroups, we write f^t for $f(t\varphi)$. The embedding map $\delta : S^Q \rtimes_\varphi T \to \mathcal{T}_{P\times Q}$ is defined by

$$[p, q](f, t)\delta = [p(((q)f)\alpha), q(t\beta)].$$

(For clarity, we use square brackets for elements of the set $P \times Q$.) We must check that δ is a monomorphism. First,

$$\begin{aligned}
&(f_1, t_1)\delta = (f_2, t_2)\delta \\
\Rightarrow\ &(\forall [p, q] \in P \times Q)\big([p, q](f_1, t_1)\delta = [p, q](f_2, t_2)\delta\big) \\
\Rightarrow\ &(\forall [p, q] \in P \times Q)\big([p(((q)f_1)\alpha), q(t_1\beta)] = [p(((q)f_2)\alpha), q(t_2\beta)]\big) \\
\Rightarrow\ &(\forall [p, q] \in P \times Q)\big(p(((q)f_1)\alpha) = p(((q)f_2)\alpha) \wedge q(t_1\beta) = q(t_2\beta)\big) \\
\Rightarrow\ &(\forall q \in Q)\big(((q)f_1)\alpha = ((q)f_2)\alpha \wedge t_1\beta = t_2\beta\big) \\
\Rightarrow\ &(\forall q \in Q)\big((q)f_1 = (q)f_2 \wedge t_1 = t_2\big) \qquad \text{[since } \alpha \text{ and } \beta \text{ are injective]} \\
\Rightarrow\ &f_1 = f_2 \wedge t_1 = t_2 \\
\Rightarrow\ &(f_1, t_1) = (f_2, t_2);
\end{aligned}$$

thus δ is injective. Second

$$\begin{aligned}
&[p, q]\big((f_1, t_1)(f_2, t_2)\big)\delta \\
&= [p, q]\big(f_1 f_2^{t_1}, t_1 t_2\big)\delta \\
&= [p(((q)f_1 f_2^{t_1})\alpha), q((t_1 t_2)\beta)] \\
&= [p(((q)f_1(q(t_1\beta))f_2)\alpha), q((t_1 t_2)\beta)] \\
&= [p(((q)f_1)\alpha)(((q(t_1\beta))f_2)\alpha), q(t_1\beta)(t_2\beta)] \\
&\qquad\qquad \text{[since } \alpha \text{ and } \beta \text{ are homomorphisms]} \\
&= [p(((q)f_1)\alpha), q(t_1\beta)](f_2, t_2)\delta \\
&= [p, q](f_1, t_1)\delta(f_2, t_2)\delta;
\end{aligned}$$

thus δ is a homomorphism.

A homomorphism between two transformation semigroups (P, S) and (Q, T) with embedding maps $\alpha : S \to \mathcal{T}_P$ and $\beta : T \to \mathcal{T}_Q$ is a pair (φ, ψ), where $\varphi : P \to Q$ is a map and $\psi : S \to T$ is a homomorphism

such that $p(s\alpha)\varphi = (p\varphi)(s\psi\beta)$, or, equivalently, such that the following diagram commutes

$$\begin{array}{ccc} P & \xrightarrow{s\alpha} & P \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \hat{\varphi}} \\ Q & \xrightarrow{s\psi\beta} & Q \end{array} \tag{8.5}$$

An isomorphism between transformation semigroups (P, S) and (Q, T) is a homomorphism (φ, ψ) where both φ and ψ are bijective.

LEMMA 8.7. *For any three transformation semigroups* (P, S), (Q, T), *and* (R, U), *the wreath products*

$$\big((P, S) \wr (Q, T)\big) \wr (R, U) \text{ and } (P, S) \wr \big((Q, T) \wr (R, U)\big)$$

are isomorphic.

Proof of 8.7. Suppose that the transformation semigroups (P, S), (Q, T), and (R, U) have embedding maps $\alpha : S \to \mathcal{T}_P$, $\beta : T \to \mathcal{T}_Q$, and $\gamma : U \to \mathcal{T}_R$. We have to show that the transformation semigroups

$$\big((P \times Q) \times R, (S^Q \rtimes T)^R \rtimes U\big) \text{ and } \big(P \times (Q \times R), S^{Q\times R} \rtimes (T^R \times U)\big)$$

are isomorphic. Let these transformation semigroups have embedding maps ζ and η, respectively, and let the transformation semigroup $(P, S) \wr (Q, T)$ (that is, $(P \times Q, S^Q \rtimes T)$) have embedding map δ.

Define a map $\varphi : (P\times Q)\times R \to P\times(Q\times R)$ by $[[p, q], r]\varphi = [p, [q, r]]$. Define a map $\psi : (S^Q \rtimes T)^R \rtimes U \to S^{Q\times R} \rtimes (T^R \times U)$ as follows. For $f \in (S^Q \times T)^R$ and $u \in U$, define $(f, u)\psi = (g, (h, u))$, where $g \in S^{Q\times R}$ and $h \in T^R$ are such that $[p, q]((r)f)\delta = [p(([\_, r]g)\alpha), q(((r)h)\beta)]$ for any $[p, q] \in Q \times R$ and $r \in R$.

Then for $p \in P$, $q \in Q$, $r \in R$, $f \in (S^Q \rtimes T)^R$, $u \in U$, we have

$$\begin{aligned} &[[p, q], r](f, u)\zeta \\ &= [[p, q](((r)f)\delta), r(u\gamma)] \\ &= \big[[p(([q, r]g)\alpha), q(((r)h)\beta)], r(u\gamma)\big], \end{aligned}$$

while

$$[p, [q, r]](g, (h, u))\eta = \big[p(([q, r]g)\alpha), q(((r)h)\beta), r(u\gamma)\big];$$

thus $x(s\zeta)\varphi = (x\varphi)(s\psi\eta)$ for all $x \in (P \times Q) \times R$ and $s \in (S^Q \rtimes T)^R \rtimes U$; that is, the diagram (8.5) commutes.

Now let $f, f' \in (S^Q \rtimes T)^R$ and $u, u' \in U$. Then

$$\begin{aligned} &[p, q]((r)ff'^u)\delta \\ &= [p, q]((r)f(r(u\gamma))f')\delta \end{aligned}$$

$$
\begin{aligned}
&= [p,q]((r)f)\delta((r(u\gamma))f')\delta \\
&= [p(([\_,r]g)\alpha), q(((r)h)\beta)]((r(u\gamma))f')\delta \\
&= [p(([\_,r]g)\alpha(([\_,r(u\gamma)]g')\alpha), q(((r)h)\beta)(((r(u\gamma))h')\beta)] \\
&= [p(([\_,r]g[\_,r(u\gamma)]g')\alpha), q(((r)h(r(u\gamma))h')\beta)] \\
&= [p(([\_,r]g[\_(((r)h)\beta),r(u\gamma)]g')\alpha), q(((r)h(r(u\gamma))h')\beta)] \\
&= [p(([\_,r]g[\_,r]g'^{(h,u)})\alpha), q(((r)h(r)h'^{u})\beta)] \\
&= [p(([\_,r]gg'^{(h,u)})\alpha), q(((r)hh'^{u})\beta)];
\end{aligned}
$$

combine this with the definition of δ to see that ψ is a homomorphism.

The map φ and ψ are clearly bijective from their definitions. Hence (φ, ψ) is an isomorphism. 8.7

Direct product of semidirect products = semidirect product of direct products

LEMMA 8.8. *Let S_1, S_2, T_1, T_2 be semigroups and let $\varphi_1 : T_1 \to \operatorname{End} S_1$ and $\varphi_2 : T_2 \to \operatorname{End} S_2$ be homomorphisms. Then*

$$(S_1 \rtimes_{\varphi_1} T_1) \times (S_2 \rtimes_{\varphi_2} T_2) \simeq (S_1 \times S_2) \rtimes_{\psi} (T_1 \times T_2),$$

where the left action of $T_1 \times T_2$ on $S_1 \times S_2$ is defined by

$${}^{(t_1,t_2)}(s_1, s_2) = \left({}^{t_1}s_1, {}^{t_2}s_2\right).$$

Proof of 8.8. Define a map $\vartheta : (S_1 \rtimes_{\varphi_1} T_1) \times (S_2 \rtimes_{\varphi_2} T_2) \to (S_1 \times S_2) \rtimes_{\psi} (T_1 \times T_2)$ by $((s_1,t_1),(s_2,t_2))\vartheta = ((s_1,s_2),(t_1,t_2))$. Clearly, ϑ is a bijection. Furthermore,

$$
\begin{aligned}
&\big[\big((s_1,t_1),(s_2,t_2)\big)\big((s_1',t_1'),(s_2',t_2')\big)\big]\vartheta \\
&= \big[\big((s_1,t_1)(s_1',t_1'),(s_2,t_2)(s_2',t_2')\big)\big]\vartheta \\
&\qquad \text{[multiplication in the direct product } (S_1 \ltimes_{\varphi_1} T_1) \times (S_2 \ltimes_{\varphi_2} T_2)\text{]} \\
&= \big[\big(s_1\,{}^{t_1}s_1', t_1t_1'\big), \big(s_2\,{}^{t_2}s_2', t_2t_2'\big)\big]\vartheta \\
&\qquad \text{[multiplication in the semidirect products } (S_1 \rtimes_{\varphi_1} T_1) \text{ and } (S_2 \rtimes_{\varphi_2} T_2)\text{]} \\
&= \big(\big(s_1\,{}^{t_1}s_1', s_2\,{}^{t_2}s_2'\big), (t_1t_1', t_2t_2')\big) \qquad \text{[by definition of } \vartheta\text{]} \\
&= \big((s_1,s_2)({}^{t_1}s_1', {}^{t_2}s_2'), \big(t_1,t_2\big)(t_1',t_2')\big) \\
&\qquad \text{[factoring in the direct products } (S_1 \times S_2) \text{ and } (T_1 \times T_2)\text{]} \\
&= \big((s_1,s_2)\,{}^{(t_1,t_2)}(s_1',s_2')\big), (t_1,t_2)(t_1',t_2')\big) \\
&\qquad \text{[definition of the action of } T_1 \times T_2 \text{ on } S_1 \times S_2\text{]} \\
&= \big((s_1,s_2),(t_1,t_2)\big)\big[(s_1',s_2')(t_1',t_2')\big) \\
&\qquad \text{[factoring in the semidirect product } (S_1 \times S_2) \rtimes_{\psi} (T_1 \times T_2)\text{]} \\
&= \big[\big((s_1,t_1),(s_2,t_2)\big)\vartheta\big]\big[\big((s_1',t_1'),(s_2',t_2')\big)\vartheta\big];
\end{aligned}
$$

thus ϑ is a homomorphism and so an isomorphism. 8.8

LEMMA 8.9. *Let* V *and* W *be pseudovarieties. Then* $\mathsf{V} \rtimes \mathsf{W}$ *is the class of all semigroups that divide a semidirect product* $S \rtimes_\varphi T$*, where* $S \in \mathsf{V}$ *and* $T \in \mathsf{W}$.

Proof of 8.9. Let $\mathcal{X} = \{S \rtimes_\varphi T : S \in \mathsf{V}, T \in \mathsf{W}\}$. So $\mathsf{V} \rtimes \mathsf{W}$ is, by definition, the pseudovariety generated by $\mathcal{X}$; hence $\mathsf{V} \rtimes \mathsf{W} = \operatorname{Hom}\operatorname{Sub}\operatorname{Prod}_{\text{fin}} \mathcal{X}$ by Proposition 8.6.

Let $U \in \operatorname{Prod}_{\text{fin}} \mathcal{X}$. So

$$U = \prod_{i \in I} \left(S_i \rtimes_{\varphi_i} T_i\right)$$

where each $S_i \rtimes_{\varphi_i} T_i$ is in $\mathcal{X}$ and I is a finite index set. By Lemma 8.8,

$$U \simeq \left(\prod_{i \in I} S_i\right) \rtimes_\psi \left(\prod_{i \in I} T_i\right).$$

Now, each S_i lies in V and each T_i lies in W. But V and W are closed under finitary direct products, so $\prod_{i \in I} S_i \in \mathsf{V}$ and $\prod_{i \in I} T_i \in \mathsf{W}$. Hence $U \in \mathcal{X}$. Thus $\operatorname{Prod}_{\text{fin}} \mathcal{X} \subseteq \mathcal{X}$. The opposite inclusion is obvious, so $\operatorname{Prod}_{\text{fin}} \mathcal{X} = \mathcal{X}$.

Therefore $\mathsf{V} \rtimes \mathsf{W} = \operatorname{Hom}\operatorname{Sub} \mathcal{X}$, and so $\mathsf{V} \rtimes \mathsf{W}$ consists of all divisors of semidirect products $S \rtimes_\varphi T$, where $S \in \mathsf{V}$ and $T \in \mathsf{W}$. 8.9

LEMMA 8.10. *Let* V *and* W *be pseudovarieties. Then* $\mathsf{V} \rtimes \mathsf{W}$ *is the class of all semigroups that divide a wreath product* $(P, S) \wr (Q, T)$ *(that is, that divide* $S^Q \rtimes T$*), where* $S \in \mathsf{V}$ *and* $T \in \mathsf{W}$.

Proof of 8.10. Let $S \in \mathsf{V}$ and $T \in \mathsf{W}$. Then $S^Q \in \operatorname{Prod}_{\text{fin}} \mathsf{V} = \mathsf{V}$ and so $S^Q \rtimes T \in \mathsf{V} \rtimes \mathsf{W}$. Hence all divisors of $S^Q \rtimes T$ lie in $\mathsf{V} \rtimes \mathsf{W}$.

Now let $U \in \mathsf{V} \rtimes \mathsf{W}$. Then by Lemma 8.9, U divides a semidirect product $S \rtimes_\varphi T$, where $S \in \mathsf{V}$ and $T \in \mathsf{W}$. For each $s \in S$, let $f_s : T^1 \to S$ be the map $(x)f_s = s(x\varphi)$. Let $\psi : S \rtimes_\varphi T \to S^{T^1} \rtimes T$ be defined by $(s,t)\psi = (f_s, t)$. We view $S^{T^1} \rtimes T$ as the semigroup of the wreath product of transformation semigroups $(S^1, S) \wr (T^1, T)$. Then

$$\begin{aligned}
&(s,t)\psi(s',t')\psi \\
&= (f_s, t)(f_{s'}, t') \\
&= (f_s f_{s'}^t, tt') \\
&= (f_{s(s'(t\varphi))}, tt') \\
&= (s(s'(t\varphi)), tt')\psi \\
&= \big((s,t)(s',t')\big)\psi,
\end{aligned}$$

since

$$\begin{aligned}
&(x)f_s f_{s'}^t \\
&= (x)f_s (x)f_{s'}^t
\end{aligned}$$

$$
\begin{aligned}
&= s(x\varphi)s'(xt\varphi)\\
&= s(x\varphi)s'(t\varphi)(x\varphi)\\
&= s(s'(t\varphi))(x\varphi)\\
&= (x)f_{s(s'(t\varphi))}\\
&= (x)f_{ss't}.
\end{aligned}
$$

Thus ψ is a homomorphism. Furthermore,

$$
\begin{aligned}
&(s,t)\psi = (s',t')\psi\\
\Rightarrow\ &(f_s,t) = (f_{s'},t')\\
\Rightarrow\ &f_s = f_{s'} \wedge t = t'\\
\Rightarrow\ &(1)f_s = (1)f_{s'} \wedge t = t'\\
\Rightarrow\ &s(1\varphi) = s'(1\varphi) \wedge t = t'\\
\Rightarrow\ &s\,\mathrm{id}_S = s'\,\mathrm{id}_S \wedge t = t'\\
\Rightarrow\ &s = s' \wedge t = t'\\
\Rightarrow\ &(s,t) = (s',t').
\end{aligned}
$$

So ψ is a monomorphism, and hence ψ^{-1} is a homomorphism from $\operatorname{im}\psi$ to $S \rtimes_\varphi T$. Hence $S \rtimes_\varphi T$ divides the wreath product of transformation semigroups $(S^1, S) \wr (T^1, T)$. Thus, by the transitivity of divisibility, U divides the wreath product of transformation semigroups $(S^1, S) \wr (T^1, T)$ 8.10

PROPOSITION 8.11. *The semidirect product of pseudovarieties is associative.*

Proof of 8.11. This following immediately from Lemma 8.10. 8.11

The Krohn–Rhodes theorem shows that every finite semigroup is a wreath product of its subgroups and copies of the aperiodic semigroup U_3. Now, if V and W are pseudovarieties and $S \in \mathsf{V}$ and $T \in \mathsf{W}$, then $S^T \in \mathsf{V}$ (since V is closed under finitary direct products); hence $S \wr T \in \mathsf{V} \rtimes \mathsf{W}$. Notice furthermore that $\mathsf{V} \subseteq \mathsf{V} \rtimes \mathsf{W}$ since every pseudovariety contains the trivial semigroup. Therefore the Krohn–Rhodes theorem can be restated in terms of pseudovarieties as

$$
\mathsf{S} = \bigcup_{i=0}^{n} \Big(\mathsf{G} \rtimes \prod_{j=0}^{n} \big(\mathsf{A} \rtimes \mathsf{G} \big) \Big).
$$

Let V and W be pseudovarieties of semigroups. Let $\mathsf{V} \vee \mathsf{W}$ be the pseudovariety generated by $\mathsf{V} \cup \mathsf{W}$. Let $\mathsf{V} \wedge \mathsf{W}$ be $\mathsf{V} \cap \mathsf{W}$; it is easy to prove that $\mathsf{V} \wedge \mathsf{W}$ is a pseudovariety.

PROPOSITION 8.12. *The class of pseudovarieties of semigroups is a lattice with operations meet $\wedge$ and join $\vee$.* 8.12

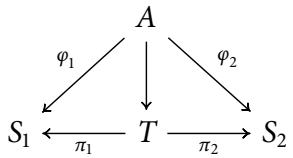
FREE OBJECTS FOR PSEUDOVARIETIES

If we want to follow the same path for pseudovarieties as for varieties, our next step should be to construct a 'free V-semigroup' for each pseudovariety V, and then to devise an analogue of laws and prove an analogue of Birkhoff's theorem. However, this is much more difficult for pseudovarieties than for varieties, for a very simple reason: free objects are usually infinite.

Consider the pseudovariety N of nilpotent semigroups. For any finite alphabet A, let $I_n = \{w \in A^+ : |w| \geq n\}$. Then A^+/I_n is a nilpotent semigroup; thus $A^+/I_n \in \mathsf{N}$. Thus N contains arbitrarily large A-generated semigroups. Since an A-generated free object for N must map surjectively onto each of these semigroups, it is clear that no semigroup in N is free.

If we try to approach the idea of a free object through laws, we encounter another problem. It is clear that A^+/I_n satisfies no law in at most $|A|$ variables where the two sides of the law have length less than n. So if we try to base our free objects on laws, all pseudovarieties containing N will have the same free object.

Let us look at free objects from another direction. The idea is that a free A-generated object for a class $\mathcal{X}$ should be just general enough to be more general than any A-generated object in $\mathcal{X}$. Suppose we take two semigroups S_1 and S_2 in a pseudovariety V. Let $\varphi_1 : A \to S_1$ and $\varphi_2 : A \to S_2$ be functions such that im φ_1 generates S_1 and im φ_2 generates S_2. Let T be the subsemigroup of $S_1 \times S_2$ generated by $\{(a\varphi_1, a\varphi_2) : a \in A\}$. Then T is A-generated and lies in V, since V is closed under $\mathrm{Prod}_{\mathrm{fin}}$ and Sub. Furthermore, the following diagram commutes:



Thus T is more general than both S_1 and S_2 as an A-generated member of V. Furthermore, T is the smallest such member of V. We could iterate this process, but, as our discussion of N shows, we will never find an element of V that is more general than all other members of V. A limiting process is needed.

PROJECTIVE SYSTEMS AND LIMITS

A partially ordered set $(I, \leq)$ is a *directed set* if every pair of elements of I have an upper bound. [Notice that a partially ordered

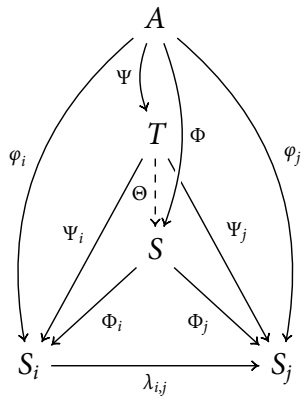


FIGURE 8.1
Property 2) of the projective limit of $\{\varphi_i : A \to S_i : i \in I\}$ with connecting homomorphisms $\lambda_{i,j}$.

set is not necessarily a join semilattice, because some pairs of elements might not have *least* upper bounds.]

A *topological semigroup* is a semigroup equipped with a topology such that the multiplication operation is a continuous mapping. Any semigroup can be equipped with the discrete topology and thus becomes a topological semigroup.

For any alphabet A, an *A-generated topological semigroup* is a pair (S, φ), where S is a topological semigroup and $\varphi : A \to S$ is a map such that $\operatorname{im} \varphi$ generates a dense subsemigroup of S. We will often denote such an A-generated topological semigroup by the map $\varphi : A \to S$. A homomorphism between A-generated topological semigroups $\varphi_1 : A \to S_1$ and $\varphi_2 : A \to S_2$ is a continuous homomorphism $\psi : S_1 \to S_2$ such that $\varphi_1\psi = \varphi_2$.

A *projective system* is a collection of A-generated topological semigroups $\{\varphi_i : A \to S_i : i \in I\}$, where I is a directed set, such that for all $i, j \in I$ with $i \geq j$ there is a *connecting homomorphism* $\lambda_{i,j}$ from $\varphi_i : A \to S_i$ to $\varphi_j : A \to S_j$ satisfying the following properties: for each $i \in I$, the homomorphism $\lambda_{i,i}$ is the identity map; for all $i, j, k \in I$ with $i \geq j \geq k$, we have $\lambda_{i,j}\lambda_{j,k} = \lambda_{i,k}$.

The *projective limit* of this projective system is an A-generated topological semigroup $\Phi : A \to S$ equipped with homomorphisms Φ_i from $\Phi : A \to S$ to $\varphi_i : A \to S_i$. such that the following properties hold:

1. for all $i, j \in I$ with $i \geq j$, we have $\Phi_i\lambda_{i,j} = \Phi_j$
2. if there is another A-generated topological semigroup $\Psi : A \to T$ and homomorphisms Ψ_i from $\Psi : A \to T$ to $\varphi_i : A \to S$ such that for all $i, j \in I$ with $i \geq j$, we have $\Psi_i\lambda_{i,j} = \Psi_j$, there exists a homomorphism Θ from $\Psi : A \to T$ to $\Phi : A \to S$ such that $\Theta\Phi_i = \Psi_i$. That is, the diagram in Figure 8.1 commutes.

Let us first show that the projective limit is unique (up to isomorphism); we will then show that it exists. Suppose $\Phi : A \to S$ and $\Phi' : A \to$

S' are both projective limits of the projective system $\{\varphi_i : A \to S_i : i \in I\}$. By property 2) above, there are homomorphisms Θ from $\Phi : A \to S$ to $\Phi' : A \to S'$ and Θ' from $\Phi' : A \to S'$ to $\Phi : A \to S$. Thus we have $\Phi\Theta\Theta' = \Phi$ and $\Phi'\Theta'\Theta = \Phi'$; hence $\Theta\Theta'|_{A\Phi} = \mathrm{id}_{A\Phi}$ and $\Theta'\Theta|_{A\Phi'} = \mathrm{id}_{A\Phi'}$. Hence $\Theta\Theta'$ restricted to the subsemigroup generated by $A\Phi$ is the identity map; since this subsemigroup is dense in S and Θ and Θ' are continuous, we have $\Theta\Theta' = \mathrm{id}_S$. Similarly $\Theta'\Theta = \mathrm{id}_{S'}$. So Θ and Θ' are mutually inverse isomorphisms between $\Phi : A \to S$ and $\Phi' : A \to S'$.

In order to construct the projective limit, we proceed as follows. Let S be the subset of the direct product $\prod_{i\in I} S_i$ consisting of all elements $(s_i)_{i\in I}$ with $s_i\lambda_{i,j} = s_j$ for all $i, j \in I$ with $i \geq j$. Notice that

$$\begin{aligned}
&(s_i)_{i\in I}, (t_i)_{i\in I} \in S \\
\Rightarrow\ &(\forall i, j \in I)\big(i \geq j \Rightarrow (s_i\lambda_{i,j} = s_j \wedge t_i\lambda_{i,j} = t_j)\big) \\
\Rightarrow\ &(\forall i, j \in I)\big(i \geq j \Rightarrow (s_i\lambda_{i,j}t_i\lambda_{i,j} = s_jt_j)\big) \\
\Rightarrow\ &(\forall i, j \in I)\big(i \geq j \Rightarrow ((s_it_i)\lambda_{i,j} = s_jt_j)\big) \\
\Rightarrow\ &(s_it_i)_{i\in I} \in S;
\end{aligned}$$

thus S is a subsemigroup of $\prod_{i\in I} S_i$. Furthermore, the S is equipped with the induced topology from the product topology on $\prod_{i\in I} S_i$. Let $\Phi : A \to S$ be defined by $a\Phi = (a\varphi_i)_{i\in I}$. For each $i \in I$, let Φ_i be the projection homomorphism from S to S_i.

PROPOSITION 8.13. *$\Phi : A \to S$ is an A-generated topological semigroup and satisfies the properties 1) and 2) above. Hence $\Phi : A \to S$ is a projective limit.*

Proof of 8.13. We first have to show that $A\Phi$ generates a dense subsemigroup of S. Since the topology of S is induced by the product topology on $\prod_{i\in I} S_i$, we can work with the product topology instead. Let $(s_i)_{i\in I} \in S$. Let K be a neighbourhood of $(s_i)_{i\in I}$. Assume without loss that K is an open set (in the product topology). Thus $K = \prod_{i\in I} K_i$, where each $K_i \subseteq S_i$ is open and $K_i = S_i$ for all but finitely many $i \in I$. Let $i_j \in I$ (where $j = 1, \ldots, n$) be the indices for which $K_{i_j} \neq \varnothing$.

Let h be an upper bound for $\{i_j : j = 1, \ldots, n\}$; such an h exists because I is a directed set. Let $L = \bigcap_{j=1}^{n} K_{i_j}\lambda_{h,i_j}^{-1} \subseteq S_h$. Notice that $s_h \in s_{i_j}\lambda_{h,i_j}^{-1}$ for all $j = 1, \ldots, n$, so L contains s_h and is thus non-empty. Furthermore, L is an intersection of open sets because each $\lambda_{i,j}$ is continuous and each K_{i_j} is open; hence L is itself open. Since $A\varphi_h$ generates a dense subset of S_h, the set there is a word $w \in A^+$ such that $w\varphi_h \in L$. Let $(t_i)_{i\in I} = w\Phi$. Thus $t_i = w\varphi_i$ for all $i \in I$. For $j = 1, \ldots, n$, we have

$$t_{i_j} = w\varphi_{i_j} = w\varphi_k\lambda_{k,i_j} \in L\lambda_{k,i_j} \subseteq K_{i_j}.$$

Hence $w\Phi = (t_i)_{i\in I} \in K$. Therefore $A\Phi$ generates a dense subset of S.

Since S consists of elements $(s_i)_{i\in I}$ with $s_i\lambda_{i,j} = s_j$, it is immediate that $\Phi_i\lambda_{i,j} = \Phi_j$; hence $\Phi : A \to S$ satisfies property 1).

Now let $\Psi : A \to T$ be an A-generated topological semigroup as described in property b). Define $\Theta : T \to S$ by $t\Theta = (t\Psi_i)_{i\in I}$. (Note that $(t\Psi_i)_{i\in I} \in S$ since $\Psi_i\lambda_{i,j} = \Psi_j$.) Then this map is a continuous homorphism since each Ψ_i is continuous. Finally, $\Theta\Phi_i = \Theta\pi_i = \Psi_i$. So $\Phi : A \to S$ satisfies property 2). 8.13

Notice that if all of the S_i are compact, so is $\prod_{i\in I} S_i$ by Tychonoff's theorem. Furthermore, since each $\lambda_{i,j}$ is continuous and the condition $s_i\lambda_{i,j} = s_j$ involves only two components of the product, S is closed in the $\prod_{i\in I} S_i$. Hence if all the S_i are compact, S is also compact.

Any finite semigroup is a topological semigroup with the discrete topology. A *profinite semigroup* is a projective limit of a projective system of finite semigroups for some suitable choice of generators.

Notice that any finite semigroup is [isomorphic to] a profinite semigroup. To see this, let S be a finite semigroup. Now take all the semigroups S_i in the projective system to be isomorphic to S; every connecting homomorphism $\lambda_{i,j}$ is the identity map. It is easy to see that the projective limit of this projective system is isomorphic to S.

A semigroup S is *residually finite as a topological semigroup* if, for any $x, y \in S$ with $x \neq y$, there is a finite semigroup $T_{x,y}$ and a continuous homomorphism $\varphi_{x,y} : S \to T_{x,y}$ such that $x\varphi_{x,y} \neq y\varphi_{x,y}$.

PROPOSITION 8.14. *Let S be a compact topological semigroup. The following are equivalent:*

a) *S is profinite;*

b) *S is residually finite as a topological semigroup;*

c) *S is a closed subdirect product of finite semigroups.*

Proof of 8.14. First part [a) ⇒ b)]. Let S be profinite. Then S arises as a projective limit $\Phi : A \to S$ of some projective system of topological semigroups $\varphi_i : A \to S_i$. Let $(x_i)_{i\in I}$ and $(y_i)_{i\in I}$ be distinct elements of S. Then $x_j \neq y_j$ for some $j \in I$. Then $(x_i)_{i\in I}\Phi_j \neq (y_i)_{i\in I}\Phi_j$.

Second part [b) ⇒ c)]. For each $x, y \in S$ with $x \neq y$, let $T_{x,y}$ be finite and $\varphi_{x,y} : S \to T_{x,y}$ be a continuous homomorphism such that $x\varphi_{x,y} \neq y\varphi_{x,y}$. Without loss of generality, assume each $\varphi_{x,y}$ is an epimorphism. Then the collection of these epimorphisms separates the elements of S and so S is a subdirect product of the finite semigroups $T_{x,y}$ by Proposition 1.29. Finally, S is closed since it is an intersection of closed subsets (the preimages of the continuous projections to each each $T_{x,y}$).

Third part [c) ⇒ a)]. Suppose S is a closed subdirect product of $\{T_i : i \in I\}$. Let $\Phi : S \to \prod_{i\in I} T_i$ be an injective continuous homomorphism such that $\Phi\pi_i : S \to T_i$ is surjective for each $i \in I$. For every finite subset F of I, let $S_F = \prod_{i\in F} T_i$; let $\pi_F : \prod_{i\in I} T_i \to S_F$ be the natural projection map, and let

$\Phi_F : S \to S_F$ be such that $\Phi_F = \Phi\pi_F$. Let J be the set of all finite subsets of I; with the inclusion ordering, J is a directed set. For $F, G \in J$ with $F \supseteq G$, let $\lambda_{F,G} : S_F \to S_G$ be the natural projection mapping. Then the finite semigroups S_F form a projective system of S-generated semigroups. It is easy to see that the projective limit is S. 8.14

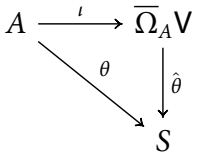
COROLLARY 8.15. *A closed subsemigroup of a profinite semigroup is itself profinite.*

PRO-V SEMIGROUPS

Let V be a pseudovariety. A profinite semigroup S is *pro-*V if it is a projective limit of a projective system made up of members of V.

Let us return of the problem of finding a free object for V. For a generating set A, the idea is to take the projective limit of the projective containing every A-generated semigroup in V. (Strictly speaking, we take one semigroup from every isomorphism class in V.) The projective limit of this system is denoted $\overline{\Omega}_A\mathsf{V}$. If the A-generated semigroups in V are $\{\varphi_i : A \to S_i : i \in I\}$, then there is a natural map $\iota : A \to \overline{\Omega}_A\mathsf{V}$ given by $a\iota = (a\varphi_i)_{i\in I}$. (This is the map Φ in the discussion of the projective limit above.) Denote by $\Omega_A\mathsf{V}$ the [dense] subsemigroup of $\overline{\Omega}_A\mathsf{V}$ generated by $A\iota$.

PROPOSITION 8.16. *The profinite semigroup $\overline{\Omega}_A\mathsf{V}$ is a free object for A-generated pro-*V *semigroups. That is, for any pro-*V *semigroup S and map $\theta : A \to S$, there is a unique continuous homomorphism $\hat{\theta} : \overline{\Omega}_A\mathsf{V} \to A$ such that $\iota\hat{\theta} = \theta$; that is, such that the following diagram commutes:*



Proof of 8.16. Since pro-V semigroups are subdirect products of members of V, it is sufficient to consider the case when S lies in V. Without loss of generality, assume S is generated by $A\theta$. Then S is [isomorphic to] an A-generated semigroup in V; that is, S is [isomorphic to] one of the A-generated semigroups $\varphi_j : A \to S_j$ in the projective system whose projective limit is $\overline{\Omega}_A\mathsf{V}$. Let $\hat{\theta}$ be the projection $\pi_j : \overline{\Omega}_A\mathsf{V} \to S_j \simeq S$. Finally, we have to show that $\hat{\theta}$ is the *unique* continuous homomorphism with this property. Let $\psi : \overline{\Omega}_A\mathsf{V} \to S$ be some continuous homomorphism with

$\iota\psi = \theta$. Since $\iota\hat{\theta} = \theta$, we see that $\psi|_{A\iota} = \hat{\theta}|_{A\iota}$ and hence, since $A\iota$ generates $\Omega_A\mathsf{V}$, we have $\psi|_{\Omega_A\mathsf{V}} = \hat{\theta}|_{\Omega_A\mathsf{V}}$. Since $\Omega_A\mathsf{V}$ is dense in $\overline{\Omega}_A\mathsf{V}$ and ψ is continuous, we have $\psi = \hat{\theta}$. 8.16

In light of Proposition 8.16, we call $\overline{\Omega}_A\mathsf{V}$ the *free pro-*V *semigroup on* A. A profinite semigroup is said to be *relatively free* if it is of the form $\overline{\Omega}_A\mathsf{V}$ for some set A and pseudovariety V.

PROPOSITION 8.17. *Let* V *be a pseudovariety that is not the trivial pseudovariety* $\mathsf{1}$. *Then the map* $\iota : A \to \overline{\Omega}_A\mathsf{V}$ *is injective.*

Proof of 8.17. Since $\mathsf{V} \neq \mathsf{1}$, there are arbitrarily large semigroups in V. Hence for any $a, b \in A$ with $a \neq b$, there is some $\varphi_i : A \to S_i$ such that $a\varphi_i \neq b\varphi_i$. Therefore, $a\iota = (a\varphi_i)_{i\in I} \neq (b\varphi_i)_{i\in I} = b\iota$. Thus ι is injective. 8.17

Proposition 8.17 means that, when working with any non-trivial pseudovariety V, we can identify A with the subset $A\iota$ of $\overline{\Omega}_A\mathsf{V}$. For the rest of the chapter, assume V is a non-trivial pseudovariety.

LEMMA 8.18. *Let* S *be a pro-*V *semigroup and let* $K \subseteq S$. *Then the following conditions are equivalent:*

a) *there exists a continuous homomorphism* $\varphi : S \to F$ *such that* $F \in \mathsf{V}$ *and* $K = K\varphi\varphi^{-1}$;

b) K *is a clopen subset of* S.

Proof of 8.18. If a continuous homomorphism as in a) exists, then K is clopen since it is the pre-image under a continuous homomorphism of a clopen set.

Suppose that K is a clopen subset of S. Now, S be a subdirect product of semigroups in V. That is, S is a subsemigroup of $\prod_{i\in I} T_i$ for some $T_i \in \mathsf{V}$. Then $K = S \cap (K_1 \cup \ldots \cup K_n)$, where each K_ℓ is a product of the form $\prod_{i\in I} X_{\ell,i}$ with $X_{\ell,i} \subseteq S_i$ and $X_{\ell,i} = S_i$ for all but finitely many indices. Let

$$J = \{i \in I : (\exists \ell \in \{1, \ldots, n\})(T_{\ell,i} \neq S_i)\};$$

notice that J is finite. Let $\varphi : S \to \prod_{i\in J} S_i$ be the natural projection. Then φ is continuous, and $K = K\varphi\varphi^{-1}$. 8.18

PROPOSITION 8.19. *Let* S *be pro-*V *and let* T *be profinite. Let* $\varphi : S \to T$ *be a continuous homomorphism. Then* $\operatorname{im}\varphi$ *is pro-*V *and belongs to* V *if is finite.*

Proof of 8.19. Since T is a subdirect product of finite semigrops, it is sufficient to consider the case where T is finite and φ is surjective and show that $T \in \mathsf{V}$.

For each $t \in T$, let $K_t = t\varphi^{-1}$. Then evey K_t is a pre-image of a clopen set under the continuous homomorphism φ and so is clopen. By Lemma 8.18, there is, for each $t \in T$, a continuous homomorphism $\psi_t : S \to F_t$

with $F_t \in \mathsf{V}$ such that $K_t\psi_t\psi_t^{-1} = K_t$. Let $F = \prod_{t\in T} F_t$; notice that $F \in \mathsf{V}$ since T is finite. Let $\psi : S \to F$ be defined by $x\psi = (x\psi_t)_{t\in T}$. Then $\ker\psi \subseteq \ker\varphi$. Hence there is a homomorphism $\theta : \operatorname{im}\psi \to T$ given by $(x\psi)\theta = x\varphi$. Since φ is surjective, θ is an epimorphism from the subsemigroup $\operatorname{im}\psi$ of F to the semigroup T. Hence $T \prec F$ and so $T \in \mathsf{V}$. 8.19

Propositions 8.16, 8.17, and 8.19 together show that $\overline{\Omega}_A\mathsf{V}$ is a very good analogy for pseudovarieties of free algebras for varieties: maps from A can be extended to homomorphisms from $\overline{\Omega}_A\mathsf{V}$, the 'basis' A (usually) embeds in $\overline{\Omega}_A\mathsf{V}$, and, finally, the only finite semigroups that are homomorphic images of $\overline{\Omega}_A\mathsf{V}$ are the semigroups in V.

PSEUDOIDENTITIES

In Chapter 8 we saw how varieties of $\mathcal{T}$-algebras, and in particular varieties of semigroups, can be defined using laws. Recall that a law in a variety V of $\mathcal{T}$-algebras is a pair $u, v \in F_{\mathcal{T}}(A)$, usually written as a formal equality $u = v$, and that a $\mathcal{T}$-algebra S satisfies this law if $u\hat{\varphi} = v\hat{\varphi}$ for all homomorphisms $\hat{\varphi} : F_{\mathcal{T}}(A) \to S$ extending maps $\varphi : A \to S$. Now that we have free objects for pseudovarieties available, we can the study the analogue of laws for finite semigroups.

Pseudoidentities

Let V be a pseudovariety. A V-*pseudoidentity* is a pair $u, v \in \overline{\Omega}_A\mathsf{V}$, usually written as a formal equality $u = v$. A pro-V semigroup S *satisfies* this pseudoidentity if, for every continuous homomorphism $\theta : \overline{\Omega}_A\mathsf{V} \to S$ we have $u\theta = v\theta$.

LEMMA 8.20. *Let* V *and* W *be pseudovarieties with* $\mathsf{W} \subseteq \mathsf{V}$ *and let* $\pi : \overline{\Omega}_A\mathsf{V} \to \overline{\Omega}_A\mathsf{W}$ *be the natual projection homomorphism. Then for any* $u, v \in \overline{\Omega}_A\mathsf{V}$, *every semigroup in* W *satisfies* $u = v$ *if and only if* $u\pi = v\pi$. 8.20

Let Σ be a set of V-pseudoidentities. Let $[\![\Sigma]\!]_{\mathsf{V}}$ denote the class of all $S \in \mathsf{V}$ that satisfy all the pseudoidentities in Σ.

Reiterman's theorem

THEOREM 8.21. *Let* $\mathcal{W}$ *be a subclass of a pseudovariety* V. *Then* $\mathcal{W}$ *is a pseudovariety if and only if* $\mathcal{W} = [\![\Sigma]\!]_{\mathsf{V}}$ *for some set* Σ *of* V*-pseudoidentities.*

Proof of 8.21. First part. Suppose $\mathcal{W} = [\![\Sigma]\!]$. By reasoning parallel to the proof of Theorem 8.2, we see that $\mathcal{W}$ is closed under Hom, Sub, and $\mathrm{Prod}_{\mathrm{fin}}$ and is thus a pseudovariety.

Second part. Suppose $\mathcal{W}$ is a pseudovariety. Fix a countably infinite alphabet A. Let Σ be the set of all V-pseudoidentities $u = v$ satisfied by all semigroups in $\mathcal{W}$, where $u, v \in \overline{\Omega}_B\mathsf{V}$ and $B \subseteq A$. Clearly $\mathcal{W} \subseteq [\![\Sigma]\!]_{\mathsf{V}}$; we aim to prove equality.

Let $\mathsf{X} = [\![\Sigma]\!]_{\mathsf{V}}$ and let $S \in \mathsf{X}$. Then there exists some $B \subseteq A$ and a surjective continuous homomorphism $\varphi : \overline{\Omega}_B\mathsf{X} \to S$. Let $\pi : \overline{\Omega}_B\mathsf{X} \to \overline{\Omega}_B\mathsf{W}$ be the natural projection.

Suppose $u, v \in \overline{\Omega}_B\mathsf{X}$ are such that $u\pi = v\pi$. Then by Lemma 8.20, every semigroup in W satisfies $u = v$. Thus $u = v$ is a pseudoidentity in Σ; and thus S satisfies $u = v$. In particular, $u\varphi = v\varphi$. This shows that $\ker \pi \subseteq \ker \varphi$.

Therefore the map $\psi : \overline{\Omega}_B\mathsf{W} \to S$ defined by $(x\pi)\psi = x\varphi$ is a well-defined surjective homomorphsim.

For any subset K of S, the subset $K\varphi^{-1}$ of $\overline{\Omega}_B\mathsf{X}$ is closed because φ is continuous. The map π maps closed sets to closed sets because it is a projection of compact spaces. Hence $K\psi^{-1} = K\varphi^{-1}\pi$ is closed. Thus ψ is continuous.

By Proposition 8.19, $S \in \mathsf{W}$. Therefore $[\![\Sigma]\!] = \mathsf{X} \subseteq \mathcal{W}$. 8.21

In Theorem 8.21, we can let V be the pseudovariety of all finite semigroups S, so that the pseudoidentities are S-pseudoidentities. For a set of S-pseudovarieties Σ, we will abbreviate $[\![\Sigma]\!]_{\mathsf{S}}$ by $[\![\Sigma]\!]$.

Bases of pseudoidentities

If V is a variety and Σ is a set of pseudoidentities such that $\mathsf{V} = [\![\Sigma]\!]$, then Σ is called a *basis of pseudoidentities* for V. If there is a finite set of pseudoidentities Σ such that $\mathsf{V} = [\![\Sigma]\!]$, then V is *finitely based*.

In order to actually write down useful pseudoidentities, we introduce some new concepts and notation. Let S be a finite semigroup, $x \in S$, and $k \in \mathbb{Z}$. Consider the sequence $(x^{n!+k})_n$. This sequence is eventually constant: for all $n > \max\{|k|, |S|\}$, all terms $x^{n!+k}$ are equal. If instead we let S be a profinite semigroup, the sequence $(x^{n!+k})_n$ converges to a limit, which we denote $x^{\omega+k}$. In particular, this holds when S is $\overline{\Omega}_A\mathsf{S}$ and $x \in A$.

Now, when S is finite (or profinite) and $\theta : \overline{\Omega}_A\mathsf{S} \to S$ is a continuous homomorphism, the powers of $x\theta$ are not all distinct: we have $(x\theta)^{m+k} = (x\theta)^m$ for some $m, k \in \mathbb{N}$. Let $(x\theta)^n$ be the identity of the cyclic group $C = \{(x\theta)^m, \ldots, (x\theta)^{m+k-1}\}$. Since $(x\theta)^n = (x\theta)^{m!} = x^{m!}\theta$ for all $m \geq n$, $(x^\omega)\theta = (x\theta)^n$. That is, $(x^\omega)\theta$ is the unique idempotent power of $x\theta$. Furthermore, $x^{\omega-1}\theta$ is the inverse of $x^{\omega+1}\theta$ in C.

We can now give explicit examples of pseudoidentities defining particular pseudovarieties of finite semigroups. See Table 8.2 for a summary.

EXAMPLES 8.22. a) The pseudovariety of finite aperiodic semigroups A is defined by the pseudoidentity $x^{\omega+1} = x^\omega$.

b) The pseudovariety of finite nilpotent semigroups N is defined by the pseudoidentities $yx^\omega = x^\omega$ and $x^\omega y = x^\omega$. Since these pseudoidentities essentially say that $x^\omega\theta$ (where $\theta : \overline{\Omega}_A\mathsf{S} \to S$ is a homomorphism) is a zero, we abbreviate them by $x^\omega = 0$.

c) The pseudovariety of finite groups G is defined by the pseudoidentities $yx^\omega = y$ and $x^\omega y = y$. Since these pseudoidentities essentially say that $x^\omega\theta$ (where $\theta : \overline{\Omega}_A\mathsf{S} \to S$ is a homomorphism) is an identity, we abbreviate them by $x^\omega = 1$.

Pseudovariety	*Symbol*	*Basis of pseudoidentities*
Trivial semigroup	1	$x = y$
Null semigroups	Z	$xy = zt$
Left zero semigroups	LZ	$xy = x$
Right zero semigroups	RZ	$xy = y$
Commutative semigroups	Com	$xy = yx$
Semilattices	Sl	$\begin{cases} x^2 = x, \\ xy = yx \end{cases}$
Aperiodic semigroups	A	$x^{\omega+1} = x^\omega$
Nilpotent semigroups	N	$x^\omega = 0$
Groups	G	$x^\omega = 1$
Semigroups	S	—

TABLE 8.2
Some pseudovarieties of semigroups.

We now have two different ways to define pseudovarieties of finite semigroups: we can specify a set of pseudoidentities and consider the pseudovariety they define, or we can specify a set of finite semigroups and consider the pseudovariety they generate. These ways of defining pseudovarieties interact with the lattice of pseudovarieties in different ways.

If Σ and T are sets of pseudoidentities, then

$$[\![\Sigma]\!] \wedge [\![T]\!] = [\![\Sigma \cup T]\!].$$

For example, the pseudovariety of finite Abelian groups is

$$\mathsf{Ab} = [\![xy = yx]\!] \wedge [\![x^\omega = 1]\!] = [\![xy = yx, x^\omega = 1]\!].$$

On the other hand, if $\mathsf{V}(\mathcal{X})$ denotes the pseudovariety generated by a set $\mathcal{X}$ of finite semigroups, then for any classes $\mathcal{X}$ and $\mathcal{Y}$,

$$\mathsf{V}(\mathcal{X}) \vee \mathsf{V}(\mathcal{Y}) = \mathsf{V}(\mathcal{X} \cup \mathcal{Y}).$$

EXERCISES

[See pages 165–171 for the solutions.]

✶8.1 a) Prove that the class of finite nilpotent semigroups is a pseudovariety.

b) Prove that the class all nilpotent semigroups is not a variety.

✶8.2 Recall that a semigroup is *orthodox* if it is regular and its idempotents form a subsemigroup. Prove that the class of orthodox completely regular semigroups forms a variety and that it is defined by the laws $xx^{-1} = x^{-1}x$ and $xyy^{-1}x^{-1}xy = xy$.

8.3 Let $\mathcal{RB}$ be the class of rectangular bands.

a) Prove that $\mathcal{RB}$ is a variety.

b) Prove that $\mathcal{RB}$ is defined by the law $xyx = x$.

c) Prove that $\mathcal{RB}$ is also defined by the laws $x^2 = x$ and $xyz = xz$.

d) Give an example of a semigroup that satisfies $xyz = xz$ but is not a rectangular band.

8.4 Let $\mathcal{X}$ be the class of semigroups isomorphic to a direct product of a group and a rectangular band. Prove that $\mathcal{X}$ is a variety and is defined by the laws $xx^{-1} = x^{-1}x$ and $x^{-1}yy^{-1}x = x^{-1}x$.

8.5 Let $\mathcal{T}$ be a type, and let $\{\mathsf{V}_i : i \in I\}$ be a collection of pseudovarieties of $\mathcal{T}$-algebras. Prove that $\bigcap_{i\in I} \mathsf{V}_i$ is a pseudovariety.

✶8.6 Prove that the pseudovariety of finite completely regular semigroups CR is $[\![x^{\omega+1} = x]\!]$.

✶8.7 Prove that the pseudovariety of finite completely simple semigroups CS is $[\![(xy)^\omega x = x]\!]$.

Automata & finite semigroups

9

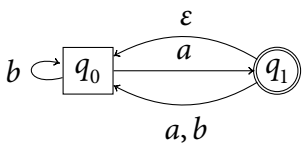
❁ This chapter starts to explore the connection between finite semigroups and rational languages. The main goal is the Eilenberg correspondence, which associates pseudovarieties of finite semigroups to certain classes of rational languages.

FINITE AUTOMATA AND RATIONAL LANGUAGES

Let A be an alphabet. A *language* over A is a subset of A^*. So a language over A is a set of words with letters in A. We will be interested in a particular class of languages over A called the rational languages. To define this class, we must first introduce finite automata.

A *finite automaton*, or simply an *automaton*, $\mathcal{A}$ is formally a quintuple (Q, A, δ, I, F), where Q is a finite set of *states*, A is a finite alphabet, $\delta : Q \times (A \cup \{\varepsilon\}) \to \wp Q$ is a map called the *transition function*, $I \subseteq Q$ is a set of distinguished states called the *initial states* or *start states*, and $F \subseteq Q$ is a distinguished set of states called *accept states* or *final states*.

We can think of an automaton as a directed graph with labelled edges, with vertices being the states, and, for each $q \in Q$ and $a \in A$, an edge labelled by a from q to each state in $(q, a)\delta$. We can thus represent an automaton in a diagrammatic form, with the states being nodes connected by arrows. Initial states are rectangular, all other states are circular. Accept states have double borders. For each $q \in Q$ and $a \in A$, there is an arrow labelled by $a \in A$ from q to each element of $(q, a)\delta$. For example, let $\mathcal{A}$ be the following automaton:



So the automaton $\mathcal{A}$ has state set is $Q = \{q_0, q_1\}$. The set of initial states is $I = \{q_0\}$, the set of final states is $F = \{q_1\}$, and the transition function $\delta : Q \times (A \cup \{\varepsilon\}) \to \wp Q$ is as given in Table 9.1.

	ε	a	b
q_0	$\varnothing$	$\{q_1\}$	$\{q_0\}$
q_1	$\{q_0\}$	$\{q_0\}$	$\{q_0\}$

TABLE 9.1
Values of $(q, a)\delta$

We say that an automaton $\mathcal{A} = (Q, A, \delta, I, F)$ *accepts* a word $w \in A^*$

if there is a directed path in the diagram starting at an initial state in I and ending at an accept state in F, such that w is the product (in A^*) of the labels on this path. For instance, in the example, $\mathcal{A}$ accepts the word *baa*, because it is the product of the labels on the path

$$I \ni q_0 \xrightarrow{b} q_0 \xrightarrow{a} q_1 \xrightarrow{\varepsilon} q_0 \xrightarrow{a} q_1 \in F.$$

It does not accept the word b, because the only path with label product b starting at a state in I is the path

$$I \ni q_0 \xrightarrow{b} q_0 \notin F,$$

which does not end at a state in F.

The idea is that the automaton is a model of a computer that can start in any state in I. While in state q, it can read a letter a from an input tape and change to any state in $(q,a)\delta$, or it can change to any state in $(q,\varepsilon)\delta$ without reading any input. The automaton accepts its input if, when it has finished reading all the input letters, it is in a state in F.

The set of all words accepted by an automaton $\mathcal{A}$ is denoted $L(\mathcal{A})$, and is called the *language recognized by* $\mathcal{A}$. If a language $L \subseteq A^*$ is recognized by some finite automaton, it is called a *recognizable* language.

Our description of an automaton reading input involves an element of choice. The automaton is *non-deterministic*: First, the automaton can start in any state in I. Second, the action it takes in a particular state with a particular input letter to read is not fixed: the automaton can change to one of several other states on reading that letter, and may indeed change to another state without reading any input.

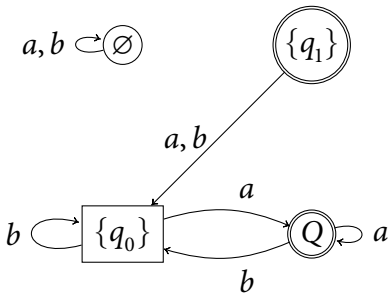
An automaton where there is no such choice is called *deterministic*. More formally, an automaton $\mathcal{A} = (Q, A, \delta, I, F)$ is *deterministic* if I contains a single state, $\delta(q,\varepsilon) = \varnothing$ for all $q \in Q$, and $\delta(q,a)$ contains a single state for all $q \in Q$ and $a \in A$. In terms of the diagram, $\mathcal{A}$ is deterministic if no edge is labelled by ε, and for every state $q \in Q$ and $a \in A$, there is at most one edge starting at q and labelled by a.

THEOREM 9.1. *Let L be a recognizable language. Then there is a deterministic automaton that recognizes L.*

Sketch proof of 9.1. Let $\mathcal{A} = (Q, A, \delta, I, F)$ recognize L. Define an automaton $D(\mathcal{A}) = (\wp Q, A, \eta, J, G)$, where $(S,\varepsilon)\eta = \varnothing$ and $(S,a)\eta$ (where $a \in A$) is defined to be the singleton set $\{T\}$, where T is the set of states that $\mathcal{A}$ can reach starting from a state in S and reading a (including the possibility of using $(q,\varepsilon)\delta$ to change state without reading input), the set of initial states J is the singleton set $\{I\}$ (recall that $I \in \wp Q$ is a *state* of $D(\mathcal{A})$), and the set of accept states G consists of all $U \in \wp Q$ with $U \cap F \neq \varnothing$.

The idea is that each state of $D(\mathcal{A})$ is a set $S \in \wp Q$ that records every state that $\mathcal{A}$ *could* be in when the current input is read. It is not difficult to prove that $L(D(\mathcal{A})) = L$. 9.1

Applying the construction in the proof of Theorem 9.1 to the example automaton $\mathcal{A}$ above, the resulting deterministic automaton $D(\mathcal{A})$ recognizing $L(\mathcal{A})$ has set of initial states $J = \{\{q_0\}\}$, set of accept states $G = \{\{q_1\}, Q\}$, and transition function $\eta : \wp Q \times (A \cup \{\varepsilon\}) \to \wp(\wp Q)$ as shown in Table 9.2. Diagrammatically, $D(\mathcal{A})$ is as follows:



	ε	a	b
$\varnothing$	$\varnothing$	$\{\varnothing\}$	$\{\varnothing\}$
$\{q_0\}$	$\varnothing$	$\{Q\}$	$\{\{q_0\}\}$
$\{q_1\}$	$\varnothing$	$\{\{q_0\}\}$	$\{\{q_0\}\}$
Q	$\varnothing$	$\{Q\}$	$\{\{q_0\}\}$

TABLE 9.2
Values of $(S, a)\eta$

Let A be an alphabet. We are going to define some operations on the class of languages over A. Let L and K be languages over A. Then $K \cup L$ and $K \cap L$ are, respectively, the (setwise) union and intersection of K and L. The language $A^* - L$ is the setwise complement of K in A^*. The concatenation KL of the language K and L is the set of words of the form uv, where $u \in K$ and $v \in L$. The submonoid of A^* generated by K is K^*; the subsemigroup generated by K is K^+. (Note that when $K = A$, this agrees with the notation for the free monoid and free semigroup.) The operations * and $^+$ are called the *Kleene star* and *Kleene plus*.

A language over A is *rational* or *regular* if it can be obtained from the languages $\{a\}$, where $a \in A$, and $\{\varepsilon\}$ and applying the union, concatenation, and Kleene star. A language L over A is *star-free* if it can be obtained from the languages $\{a\}$, where $a \in A$, and $\{\varepsilon\}$ using only the operations of union, intersection, complementation, and concatenation. A language L over A is *plus-free* if it can be obtained from the languages $\{a\}$, where $a \in A$, using only the operations of union, intersection, complementation, and concatenation.

THEOREM 9.2. *A lanaguage over a finite alphabet is rational if and only if it is recognizable.*

Proof of 9.2. [Omitted. See any standard text on automata and languages.] 9.2

As a consequence of Theorem 9.2, the class of rational languages is closed under complementation. Hence we may view the rational languages over A as the languages obtainable from $\{a\}$ (for $a \in A$) and $\{\varepsilon\}$ by applying the operations of union, intersection, complement, concatenation, Kleene star and Kleene plus.

For any language L over an alphabet A and word $u \in A^*$, defined the languages

$$u^{-1}L = \{w : uw \in L\}$$
$$Lu^{-1} = \{w : wu \in L\};$$

the languages $u^{-1}L$ and Lu^{-1} are, respectively, the *left* and *right quotients* of L with respect to u.

PROPOSITION 9.3. *If L is a rational language, then L has only finitely many distinct left and right quotients, all of which are rational languages.*

Proof of 9.3. Let $\mathcal{A} = (Q, A, \delta, I, F)$ be an automaton with $L = L(\mathcal{A})$. Let $u \in A^*$.

Let $J \subseteq Q$ consist of all states $\mathcal{A}$ can reach starting at a state in I and reading u. Let ${}_J\mathcal{A} = (Q, A, \delta, J, F)$. Then $w \in L({}_J\mathcal{A})$ if and only if $uw \in L(\mathcal{A})$. That is, $u^{-1}L = u^{-1}L(\mathcal{A}) = L({}_J\mathcal{A})$. So $u^{-1}L$ is rational. Since there are only finitely many possibilities for J, there are only finitely many distinct languages $u^{-1}L$.

Similarly, let $G \subseteq Q$ consist of all states in which $\mathcal{A}$ can start and reach a state in F after reading u. Let $\mathcal{A}_G = (Q, A, \delta, I, G)$. Then $w \in L(\mathcal{A}_G)$ if and only if $wu \in L(\mathcal{A})$. That is, $Lu^{-1} = L(\mathcal{A})u^{-1} = L(\mathcal{A}_G)u^{-1}$. So Lu^{-1} is rational. Since there are only finitely many possibilities for G, there are only finitely many distinct languages $u^{-1}L$. 9.3

Let $\mathcal{A} = (Q, A, \delta, \{q_0\}, F)$ be a deterministic automaton. For each $a \in A$, there is a partial map $\tau_a : Q \to Q$ with $q\tau_a$ given by $(q, a)\delta = \{q\tau_a\}$ whenever $(q, a)\delta \neq \varnothing$, and with $q\tau_a$ undefined when$(q, a)\delta = \varnothing$. Notice that $\tau_a \in \mathcal{T}_Q$ for each $a \in A$. So we have a homomorphism $\varphi : A^* \to \mathcal{T}_Q$ extending the map $a \mapsto \tau_a$. The set $\operatorname{im}\varphi$ is a submonoid of $\mathcal{T}_Q$ called the *transition monoid* of $\mathcal{A}$. For any word $w \in A^*$, the element $w\varphi$ is a transformation of Q. For any $q \in Q$, the state $q(w\varphi)$ is the state that $\mathcal{A}$ will reach if it starts in q and reads w. Let $Y = \{\sigma \in \operatorname{im}\varphi : q_0\sigma \in F\}$. Then $w\varphi \in Y$ if and only if $w \in L(\mathcal{A})$. This motivates the following definition.

A language L over A is *recognized* by a homomorphism $\varphi : A^* \to M$, where M is a monoid, if there exists a subset M' of M such that $L = M'\varphi^{-1}$, or, equivalently, if $L = L\varphi\varphi^{-1}$. Similarly, a language L not including the empty word is *recognized* by $\varphi : A^+ \to S$, where S is a semigroup, if $L = L\varphi\varphi^{-1}$. A language over A is recognized by a semigroup if it is recognized by a homomorphism into that semigroup. Notice that in the discussion in the previous paragraph, $\mathcal{T}_Q$ is a finite monoid. So any recognizable language is recognized by a finite monoid.

On the other hand, suppose L is recognized by a finite monoid M. Let $\varphi : A^* \to M$ be a homomorphism recognizing L, so that by $L = L\varphi\varphi^{-1}$ Then we can construct an automaton $\mathcal{A}$ recognizing L as follows. The state set is M. The set of initial states is $\{1_M\}$, the set of accept states is $L\varphi$, and the transition function $\delta : M \times (A \cup \{\varepsilon\}) \to M$ is given by $(m, a)\delta = \{m(a\varphi)\}$. It is easy to see that $L(\mathcal{A}) = L\varphi\varphi^{-1} = L$, since the unique path starting at 1_M and labelled by $w = w_1 \cdots w_n$ (where $w_i \in A$) is

$$I \ni 1_M \xrightarrow{w_1} w_1\varphi \xrightarrow{w_2} (w_1w_2)\varphi \xrightarrow{w_3} \dots \xrightarrow{w_n} (w_1 \cdots w_n)\varphi;$$

this path ends in $L\varphi$ if and only if $w \in L$. Similarly, if $L \subseteq A^+$ is recognized by a semigroup S, we can construct an automaton recognizing S with state set S^1.

PROPOSITION 9.4. *A language is recognizable if and only if it is recognized by a finite monoid.* 9.4

Let V be a pseudovariety of semigroups. A language L is V-*recognizable* if it is recognized by some semigroup S in V. Thus a language is recognizable if and only if it is S-recognizable.

SYNTACTIC SEMIGROUPS

For an language L over a finite alphabet A, define a relation on A^* as follows: for $u, v \in A^*$,

$$u \,\sigma_L\, v \Leftrightarrow (\forall p, q \in A^*)(puq \in L \Leftrightarrow pvq \in L).$$

PROPOSITION 9.5. *Let $L \subseteq A^*$ be a language. Then:*

a) *The relation σ_L is a congruence on A^*.*

b) *The language L is a union of σ_L-classes.*

c) *If ρ is a congruence on A^* with the property that L is a union of ρ-classes, then $\rho \subseteq \sigma_L$.*

Proof of 9.5. See Exercise 9.1. 9.5

For any language L over an alphabet A, the congruence σ_L is called the *syntactic congruence* of L, the factor semigroup A^*/σ_L is called the *syntactic semigroup* of L and is denoted $\operatorname{Synt} L$, and the natural homomorphism $\sigma_L^\natural : A^* \to A^*/\sigma_L = \operatorname{Synt} L$ is the *syntactic homomorphism* of L.

PROPOSITION 9.6. *Let L be a language over A. Then L is recognized by a semigroup S if and only if* $\operatorname{Synt} L$ *divides S.*

Proof of 9.6. Let $\varphi : A^+ \to S$ recognize L. So $L = L\varphi\varphi^{-1}$. Then $\ker\varphi$ is a congruence on A^+ and L is a union of $\ker\varphi$-classes. Hence $\ker\varphi \subseteq \sigma_L$. Define a map $\psi : \operatorname{im}\varphi \to \operatorname{Synt} L$ by $(u\varphi)\psi = [u]_{\sigma_L}$; this map is a well-defined homomorphism since $\ker\varphi \subseteq \sigma_L$. It is clearly surjective. Since $\operatorname{im}\varphi$ is a subsemigroup of S and $\psi : \operatorname{im}\varphi \to \operatorname{Synt} L$ is an epimorphism, $\operatorname{Synt} L \prec S$.

Let $\operatorname{Synt} L \prec S$. So there is a subsemigroup T of S and an epimorphism $\psi : T \to \operatorname{Synt} L$. For each $a \in A$, define a map $\varphi : A \to T$ by choosing $a\varphi$ such that $(a\varphi)\psi = a\sigma_L^\natural$. Since A^+ is free on A, there is a unique extension of φ to a homomorphism $\hat{\varphi} : A^+ \to T$; notice that $(u\varphi)\psi = u\sigma_L^\natural$ for

all $u \in A^+$ since ψ and $\sigma_L^\natural$ are homomorphisms. Let $T' = L\sigma_L^\natural\psi^{-1}$. Then, viewing $\hat{\varphi}$ as a homomorphism from A^+ to S, we have

$$L = L\sigma_L^\natural(\sigma_L^\natural)^{-1} = L\sigma_L^\natural\psi^{-1}\hat{\varphi}^{-1} = T'\hat{\varphi}^{-1},$$

and so S recognizes L. 9.6

PROPOSITION 9.7. *Let A and B be alphabets. For all languages L and K over A, for all $a \in A$, and for all homomorphisms $\varphi : B^+ \to A^+$:*

a) $\operatorname{Synt} L = \operatorname{Synt}(A^+ - L)$;
b) $\operatorname{Synt}(L \cap K) \prec (\operatorname{Synt} L) \times (\operatorname{Synt} K)$;
c) $\operatorname{Synt}(a^{-1}L) \prec \operatorname{Synt} L$;
d) $\operatorname{Synt}(La^{-1}) \prec \operatorname{Synt} L$;
e) $\operatorname{Synt}(L\varphi^{-1}) \prec \operatorname{Synt} L$.

Proof of 9.7. a) For any $u, v \in A^+$, we have

$$\begin{aligned} u\ \sigma_L\ v &\Leftrightarrow (\forall p, q \in A^*)(puq \in L \Leftrightarrow pvq \in L) \\ &\Leftrightarrow (\forall p, q \in A^*)(puq \in A^+ - L \Leftrightarrow pvq \in A^+ - L) \\ &\Leftrightarrow u\ \sigma_{A^+-L}\ v; \end{aligned}$$

Hence $\sigma_L = \sigma_{A^+-L}$ and so $\operatorname{Synt} L = \operatorname{Synt} A^+ - L$.

b) Define a homomorphism $\varphi : A^+ \to (\operatorname{Synt} L) \times (\operatorname{Synt} K)$ by $u\varphi = (u\sigma_L^\natural, u\sigma_K^\natural)$. Let $S = L\sigma_L^\natural \times K\sigma_K^\natural \subseteq (\operatorname{Synt} L) \times (\operatorname{Synt} K)$. Then

$$\begin{aligned} & u \in S\varphi^{-1} \\ \Rightarrow\ & u\varphi \in L\sigma_L^\natural \times K\sigma_K^\natural \\ \Rightarrow\ & (\exists v \in L, w \in K)\big((v\sigma_L^\natural, w\sigma_K^\natural) = (u\sigma_L^\natural, u\sigma_K^\natural)\big) \\ \Rightarrow\ & (\exists v \in L, w \in K)\big((v\sigma_L^\natural = u\sigma_L^\natural) \wedge (w\sigma_K^\natural = u\sigma_K^\natural)\big) \\ \Rightarrow\ & (u \in L\sigma_L^\natural(\sigma_L^\natural)^{-1}) \wedge (u \in K\sigma_K^\natural(\sigma_K^\natural)^{-1}) \\ \Rightarrow\ & (u \in L) \wedge (u \in K) \\ \Rightarrow\ & u \in L \cap K. \end{aligned}$$

Hence $S\varphi^{-1} \subseteq L \cap K$. The opposite inclusion is obvious, so $S\varphi^{-1} = L \cap K$. Thus $\varphi : A^+ \to (\operatorname{Synt} L) \times (\operatorname{Synt} K)$ recognizes $L \cap K$, and so $\operatorname{Synt} L \cap K \prec (\operatorname{Synt} L) \times (\operatorname{Synt} K)$.

c) Let $S = L\sigma_L^\natural \subseteq \operatorname{Synt} L$. Let $s = a\sigma_L^\natural$. Define

$$s^{-1}S = \{x \in \operatorname{Synt} L : sx \in S\}.$$

Then $a^{-1}L = (s^{-1}S)\varphi^{-1}$ and so $\varphi : A^+ \to \operatorname{Synt} L$ recognizes $a^{-1}L$. Hence $\operatorname{Synt}(a^{-1}L) \prec \operatorname{Synt} L$.

d) This is similar to part c).

e) The homomorphism $\varphi\sigma_L^\natural : B^+ \to \operatorname{Synt} L$ recognizes $L\varphi^{-1}$ since

$$L\varphi^{-1}\varphi\sigma_L^\natural(\varphi\sigma_L^\natural)^{-1} = L\sigma_L^\natural(\sigma_L^\natural)^{-1}\varphi^{-1} = L\varphi^{-1}.$$

Hence $\operatorname{Synt}(L\varphi^{-1}) \prec \operatorname{Synt} L$. 9.7

EILENBERG CORRESPONDENCE

A *variety of rational languages* is a correspondence $\mathcal{V}$ that associates to each finite alphabet A a class of rational languages $\mathcal{V}(A^+)$ over A with the following properties:

- $\mathcal{V}(A^+)$ is closed under union, intersection, and complementations;
- if $L \in \mathcal{V}(A^+)$ and $a \in A$, then the right and left quotient languages

$$a^{-1}L = \{w \in A^+ : aw \in L\}$$
$$La^{-1} = \{w \in A^+ : wa \in L\}$$

  are also in $\mathcal{V}(A^+)$;
- if $\varphi : A^+ \to B^+$ is a homomorphism and $L \in \mathcal{V}(B^+)$, then $L\varphi^{-1} \in \mathcal{V}(A^+)$.

EXAMPLES 9.8. a) The correspondence $\mathcal{E}$ such that $\mathcal{E}(A^+) = \{\varnothing, A^+\}$ is a variety of rational languages. To see this, first note that each $\mathcal{E}(A^+)$ is clearly closed under union, intersection, and complement. Next, for any $a \in A$, we have $a^{-1}\varnothing = \varnothing a^{-1} = \varnothing \in \mathcal{E}(A^+)$ and $a^{-1}A^+ = A^+a^{-1} = A^+ \in \mathcal{E}(A^+)$, so $\mathcal{E}(A^+)$. Finally, for any homomorphism $\varphi : B^+ \to A^+$, we have $\varnothing\varphi^{-1} = \varnothing \in \mathcal{E}(B^+)$ and $A^+\varphi^{-1} = B^+ \in \mathcal{E}(B^+)$.

b) Let $\mathcal{F}$ be the correspondence that associates to each finite alphabet A the class of all plus-free languages over A. Then $\mathcal{F}$ is a variety of rational languages.

c) A language L over an alphabet A is said to be cofinite if $A^* - L$ is finite. Let $\mathcal{N}$ be the correspondence that associates to each finite alphabet A the class of all finite or cofinite languages over A. Then $\mathcal{N}$ is a variety of rational languages (see Exercise 9.3).

LEMMA 9.9. *Let $\mathcal{V}$ be a variety of rational languages. Let A be an alphabet and let $K \in \mathcal{V}(A^+)$. Then $s(\sigma_K^\natural)^{-1} \in \mathcal{V}(A^+)$ for all $s \in \operatorname{Synt} K$.*

Proof of 9.9. For $w \in A^+$, define

$$\begin{aligned} R_w &= \{(p,q) : p, q \in A^+, pwq \in K\} \\ &= \{(p,q) : p, q \in A^+, w \in p^{-1}Kq^{-1}\}; \end{aligned}$$

then $u \ \sigma_K \ v$ if and only if $R_u = R_v$. Hence $u\sigma_K^\natural(\sigma_K^\natural)^{-1}$, which is the σ_K-class of $u \in A^+$, is given by

$$u\sigma_K^\natural(\sigma_K^\natural)^{-1} = \bigcap_{p,q \in R_u} p^{-1}Kq^{-1} - \bigcup_{p,q \notin R_u} p^{-1}Kq^{-1}. \tag{9.1}$$

Since K is recognizable, by Proposition 9.3 there are only finitely many distinct sets $p^{-1}Kq^{-1}$. Therefore the intersections and unions in (9.1) are finite. By repeated application of the closure of $\mathcal{V}(A^+)$ under left and right quotients, each of the sets $p^{-1}Kq^{-1}$ lies in $\mathcal{V}(A^+)$. Since $\mathcal{V}(A^+)$ is closed under unions, intersections, and complements, $u\sigma_K^\natural(\sigma_K^\natural)^{-1}$ lies in $\mathcal{V}(A^+)$. Consequently $s(\sigma_K^\natural)^{-1} \in \mathcal{V}(A^+)$ for all $s \in \operatorname{Synt} K$. 9.9

Eilenberg's correspondence

There is a natural correspondence, known as *Eilenberg's correspondence*, between varieties of rational languages and pseudovarieties of semigroups. This correspondence is defined as follows:

- Let $\mathcal{V}$ be a variety of rational languages. The corresponding pseudovariety V is generated by all semigroups $\operatorname{Synt} L$ where $L \in \mathcal{V}(A^+)$ for some finite alphabet A. That is, we have a map

$$\mathcal{V} \mapsto \mathsf{V}, \tag{9.2}$$

  where V is the pseudovariety generated by

$$\{\operatorname{Synt} L : L \in \mathcal{V}(A^+) \text{ for some finite alphabet } A\}.$$

- Let V be a pseudovariety of semigroups. The corresponding variety of rational languages $\mathcal{V}$ associates to each finite alphabet A the class of languages L such that $\operatorname{Synt} L \in \mathsf{V}$, or, equivalently, the class of languages L such that L is recognized by some semigroup in L. That is, we have a map

$$\mathsf{V} \mapsto \mathcal{V}, \tag{9.3}$$

  where

$$\mathcal{V}(A^+) = \{L \subseteq A^+ : \operatorname{Synt} L \in \mathsf{V}\}$$

  for any finite alphabet A.

Eilenberg's theorem

THEOREM 9.10. *The maps* (9.2) *and* (9.3) *are mutually inverse.*

Proof of 9.10. Let $\mathcal{V}$ be a variety of rational languages. Let V be the pseudovariety associated to it by (9.2). Let $\mathcal{V}'$ be the variety of rational languages associated to V by (9.3). We aim to show that $\mathcal{V}(A^+) = \mathcal{V}'(A^+)$. for each finite alphabet A.

First, we prove that $\mathcal{V}(A^+) \subseteq \mathcal{V}'(A^+)$. Let $L \in \mathcal{V}(A^+)$. Then $\operatorname{Synt} L \in \mathsf{V}$ by the definition of (9.2), and so $L \in \mathcal{V}'(A^+)$ by the definition of (9.3). Hence $\mathcal{V}(A^+) \subseteq \mathcal{V}'(A^+)$.

Next we prove that $\mathcal{V}'(A^+) \subseteq \mathcal{V}(A^+)$. This part of the proof is more complicated. Let $L \in \mathcal{V}'(A^+)$. Then $\operatorname{Synt} L \in \mathsf{V}$ by the definition of (9.3). Now, V is generated by

$$\mathcal{X} = \{\operatorname{Synt} K : K \in \mathcal{V}(A^+) \text{ for some finite alphabet } A\};$$

that is, $\mathsf{V} = \operatorname{Hom} \operatorname{Sub} \operatorname{Prod}_{\text{fin}} \mathcal{X}$. Hence there exist alphabets A_i and languages $K_i \in \mathcal{V}(A_i^+)$ for $i = 1, \ldots, n$ such that

$$\operatorname{Synt} L \prec \prod_{i=1}^{n} \operatorname{Synt} K_i.$$

Let $W = \prod_{i=1}^n A_i^+$ and $T = \prod_{i=1}^n \operatorname{Synt} K_i$. Define a map

$$\gamma : W \to T, \qquad (w_1, \ldots, w_n)\gamma = (w_1\sigma_{K_1}^\natural, \ldots, w_n\sigma_{K_n}^\natural);$$

then γ is an epimorphism because all of the maps $\sigma_{K_i}^{\natural} : A_I^+ \to \operatorname{Synt} K_i$ are epimorphisms. Since $\operatorname{Synt} L \prec T$, the semigroup T recognizes L; that is, there is a homomorphism $\varphi : A^+ \to T$ and a subset M of T such that $L = M\varphi^{-1}$.

Define $\psi : A \to W$ by letting $a\psi$ be such that $a\psi\gamma = a\varphi$; since A^+ is free on A, this map extends to a unique homomorphism $\hat{\psi} : A^+ \to W$. Notice that $u\hat{\psi}\gamma = u\varphi$ since φ and γ are homomorphisms. For each $i = 1, \ldots, n$, let $\psi_i : A^+ \to A_i^+$ be such that

$$u\hat{\psi} = (u\psi_1, \ldots, u\psi_n)$$

and $\varphi_i : A^+ \to \operatorname{Synt} K_i$ be such that

$$u\varphi = (u\varphi_1, \ldots, u\varphi_n).$$

Then $\varphi_i = \psi_i \sigma_{K_i}^{\natural}$.

We have

$$L = M\varphi^{-1} = \bigcup_{m \in M} m\varphi^{-1}.$$

Since $\mathcal{V}(A^+)$ is closed under Boolean operations, it is sufficient to show that $m\varphi^{-1} \in \mathcal{V}(A^+)$ for all $m \in M$. If $m = (s_1, \ldots, s_n) \in M \subseteq T$, where $s_i \in \operatorname{Synt} K_i$, then

$$m\varphi^{-1} = \bigcap_{i=1}^{n} s_i \varphi_i^{-1}.$$

Again, since $\mathcal{V}(A^+)$ is closed under Boolean operations, it is sufficient to show that $s_i\varphi_i^{-1} \in \mathcal{V}(A^+)$ for all $s_i \in \operatorname{Synt} K_i$ and $i = 1, \ldots, n$.

Since $s_i\varphi_i^{-1} = s_i(\sigma_{K_i}^{\natural})^{-1}\psi_i^{-1}$, the closure of $\mathcal{V}$ under inverse homomorphisms shows that it is sufficient to show that $s_i(\sigma_{K_i}^{\natural})^{-1} \in \mathcal{V}(A_i^+)$. This follows immediately from Lemma 9.9. 9.10

PROPOSITION 9.11. *The Eilenberg correspondence associates the pseudovariety of nilpotent semigroups* N *with the variety of finite or cofinite rational languages* $\mathcal{N}$.

Proof of 9.11. Let $S \in \mathsf{N}$, with $S^n = 0$ for all $x \in S$. Let A be a finite alphabet and suppose $\varphi : A^+ \to S$ recognizes a language L.

Suppose that $L\varphi$ contains 0_S. Then if $w \in A^*$ with $|w| \geq n$, then $w\varphi = 0_S$ and so $w \in L\varphi\varphi^{-1} = L$. Hence L contains all words with at least n letters and so is confinite. Hence $L \in \mathcal{N}(A^+)$

Suppose that $L\varphi$ does not contain 0_S. Then if $w \in A^*$ with $|w| \geq n$, then $w \notin L$, since otherwise $L\varphi \ni w\varphi \in S^n = \{0\}$. Hence L contains only words with fewer than n symbols and so L is finite. Hence $L \in \mathcal{N}(A^+)$.

Thus if L is a language over A recognized by a semigroup in N, then $L \in \mathcal{N}(A^+)$.

On the other hand, let L be a language in $\mathcal{N}(A^+)$. So L is either finite or cofinite. Then, for some $n \in \mathbb{N}$, either $L \cap I_n = \varnothing$ or $L \supseteq I_n$, where

$I_n = \{w \in A^* : |w| \geq n\}$. Notice that I_n is an ideal of A^+, and that $S = A^+/I_n$ is a nilpotent semigroup with $S^n = 0_S$; thus $S \in \mathsf{N}$. Then the natural homomorphism $\rho^{\natural}_{I_n} : A^+ \to S$ recognizes L. 9.11

It is important to notice that although Proposition 9.11 describes an instance of Eilenberg's correspondence, it is not a consequence of Theorem 9.10. In general, finding and proving instances of Eilenberg's correspondence is difficult.

Schützenberger's theorem

THEOREM 9.12. *The Eilenberg correspondence associates the variety of star-free rational languages and the pseudovariety* A *of aperiodic semigroups.*

Proof of 9.12. [Omitted.] 9.12

EXERCISES

[See pages 171–172 for the solutions.]

∗9.1 Prove Proposition 9.5.

∗9.2 Prove that a language $L \subseteq A^*$ is rational if and only if Synt L is finite. [Hint: this is an easy consequence of results in this chapter.]

∗9.3 Prove that the correspondence $\mathcal{N}$ in Example 9.8(c) (with $\mathcal{N}(A^+)$ being the class of finite or cofinite languages over A) is a variety of rational languages.

9.4 Recall that 1 is the pseudovariety containing only the trivial semigroup $E = \{e\}$. Describe the variety of rational languages $\mathcal{V}$ associated to 1 by the Eilenberg correspondence. (That is, describe $\mathcal{V}(A^+)$ for each alphabet A.)

Solutions to exercises

EXERCISES FOR CHAPTER 1

[See pages 25–26 for the exercises.]

1.1 For $n = 2$ the result in the hint is obviously true. So assume it is true for all $n < k$; we aim to show it is true for $n = k$. Take some bracketing of the product $s_1 s_2 \cdots s_k$ and let t be the result. This bracketing is a product of some bracketing of $s_1 \cdots s_\ell$ and some bracketing of $s_{\ell+1} \cdots s_k$, for some ℓ with $1 \leq \ell < k$. By the assumption, the result of the bracketing of $s_1 \cdots s_\ell$ is $s_1(s_2(\cdots s_\ell)\cdots)$ and the result of the bracketing of $s_{\ell+1} \cdots s_n$ is $s_{\ell+1}(s_{\ell+2}(\cdots s_k)\cdots)$. Thus

$$\begin{aligned} t &= \big(s_1(s_2(\cdots s_\ell)\cdots)\big)\big(s_{\ell+1}(s_{\ell+2}(\cdots s_k)\cdots)\big) \\ &= s_1\big((s_2(\cdots s_\ell)\cdots)\big)\big(s_{\ell+1}(s_{\ell+2}(\cdots s_k)\cdots)\big) && \text{[by associativity]} \\ &= s_1(s_2(s_3 \cdots s_k)\cdots) && \text{[by assumption with } n = k-1\text{]} \end{aligned}$$

which is the result with $n = k$.

1.2 Yes. A group is left cancellative and its identity is an idempotent.

1.3 Since z is a left zero, $zz' = z$. Since z' is a right zero, $zz' = z'$. Hence $z = zz' = z'$.

1.4 Let $x \in S$. Then $x = xe$ since e is a right identity, and $e = xe$ since e is a right zero. Hence $x = xe = e$. Thus e is the only element of S.

1.5 a) If S contains a zero, then $S^0 = S$ and there is nothing to prove. Otherwise $S^0 = S \cup \{0\}$. Then $x1_S = x1_S = x$ for all $x \in S$ since 1_S is an identity for S, and $01_S = 1_S 0 = 0$ by the definition of S^0. Hence 1_S is an identity for S^0.

b) The reasoning is similar to part a).

1.6 Let S be left-cancellative and $e \in S$ an idempotent. Let $x \in S$. Since e is idempotent, $eex = ex$. Since S is left-cancellative, $ex = x$. Since $x \in S$ was arbitrary, this proves that e is a left-identity for x.

Suppose now that S is cancellative and that $e, f \in S$ are idempotents. By the preceding paragraph and the symmetric result for right-cancellativity, e and f are left and right identities for S. By Proposition 1.2, $e = f$.

1.7 Let S be a right zero semigroup. Suppose $x, y, z \in S$ are such that $zx = zy$. Since S is a right zero semigroup, $zx = x$ and $zy = y$. Hence $x = zx = zy = y$. That is, $x = y$. So $zx = zy \Rightarrow x = y$ for all $x, y, z \in S$ and thus S is left-cancellative.

1.8 Let S be a finite cancellative semigroup. Let $x \in S$. Then x is periodic and so some power of x is an idempotent. By Exercise 1.6, this idempotent is an identity 1_S for S. Now let $y \in S$ be arbitrary. Then y^n is idempotent for some $n \in \mathbb{N}$. Again by Exercise 1.6, $y^n = 1_S$ and so y^{n-1} is a left and right inverse for y. Since $y \in S$ was arbitrary, S is a group.

1.9 Let $\rho \in \mathcal{B}_X$. Let $x, y \in X$. Then

$$\begin{aligned}
&(x,y) \in \rho \circ \mathrm{id}_X \\
&\Leftrightarrow (\exists z \in X)\big((x,z) \in \rho \wedge (z,y) \in \mathrm{id}_X\big) && \text{[by definition of } \circ\text{]} \\
&\Leftrightarrow (\exists z \in X)\big((x,z) \in \rho \wedge (z = y)\big) && \text{[by definition of } \mathrm{id}_X\text{]} \\
&\Leftrightarrow (x,y) \in \rho.
\end{aligned}$$

So $\rho \circ \mathrm{id}_X = \rho$ and similarly $\mathrm{id}_X \circ \rho = \rho$. So id_X is the identity of $\mathcal{B}_X$.

The zero of $\mathcal{B}_X$ is the empty relation $\varnothing$. So see this, we must prove that $\rho \circ \varnothing = \varnothing \circ \rho = \varnothing$. So suppose, with the aim of obtaining a contradiction, that $\rho \circ \varnothing \neq \varnothing$. Then $(x,y) \in \rho \circ \varnothing$ for some $x, y \in X$. Then there exists $z \in X$ such that $(x,z) \in \rho$ and $(z,y) \in \varnothing$. But $(z,y) \in \varnothing$ is a contradiction. So $\rho \circ \varnothing = \varnothing$ and similarly $\varnothing \circ \rho = \varnothing$.

1.10 No. Let S be a non-trivial semigroup. Choose some element $x \in S$ and let $T = \{x^n : n \in \mathbb{N}\}$ be the subsemigroup generated by x. If T is finite (that is, if x is periodic), then some x^n is idempotent and so $\{x^n\}$ is a subsemigroup of S; furthermore, it must be a proper subsemigroup since S is non-trivial. If, on the other hand, T is infinite, then $\{x^{2n} : n \in \mathbb{N}\}$ is a proper subsemigroup of T and hence of S.

1.11 The easiest examples are infinite right or left zero semigroup, and the semigroups $(\mathbb{N}, \triangle)$ and $(\mathbb{Z}, \triangle)$ from Examples 1.6(a)–(b).

1.12 The empty relation $\varnothing$ is a partial transformation. It is a zero for $\mathcal{B}_X$, so it is certainly a zero for $\mathcal{P}_X$.

The semigroup of transformations $\mathcal{T}_X$ contains $|X|$ right zeros, namely the constant maps $\tau_x : X \to X$ defined by $y\tau_x = x$ for all $y \in X$. Each map τ_x is a right zero because for any $\sigma \in \mathcal{T}_X$, we have $y\sigma\tau_x = x$ for all $y \in X$, and so $\sigma\tau_x = \tau_x$. Suppose $\tau \in \mathcal{T}_X$ is a right zero. Then $\sigma\tau = \tau$ for all $\sigma \in \mathcal{T}_X$. In particular, this is true for all $\sigma \in \mathcal{S}_X$. Choose some $y \in X$ and let $x = y\tau$. Now let $z \in X$. Choose $\sigma \in \mathcal{S}_X$ with $z\sigma = y$. Then $z\tau = z\sigma\tau = y\tau = x$. Since $z \in X$ was arbitrary, we have $\tau = \tau_x$. Thus the right zeros in $\mathcal{T}_X$ are precisely the constant maps τ_x. Thus, if $|X| \geq 2$, then $\mathcal{T}_X$ contains more than one right zero, and so cannot contain a left zero and thus cannot contain a (two-sided) zero. If $|X| = 1$, then $\mathcal{T}_X$ is trivial and so trivially contains a zero.

1.13 a) To prove the four identities, we have to show that the transformations on each side act the same way on every element of X. For the first identity, let $i \geq 3$; then

$$\begin{aligned}
1(1\ i)|1\ 2|(1\ i) &= i|1\ 2|(1\ i) = i(1\ i) = 1 = 1|i\ 2|; \\
2(1\ i)|1\ 2|(1\ i) &= 2|1\ 2|(1\ i) = 2(1\ i) = 2 = 2|i\ 2|;
\end{aligned}$$

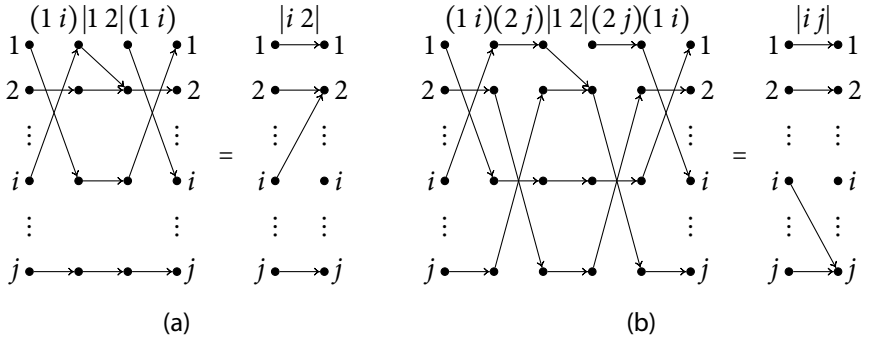


FIGURE S.1
Generating (a) $|2\ j|$ and (b) $|i\ j|$ using transpositions and $|1\ 2|$.

$$i(1\ i)|1\ 2|(1\ i) = 1|1\ 2|(1\ i) = 2(1\ i) = 2 = 2|i\ 2|;$$
$$x(1\ i)|1\ 2|(1\ i) = x|1\ 2|(1\ i) = x(1\ i) = x = x|i\ 2| \quad \text{for } x \in X - \{1, 2, i\}.$$

(Figure S.1(a) illustrates the first identity diagrammatically.) The second identity is proved similarly.

For the third identity, let $i, j \geq 3$ with $i \neq j$; then

$$\begin{aligned}
1(1\ i)(2\ j)|1\ 2|(2\ j)(1\ i) &= i(2\ j)|1\ 2|(2\ j)(1\ i) \\
&= i|1\ 2|(2\ j)(1\ i) = i(2\ j)(1\ i) = i(1\ i) = 1 = 1|i\ j|; \\
2(1\ i)(2\ j)|1\ 2|(2\ j)(1\ i) &= 2(2\ j)|1\ 2|(2\ j)(1\ i) \\
&= j|1\ 2|(2\ j)(1\ i) = j(2\ j)(1\ i) = 2(1\ i) = 2 = 2|i\ j|; \\
i(1\ i)(2\ j)|1\ 2|(2\ j)(1\ i) &= 1(2\ j)|1\ 2|(2\ j)(1\ i) \\
&= 1|1\ 2|(2\ j)(1\ i) = 2(2\ j)(1\ i) = j(1\ i) = j = i|i\ j|; \\
j(1\ i)(2\ j)|1\ 2|(2\ j)(1\ i) &= j(2\ j)|1\ 2|(2\ j)(1\ i) \\
&= 2|1\ 2|(2\ j)(1\ i) = 2(2\ j)(1\ i) = j(1\ i) = j = j|i\ j|; \\
x(1\ i)(2\ j)|1\ 2|(2\ j)(1\ i) &= x(2\ j)|1\ 2|(2\ j)(1\ i) \\
&= x|1\ 2|(2\ j)(1\ i) = x(2\ j)(1\ i) = x(1\ i) = x = x|i\ j| \\
&\qquad \text{for } x \in X - \{1, 2, i, j\}.
\end{aligned}$$

(Figure S.1(b) illustrates the third identity diagrammatically.)

For the fourth identity, let $i \neq j$; then

$$\begin{aligned}
i(i\ j)|i\ j|(i\ j) &= j|i\ j|(i\ j) = j(i\ j) = i = i|j\ i|; \\
j(i\ j)|i\ j|(i\ j) &= i|i\ j|(i\ j) = j(i\ j) = i = j|j\ i|; \\
x(i\ j)|i\ j|(i\ j) &= x|i\ j|(i\ j) = x(i\ j) = i = x|j\ i| \quad \text{for } x \in X - \{i, j\}.
\end{aligned}$$

b) To prove that $|i\ j|\varphi' = \varphi$, we must show that both sides act the same way on every element of X. By the definition of φ',

$$\begin{aligned}
i|i\ j|\varphi' &= j\varphi' = j\varphi, \\
x|i\ j|\varphi' &= x\varphi' = x\varphi \qquad \text{for } x \neq i.
\end{aligned}$$

c) Proceed by induction on $|X - \operatorname{im}\varphi|$. If $|X - \operatorname{im}\varphi| = 0$, then $\operatorname{im}\varphi = X$ and so φ is surjective and so (since X is finite) injective. Hence $\varphi \in \mathcal{S}_X = \langle \tau, \zeta \rangle \subseteq \langle \tau, \zeta, |1\ 2| \rangle$. So assume that $\psi \in \langle \tau, \zeta, |1\ 2| \rangle$ is true for all $\psi \in \mathcal{T}_X$ with $|X - \operatorname{im}\psi| = k - 1 < n$. Let φ be such that $|X - \operatorname{im}\varphi| = k$. Then by parts a) and b), we have $\varphi = |i\ j|\varphi' = (1\ i)(2\ j)|1\ 2|(2\ j)(1\ i)\varphi'$, where $\operatorname{im}\varphi' \subsetneq \operatorname{im}\varphi$. Hence $|X - \operatorname{im}\varphi'| = k - 1$ and so $\varphi' \in \langle \tau, \zeta, |1\ 2| \rangle$. Hence $\varphi \in \langle \tau, \zeta, |1\ 2| \rangle$. By induction, $\mathcal{T}_X = \langle \tau, \zeta, |1\ 2| \rangle$.

1.14 Suppose x is right invertible. Then there exists $y \in S$ such that $xy = 1$. Since S is finite, $x^k = x^{k+m}$ for some $k, m \in \mathbb{N}$. So $1 = x^k y^k = x^{k+m} y^k = x^m = x^{m-1}x$ and so x^{m-1} is a left inverse for x. Similarly, if x is left invertible, it is right invertible.

1.15 a) Let $\rho \in \mathcal{T}_X$ be left-invertible. Then there exists $\sigma \in \mathcal{T}_X$ such that $\sigma \circ \rho = \mathrm{id}_X$. Let $x \in X$. Then $x(\sigma \circ \rho) = x$. So $(x\sigma)\rho = x$. So ρ is surjective. Now let $\rho \in \mathcal{T}_X$ be surjective. Define $\sigma \in \mathcal{T}_X$ as follows. For each $x \in X$, choose $y \in X$ such that $y\rho = x$. (Such a y exists because ρ is surjective.) Define $x\sigma = y$. Clearly $\sigma \circ \rho = \mathrm{id}_X$ and so ρ is left-invertible.

b) Let $\rho \in \mathcal{T}_X$ be right-invertible. Then there exists $\sigma \in \mathcal{T}_X$ such that $\rho \circ \sigma = \mathrm{id}_X$. Then $x\rho = y\rho \Rightarrow (x\rho)\sigma = (y\rho)\sigma \Rightarrow x = y$ and so ρ is injective. Now let $\rho \in \mathcal{T}_X$ be injective. Define $\sigma \in \mathcal{T}_X$ as follows. For $x \in \operatorname{im}\rho$, let $y \in X$ be the unique element such that $y\rho = x$. Define $x\sigma = y$. For $x \in X - \operatorname{im}\rho$, define $x\sigma$ arbitrarily. Clearly $\rho \circ \sigma = \mathrm{id}_X$ and so ρ is right-invertible.

1.16 Let $x, y \in X$. Since $(X, \leq)$ is a total order, $x \leq y$ or $y \leq x$. In the first case, $x \wedge y = x$ and $x \vee y = y$. In the second, $x \wedge y = y$ and $x \vee y = x$. So $x \wedge y$ and $x \vee y$ exist for all $x, y \in X$ and so $(X, \leq)$ is a lattice.

1.17 a) By definition, $x \wedge y \leq x$. So the least upper bound of $x \wedge y$ and x (which is the definition of $(x \wedge y) \vee x$) must be x itself. Dual reasoning gives $(x \vee y) \wedge x = x$.

b) Assume that for all $p, q, r \in S$, we have $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$. (We have re-labelled variables to avoid confusion.) Then

$$
\begin{aligned}
&(x \vee y) \wedge (x \vee z) \\
&= \big((x \vee y) \wedge x\big) \vee \big((x \vee y) \wedge z\big) \\
&\qquad\qquad \text{[by assumption, with } p = (x \vee y),\ q = x,\ r = z\text{]} \\
&= x \vee \big((x \vee y) \wedge z\big) \qquad \text{[by part a)]} \\
&= x \vee \big((x \wedge z) \vee (y \wedge z)\big) \\
&\qquad\qquad \text{[by assumption, with } p = z,\ q = x,\ r = y\text{]} \\
&= \big(x \vee (x \wedge z)\big) \vee (y \wedge z) \qquad \text{[by associativity of } \vee\text{]} \\
&= x \vee (y \wedge z). \qquad \text{[by part a)]}
\end{aligned}
$$

The other direction is similar.

1.18 There are many examples. For instance, let S be any non-trivial monoid, let $T = S^0$, and define $\varphi : S \to T$ by $x\varphi = 0$ for all $x \in S$. It is easy to see that φ is a homomorphism, but $1_S\varphi = 0 \neq 1_{S^0}$.

1.19 a) Since ρ^{R} is a reflexive relation containing ρ, it is immediate that $\rho \cup \mathrm{id}_X \subseteq \rho^{\mathsf{R}}$. On the other hand, $\rho \cup \mathrm{id}_X$ is a reflexive relation containing ρ; since ρ^{R} is the smallest reflexive relation containing ρ, we have $\rho^{\mathsf{R}} \subseteq \rho \cup \mathrm{id}_X$. Hence $\rho^{\mathsf{R}} = \rho \cup \mathrm{id}_X$.

b) Since ρ^{S} is a symmetric relation containing ρ, it is immediate that $\rho \cup \rho^{-1} \subseteq \rho^{\mathsf{S}}$. On the other hand, $\rho \cup \rho^{-1}$ is a symmetric relation containing ρ; since ρ^{S} is the smallest symmetric relation containing ρ, we have $\rho^{\mathsf{S}} \subseteq \rho \cup \rho^{-1}$. Hence $\rho^{\mathsf{S}} = \rho \cup \rho^{-1}$.

c) Since ρ^{T} contains ρ, transitivity implies that it contains $\rho^2 = \rho \circ \rho$. Transitivity again implies that ρ^{T} contains $\rho^3 = \rho \circ \rho^2$. Continuing inductively, we see that ρ^{T} contains ρ^n for all $n \in \mathbb{N}$; hence $\bigcup_{n=1}^{\infty} \rho^n \subseteq \rho^{\mathsf{T}}$. On the other hand, let $(x,y), (y,z) \in \bigcup_{n=1}^{\infty} \rho^n$. Then $(x,y) \in \rho^k$ and $(y,z) \in \rho^\ell$ for some $k, \ell \in \mathbb{N}$. So $(x,z) \in \rho^k \circ \rho^\ell = \rho^{k+\ell} \subseteq \bigcup_{n=1}^{\infty} \rho^n$. So $\bigcup_{n=1}^{\infty}$ is a transitive relation containing ρ. Since ρ^{T} is the smallest such relation, we have $\rho^{\mathsf{T}} \subseteq \bigcup_{n=1} \rho^n$. Hence $\rho^{\mathsf{T}} = \bigcup_{n=1}^{\infty} \rho^n$.

d) We have

$$
\begin{aligned}
& (\rho^{\mathsf{R}})^{\mathsf{S}} && && \text{(S.4)}\\
&= \rho^{\mathsf{R}} \cup (\rho^{\mathsf{R}})^{-1} && [\text{by definition of } {}^{\mathsf{S}}]\\
&= \rho \cup \mathrm{id}_X \cup (\rho \cup \mathrm{id}_X)^{-1} && [\text{by definition of } {}^{\mathsf{R}}]\\
&= \rho \cup \mathrm{id}_X \cup \rho^{-1} \cup \mathrm{id}_X^{-1} && [\text{by definition of converse}]\\
&= \rho \cup \rho^{-1} \cup \mathrm{id}_X && [\text{since } \mathrm{id}_X^{-1} = \mathrm{id}_X] && \text{(S.5)}\\
&= \rho^{\mathsf{S}} \cup \mathrm{id}_X && [\text{by definition of } {}^{\mathsf{S}}]\\
&= (\rho^{\mathsf{S}})^{\mathsf{R}}. && [\text{by definition of } {}^{\mathsf{R}}] && \text{(S.6)}
\end{aligned}
$$

The result is given by lines (S.4), (S.5), and (S.6).

e) Since ρ^{E} is reflexive and contains ρ, it contains ρ^{R}. Since it is symmetric and contains ρ^{R}, it contains $(\rho^{\mathsf{R}})^{\mathsf{S}}$. Since it is transitive and contains $(\rho^{\mathsf{R}})^{\mathsf{S}}$, it contains $((\rho^{\mathsf{R}})^{\mathsf{S}})^{\mathsf{T}}$. On the other hand, $((\rho^{\mathsf{R}})^{\mathsf{S}})^{\mathsf{T}}$ is transitive by the definition of ${}^{\mathsf{T}}$. Furthermore, $((\rho^{\mathsf{R}})^{\mathsf{S}})^{\mathsf{T}}$ contains $(\rho^{\mathsf{R}})^{\mathsf{S}}$, which contains ρ^{R}, which contains id_X and ρ. In particular, $((\rho^{\mathsf{R}})^{\mathsf{S}})^{\mathsf{T}}$ contains id_X and is thus reflexive. Let $(x,y) \in ((\rho^{\mathsf{R}})^{\mathsf{S}})^{\mathsf{T}} = \bigcup_{n=1}^{\infty}((\rho^{\mathsf{R}})^{\mathsf{S}})^n$. Then $(x,y) \in ((\rho^{\mathsf{R}})^{\mathsf{S}})^m$ for some $m \in \mathbb{N}$. Hence there exist $x_0, \ldots, x_n \in X$ with $x_0 = x$, $x_n = y$ and $(x_i, x_{i+1}) \in (\rho^{\mathsf{R}})^{\mathsf{S}}$ for $i = 0, \ldots, n-1$. Since $(\rho^{\mathsf{R}})^{\mathsf{S}}$ is symmetric, $(x_{i+1}, x_i) \in (\rho^{\mathsf{R}})^{\mathsf{S}}$ for each i, and so $(y,z) \in ((\rho^{\mathsf{R}})^{\mathsf{S}})^m \subseteq ((\rho^{\mathsf{R}})^{\mathsf{S}})^{\mathsf{T}}$. So $((\rho^{\mathsf{R}})^{\mathsf{S}})^{\mathsf{T}}$ is an equivalence relation containing ρ. Since ρ^{E} is the smallest equivalence relation containing ρ, we have $\rho^{\mathsf{E}} \subseteq ((\rho^{\mathsf{R}})^{\mathsf{S}})^{\mathsf{T}}$. Hence $\rho^{\mathsf{E}} = ((\rho^{\mathsf{R}})^{\mathsf{S}})^{\mathsf{T}}$.

1.20 a) For $u, v \in S$,

$$\begin{aligned}
&(u,v) \in (\rho \cup \sigma)^{\mathsf{C}} \\
\Leftrightarrow\ &(\exists p, q \in S^1, (x,y) \in \rho \cup \sigma)(u = pxq \wedge v = pyq) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{[by Proposition 1.24]} \\
\Leftrightarrow\ &(\exists p, q \in S^1, (x,y) \in \rho)(u = pxq \wedge v = pyq) \\
&\qquad \vee (\exists p, q \in S^1, (x,y) \in \sigma)(u = pxq \wedge v = pyq) \\
\Leftrightarrow\ &(u,v) \in \rho^{\mathsf{C}} \vee (u,v) \in \sigma^{\mathsf{C}} \qquad \text{[by Proposition 1.24]} \\
\Leftrightarrow\ &(u,v) \in \rho^{\mathsf{C}} \cup \sigma^{\mathsf{C}}.
\end{aligned}$$

b) For $u, v \in S$,

$$\begin{aligned}
&(u,v) \in (\rho^{-1})^{\mathsf{C}} \\
\Leftrightarrow\ &(\exists p, q \in S^1, (x,y) \in \rho^{-1})(u = pxq \wedge v = pyq) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{[by Proposition 1.24]} \\
\Leftrightarrow\ &(\exists p, q \in S^1, (y,x) \in \rho)(v = pyq \wedge u = pxq) \\
\Leftrightarrow\ &(v,u) \in \rho^{\mathsf{C}} \\
\Leftrightarrow\ &(v,u) \in (\rho^{\mathsf{C}})^{-1}.
\end{aligned}$$

1.21 Suppose S is a right zero semigroup. Let $x, y \in S$. Then $\rho_x = \rho_y \Rightarrow z\rho_x = z\rho_y \Rightarrow zx = zy \Rightarrow x = y$ and so the map $x \mapsto \rho_x$ is injective.

Suppose now that S is a left zero semigroup. Let $x, y \in S$ with $x \neq y$. Then $zx = zy$ for all $z \in S$. Hence $z\rho_x = z\rho_y$ for all $z \in S$, and so $\rho_x = \rho_y$. Thus $x \mapsto \rho_x$ is not injective.

1.22 Define a homomorphism $\varphi : S/I \to S/J$ by $[x]_I\varphi = [x]_J$. Since $I \subseteq J$, the homomorphism φ is well defined. Its image is clearly S/J. Now, $([x]_I, [y]_I) \in \ker\varphi \Leftrightarrow [x]_J = [y]_J \Leftrightarrow x, y \in J \Leftrightarrow [x]_I, [y]_I \in J/I$. Hence, by Theorem 1.21, $(S/J) \simeq (S/I)/\ker\varphi \simeq (S/I)/(J/I)$.

1.23 Notice that $IJ \subseteq IS \cap SJ \subseteq I \cap J$, so $I \cap J \neq \varnothing$. Define a homomorphism $\varphi : I \to (I \cup J)/J$ by $x\varphi = [x]_J$. Let $[y]_J \in (I \cup J)/J$. If $y \in J$ then let $z \in I \cap J$ and notice that $z\varphi = [z]_J = [y]_J$; if $y \notin J$ then $y \in I$ and $y\varphi = [y]_J$. Hence $\operatorname{im}\varphi$ is $(I \cup J)/J$. Now for any $x, y \in I$, we have $(x,y) \in \ker\varphi \Leftrightarrow [x]_J = [y]_J \Leftrightarrow x, y \in J$. Hence $(I \cup J)/J \simeq I/(I \cap J)$ by Theorem 1.21.

EXERCISES FOR CHAPTER 2

[See page 37 for the exercises.]

2.1 a) Suppose $uv = vw$. If $|v| = 0$, then let $p = \varepsilon$, $q = u$, $k = 0$. Since $v = \varepsilon$ and $u = w$, we have $u = pq$, $v = (pq)^k p$, $w = qp$. So suppose the result holds for $|v| < k$. Then if $|v| = k$, by equidivisibility we have

either $u = vs$ and $sv = w$ for some $s \in A^*$ or $ut = v$ and $v = tw$ for some $t \in A^*$. In the former case, let $p = v$, $q = s$, and $k = 0$; then $u = pq$, $v = (pq)^k p$, and $w = qp$. In the latter case, first note that if $|t| = 0$ we have $ut = tw$, with $|t| < |v|$. By the induction hypothesis, $u = pq$, $t = (pq)^k p$, and $w = qp$ for some $p, q \in A^*$ and $k \in \mathbb{N} \cup \{0\}$. Then $v = ut = (pq)^{k+1} p$. This proves the induction step.

b) Let k be maximal such that $v = u^k p$ for some $p \in A^*$. Then $u^{k+1} p = uv = vw = u^k pw$ and so by cancellativity $up = pw$. So by equivdivisibity, either p is a left factor of u or u is left factor of p. But the latter contradicts the maximality of k. Hence $u = pq$ for some $q \in A^*$. Hence $v = (pq)^k p$ and so $(pq)^{k+1} p = uv = vw = (pq)^k pw$ and so by cancellativity $w = qp$.

2.2 a) Let S be a group. Suppose $u \sim v$, then $u = xy$ and $v = yx$ for some $x, y \in S$. (Note that $S^1 = S$ since S is a group.) So $u = xy = y^{-1}yxy = y^{-1}vy$. So u and v are conjugate in the group-theoretic sense.

On the other hand, suppose $u = y^{-1}vy$. Let $x = y^{-1}v$. Then $v = yx$ and $u = y^{-1}yxy = xy$, and so $u \sim v$.

b) To show $\sim$ is reflexive, let $x = u$ and $y = 1$; then $u = xy$ and $u = yx$, so $u \sim u$. To show $\sim$ is symmetric, suppose $u \sim v$, then $u = xy$ and $v = yx$ for some $x, y \in S^1$. Interchanging x and y shows that $v \sim u$. To show $\sim$ is transitive, suppose $u \sim v$ and $v \sim w$. Then $u = xy$ and $v = yx$ for some $x, y \in S^1$, and $v = x'y'$ and $w = y'x'$ for some $x', y' \in S^1$. So $yx = x'y'$. Since S is equidivisibile, either $y = x'p$ and $px = y'$ for some $p \in S^1$, or $yq = x'$ and $x = qy'$ for some $q \in S^1$. In the former case, let $s = xx'$ and $t = p$; then $u = xy = xx'p = st$ and $w = y'x' = pxx' = ts$ and so $u \sim w$. In the latter case, let $s = q$ and $t = y'y$; then $u = xy = qy'y = st$ and $v = y'x' = y'yq = ts$ and so $u \sim w$.

c) Suppose $u \sim v$. Then $u = xy$ and $v = yx$ for some $x, y \in A^*$. Let $w = x$; then $uw = xyx = wv$.

Suppose now that $uw = wv$ for some $w \in A^*$. Then $u = xy$, $w = (xy)^k x$, $v = yx$ for some $x, y \in A^*$ by Exercise 2.1. Hence $u \sim v$.

2.3 First, notice that if $\langle u, v \rangle$ is free, then every element of $\langle u, v \rangle$ has a unique representation as a a product of elements of $\{u, v\}$; hence $uv \neq vu$.

So suppose $\langle u, v \rangle$ is not free. Without loss, assume $|u| \geq |v|$ and let $u = v^k z$, where $k \in \mathbb{N} \cup \{0\}$ is maximal and $z \in A^*$. Then there are two distinct products $x_1 \cdots x_m$ and $y_1 \cdots y_n$ (where $x_i, y_i \in \{u, v\}$) such that $x_1 \cdots x_m = y_1 \cdots y_n$. By cancellativity, assume $x_1 \neq y_1$. Interchanging the two products if necessary, assume $x_1 = u$ and $y_1 = v$. Let $h \in \mathbb{N}$ be maximal such that $y_1 = y_2 = \ldots = y_\ell = v$. Then $v^k z x_2 \cdots x_m = v^\ell y_{\ell+1} \cdots y_n$. By cancellativity, $z x_2 \cdots x_m = v^{\ell-k} y_{\ell+1} \cdots y_n$. By equidivisibility, either $z = vp$ and $p x_2 \cdots x_m = v^{\ell-k} y_{\ell+1} \cdots y_n$ for some $p \in A^*$, or $v = zq$ and $q v^{\ell-k} y_{\ell+1} \cdots y_n$. The former case is impossible since k is maximal; thus

the latter case holds. So $u = (zq)^k z$. Repeat this reasoning but focussing on u_m and v_n shows that v is a right factor of u. But since $u = (zq)^k z$ and $|v| = |z| + |q| = |qz|$, we conclude that $v = qz$. Hence $zq = v = qz$, and so $uv = (qz)^k zqz = (zq)^k zqz = zq(zq)^k z = zq(qz)^k z = vu$.

2.4 Suppose that $p_1 \dots p_k = q_1 \dots q_\ell$, where $p_i, q_i \in X$. Suppose, with the aim of obtaining a contradiction, that $k \neq \ell$. Without loss of generality, assume $k < \ell$. Let $r \in X - \{q_{k+1}\}$; such an element r exists since $|X| \geq 2$. Now, $p_1 \cdots p_k r q_1 \cdots q_\ell = q_1 \cdots q_\ell r p_1 \cdots p_k$. Both products have length $k+\ell+1$ and so their corresponding terms are equal by the supposition. In particular, $r = q_{k+1}$, which contradicts the choice of r. Hence $k = \ell$, and so by the supposition $p_i = q_i$ for all i. Since S is generated by X, this proves that S is free with basis X.

2.5 a) Let $w \in A^*$. We can find a sequence of elementary transition from w to a word $a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n}$, where each $k_i \leq 1$ as follows. First we use the defining relations $(a_i a_j, a_j a_i)$ to find a sequence from w to a word $a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n}$, where each $k_i \in \mathbb{N} \cup \{0\}$. Then we use the defining relations (a_i^2, a_i) to find a sequence from this word to one where each $k_i \leq 1$.

b) Suppose two words $a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n}$ and $a_1^{l_1} a_2^{l_2} \cdots a_n^{l_n}$, where $k_i, l_i \leq 1$, represent the same element of the monoid. Then $k_i = 1 \Leftrightarrow l_i = 1$, since every defining relation with a_i on one side has a_i on the other side.

c) Define a monoid homomorphism $\varphi : A^* \to \wp X$ to be the unique homomorphism extending $a_i \mapsto \{x_i\}$. Since the elements $\{x_i\}$ generate $\wp X$, the map φ is surjective. Since $(a_i a_j)\varphi = \{x_i\} \cup \{x_j\} = \{x_i, x_j\} = \{x_j\} \cup \{x_i\} = (a_j a_i)\varphi$ and $(a_i^2)\varphi = \{x_i\} \cup \{x_i\} = \{x_i\} = a_i \varphi$, we have $\rho \in \ker \varphi$. Since $\ker \varphi$ is a congruence, we have $\rho^\# \subseteq \ker \varphi$. Clearly, for every element Y of $\wp X$, there is a unique word $w = a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n}$, where each $k_i \leq 1$, with $w\varphi = Y$. By part b), every $\rho^\#$-class contains a unique such word. Hence $\ker \varphi = \rho^\#$. By Theorem 1.21, $A^*/\rho^\# \simeq M$.

2.6 a) Suppose $c^\gamma b^\beta$ is idempotent. If $\gamma > \beta$, then $(c^\gamma b^\beta)^2 =_B c^\gamma b^\beta c^\gamma b^\beta =_B c^{\gamma+\gamma-\beta} b^\beta \neq_B c^\gamma b^\beta$. If $\gamma < \beta$, then $(c^\gamma b^\beta)^2 =_B c^\gamma b^\beta c^\gamma b^\beta =_B c^\gamma b^{\beta+\beta-\gamma} \neq_B c^\gamma b^\beta$. Hence $\gamma = \beta$. On the other hand, $(c^\gamma b^\gamma)^2 = c^\gamma b^\gamma c^\gamma b^\gamma =_B c^\gamma b^\gamma$ and so $c^\gamma b^\gamma$ is idempotent.

b) Suppose first that c is right-invertible. Then there exists $c^\zeta b^\eta$ such that $c c^\zeta b^\eta =_B \varepsilon$. But this is impossible, since $c^{1+\zeta} b^\eta \neq \varepsilon$ since $1 + \zeta > 0$. Now suppose that $c^\gamma b^\beta$, where $\gamma \geq 1$, has a right inverse y. Then $c c^{\gamma-1} b^\beta y =_B \varepsilon$ and so c is right-invertible, which is a contradiction. Hence if $c^\gamma b^\beta$ is right-invertible, then $\gamma = 0$. On the other hand, $b^\beta c^\beta =_B \varepsilon$ and so c^β is a right inverse for b^β.

2.7 The Cayley graph $\Gamma(B, \{b, c\})$ is shown in Figure S.2.

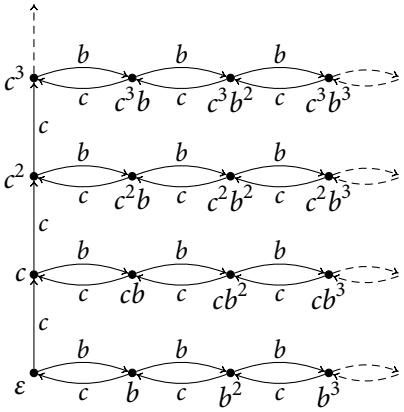


FIGURE S.2
Cayley graph of the bicyclic monoid

EXERCISES FOR CHAPTER 3

[See pages 50–51 for the exercises.]

3.1 For any $x, y, z \in S$,

$$x \mathcal{L} y \Rightarrow S^1x = S^1y \Rightarrow S^1xz = S^1yz \Rightarrow xz \mathcal{L} yz,$$

and so $\mathcal{L}$ is a right congruence. Dual reasoning shows that $\mathcal{R}$ is a left congruence.

3.2 Let G be a subgroup of a semigroup. Let $x, y \in G$. Let $p = x^{-1}y$ and $q = y^{-1}x$. Then $xp = y$ and $yq = x$. So $x \mathcal{R} y$. Similarly $x \mathcal{L} y$. Hence $x \mathcal{H} y$.

3.3 Suppose $u, v \in A^*$ are such that $u \mathcal{R} v$. Then there exist $p, q \in A^*$ such that $up = v$ and $vq = p$. Then $upq = p$, so $|u| + |p| + |q| = |u|$, and so $|p| = |q| = 0$. Thus $p = q = \varepsilon$ and so $u = v$. That is, $\mathcal{R}$ is the identity relation id_{A^*}. Similarly, the other Green's relations $\mathcal{H}$, $\mathcal{R}$, $\mathcal{D}$, and $\mathcal{J}$ are all the identity relation.

3.4 First, note that if S has a zero 0, its unique minimal ideal is $\{0\}$, which is simple. So suppose I is a minimal ideal of a semigroup S that does not contain a zero. Since $I^2 \subseteq I$ is an ideal of S and I is minimal, we have $I^2 = I$ and so $I^3 = I$.

Suppose J is an ideal of I. Let $x \in J$. Then $IxI \subseteq J$ since J is an ideal of I. Then $S^1xS^1 \subseteq I$ is an ideal of S and hence $S^1xS^1 = I$. Therefore $J \subseteq I = I^3 = IS^1xS^1I \subseteq IxI \subseteq J$ and so $J = I$. Hence I is simple.

3.5 Let $(\ell_1, r_1), (\ell_2, r_2) \in B$. Then

$$\begin{aligned}(\ell_1, r_1)\,\mathcal{R}(\ell_2, r_2) &\Rightarrow (\exists (k, s) \in B)\big((\ell_1, r_1)(k, s) = (\ell_2, r_2)\big)\\ &\Rightarrow (\exists (k, s) \in B)\big((\ell_1, s) = (\ell_2, r_2)\big)\\ &\Rightarrow \ell_1 = \ell_2.\end{aligned}$$

On the other hand, if $(\ell, r_1), (\ell, r_2) \in \{\ell\} \times R$, then $(\ell, r_1)(\ell, r_2) = (\ell, r_2)$ and $(\ell, r_2)(\ell, r_1) = (\ell, r_1)$ and so $(\ell, r_1)\,\mathcal{R}(\ell, r_2)$. So the $\mathcal{R}$-classes of B are the sets $\{\ell\} \times R$.

The result for $\mathcal{L}$-classes is proved similarly.

Finally, let $(\ell_1, r_1), (\ell_2, r_2) \in B$. Then $(\ell_1, r_1)\, \mathcal{R}(\ell_1, r_2)\, \mathcal{L}(\ell_2, r_2)$ and so $(\ell_1, r_1)\, \mathcal{D}(\ell_2, r_2)$. Hence B has a single $\mathcal{D}$-class.

3.6 If $x\, \mathcal{R}\, y$, then there exist $p, q \in S^1$ with $xp = y$ and $yq = x$. So $xpq = x$. Suppose that $pq \in S$. Then for any $z \in S$, we have $xpqz = xz$ and so $pqz = z$ by cancellativity. So pq is a left identity for S and in particular an idempotent. By Exercise 1.6, pq is an identity, which is a contradiction. So $pq \notin S$ and so $pq = 1$, the adjoined identity of S^1. Hence $p = q = 1$ and so $x = y$. Thus $\mathcal{R} = \mathrm{id}_S$. Similarly $\mathcal{L} = \mathrm{id}_S$, and so $\mathcal{H} = \mathcal{R} \cap \mathcal{L} = \mathrm{id}_S$ and $\mathcal{D} = \mathcal{R} \circ \mathcal{L} = \mathrm{id}_S$.

3.7 First, notice that if $a, b, c, d \in \mathbb{R}$ with $a, b, c, d > 0$, then

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ac & ad+b \\ 0 & 1 \end{bmatrix};$$

since $ac > 0$ and $ad + b > 0$, we see that S is a subsemigroup of $M_2(\mathbb{R})$. Let $e, f \in \mathbb{R}$ with $e, f > 0$. Then

$$\begin{aligned}
&\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} e & f \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix} \begin{bmatrix} e & f \\ 0 & 1 \end{bmatrix} \\
\Rightarrow &\begin{bmatrix} ae & af+b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ce & cf+d \\ 0 & 1 \end{bmatrix} \\
\Rightarrow\ & ae = ce \wedge af + b = cf + d \\
\Rightarrow\ & a = c \wedge af + b = af + d \\
\Rightarrow\ & a = c \wedge b = d \\
\Rightarrow &\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix}
\end{aligned}$$

and

$$\begin{aligned}
&\begin{bmatrix} e & f \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} e & f \\ 0 & 1 \end{bmatrix} \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix} \\
\Rightarrow &\begin{bmatrix} ea & eb+f \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ec & ed+f \\ 0 & 1 \end{bmatrix} \\
\Rightarrow\ & ea = ec \wedge eb + f + ed + f \\
\Rightarrow\ & a = c \wedge d = f \\
\Rightarrow &\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix}.
\end{aligned}$$

Hence S is cancellative. Furthermore,

$$\begin{aligned}
&\begin{bmatrix} e & f \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \\
\Rightarrow &\begin{bmatrix} ea & eb+f \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}
\end{aligned}$$

$$\Rightarrow ea = a \wedge eb + f = b$$
$$\Rightarrow e = 1 \wedge eb + f = b$$
$$\Rightarrow e = 1 \wedge f = 0,$$

which shows that S does not contain an identity. Finally, let $g, h \in \mathbb{R}$ with $g, h > 0$. Choose $f = 1$, $d = 0$,$c = h/(a + b)$, and $e = g/ca$. Then $c, d, e, f > 0$ and

$$\begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} e & f \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} cae & caf + cb + d \\ 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} ca(g/ca) & (h/(a+b))a + (h/(a+b))b \\ 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} g & h \\ 0 & 1 \end{bmatrix}.$$

Thus for any $x \in S$, we have $SxS = S$ and so S is simple. Hence $S = \mathcal{J} \times \mathcal{J}$.

3.8 a) Suppose $\sigma \mathcal{L} \tau$. Then there exist $\pi, \rho \in \mathcal{T}_X$ such that $\pi\sigma = \tau$ and $\rho\tau = \sigma$. Therefore $\operatorname{im}\sigma \subseteq \operatorname{im}(\pi\sigma) = \operatorname{im}\tau$ and $\operatorname{im}\tau \subseteq \operatorname{im}(\rho\tau) = \operatorname{im}\sigma$. Hence $\operatorname{im}\sigma = \operatorname{im}\tau$.

Now suppose $\operatorname{im}\sigma = \operatorname{im}\tau$. For each $x \in X$, we have $x\tau \in \operatorname{im}\tau = \operatorname{im}\sigma$ and we can define $x\pi$ be some element of X such that $(x\pi)\sigma = x\tau$. Then $\pi\sigma = \tau$. Similarly we can define $\rho \in \mathcal{T}_X$ so that $\rho\tau = \sigma$. Hence $\sigma \mathcal{L} \tau$.

b) Suppose $\sigma \mathcal{R} \tau$. Then there exist $\pi, \rho \in \mathcal{T}_X$ such that $\sigma\pi = \tau$ and $\tau\rho = \sigma$. Therefore $(x, y) \in \ker\sigma \Rightarrow x\sigma = y\sigma \Rightarrow x\sigma\pi = y\sigma\pi \Rightarrow x\tau = y\tau \Rightarrow (x, y) \in \ker\tau$. Thus $\ker\sigma \subseteq \ker\tau$. Similarly, $\ker\tau \subseteq \ker\sigma$. Hence $\ker\sigma = \ker\tau$.

Now suppose $\ker\sigma = \ker\tau$. Let $x \in \operatorname{im}\sigma$, and for all $y \in X$ such that $y\sigma = x$, define $x\pi = y\tau$. (Note that $x\pi$ is well-defined since $\ker\sigma = \ker\tau$.) For $x \notin \operatorname{im}\sigma$, let $x\pi$ be arbitrary. Then $y\sigma\pi = x\pi = y\tau$ for all $y \in X$ and so $\sigma\pi = \tau$. Similarly, we can define $\rho \in \mathcal{T}_X$ so that $\tau\rho = \sigma$. Hence $\sigma \mathcal{R} \tau$.

c) Suppose $\sigma \mathcal{D} \tau$. Then there exists $\upsilon \in \mathcal{T}_X$ such that $\sigma \mathcal{L} \upsilon \mathcal{R} \tau$. Since $\upsilon \mathcal{R} \tau$, there exist $\pi, \rho \in \mathcal{T}_X$ such that $\upsilon\pi = \tau$ and $\tau\rho = \upsilon$. Hence $\tau\rho\pi = \tau$ and $\upsilon\pi\rho = \upsilon$. Therefore $\rho|_{\operatorname{im}\tau} : \operatorname{im}\tau \to \operatorname{im}\upsilon$ and $\pi|_{\operatorname{im}\upsilon} : \operatorname{im}\upsilon \to \operatorname{im}\tau$ are mutually inverse bijections. So $|\operatorname{im}\upsilon| = |\operatorname{im}\tau|$. Since $\sigma \mathcal{L} \upsilon$, we have $\operatorname{im}\sigma = \operatorname{im}\upsilon$ and thus $|\operatorname{im}\sigma| = |\operatorname{im}\tau|$.

Now suppose $|\operatorname{im}\sigma| = |\operatorname{im}\tau|$. Then there is a bijection $\mu : \operatorname{im}\sigma \to \operatorname{im}\tau$. Extend μ to a map $\pi \in \mathcal{T}_X$ by defining $x\pi$ arbitrarily for $x \in X - \operatorname{im}\sigma$. Similarly extend μ^{-1} to a map $\rho \in \mathcal{T}_X$. Let $\upsilon = \sigma\pi$. Then $\upsilon\rho = \sigma$, so $\upsilon \mathcal{R} \sigma$. Furthermore $\operatorname{im}\upsilon = \operatorname{im}(\sigma\pi) = \operatorname{im}(\sigma\mu) = \operatorname{im}\tau$, so $\upsilon \mathcal{L} \sigma$. Hence $\sigma \mathcal{D} \tau$.

Suppose $\sigma \mathcal{J} \tau$. Then there exist π, ρ, π', ρ' such that $\sigma = \pi\tau\rho$ and $\tau = \pi'\sigma\rho'$. Therefore $|\operatorname{im}\sigma| = |X\sigma| = |X\pi\tau\rho| \leq |X\tau\rho| \leq$

$|X\tau| = |\operatorname{im}\tau|$; similarly $|\operatorname{im}\tau| \leq |\operatorname{im}\sigma|$. Thus $|\operatorname{im}\sigma| = |\operatorname{im}\tau|$. Hence $\sigma \mathcal{D} \tau$. Therefore $\mathcal{J} \subseteq \mathcal{D}$ and so $\mathcal{D} = \mathcal{J}$.

3.9 First, let $x, y \in \{c^\gamma b^\beta : \beta \in \mathbb{N} \cup \{0\}\}$. Interchanging x and y if necessary, suppose $x = c^\gamma b^\beta$ and $y = c^\gamma b^\delta$ where $\beta \leq \delta$. Then $xb^{\delta-\beta} = y$ and $yc^{\delta-\beta} = x$. Hence $x \mathcal{R} y$.

Now suppose $c^\gamma b^\beta \mathcal{R} c^{\gamma+\eta} b^\delta$ for some $\eta > 0$. Then since $\mathcal{R}$ is a left congruence, we have $b^\beta =_B b^\gamma c^\gamma b^\beta \mathcal{R} b^\gamma c^{\gamma+\eta} b^\delta =_B c^\eta b^\delta$. Therefore there exists $p \in B$ such that $c^\eta b^\delta p =_B b^\beta$. Hence $c^\eta b^\delta p c^\beta =_B \varepsilon$ and so c^η is right-invertible, which contradicts Exercise 2.6(b). Hence $\{c^\gamma b^\beta : \beta \in \mathbb{N} \cup \{0\}\}$ is an $\mathcal{R}$-class. Similarly, $\mathcal{L}$-classes are of the form $\{c^\gamma b^\beta : \gamma \in \mathbb{N} \cup \{0\}\}$. Finally, note that $c^\gamma b^\beta \mathcal{R} c^\gamma b^\delta \mathcal{L} c^\eta b^\delta$ and so $c^\gamma b^\beta \mathcal{D} c^\eta b^\delta$. Thus B consists of a single $\mathcal{D}$-class.

3.10 Let $e \in L \cap R$ be idempotent. Then e is a right identity for L and a left identity for R. For any $y \in R$, we have $ey = y$ and so $\rho_y|_L$ is a bijection from L to L_y. Let $z \in D$. Choose $y \in R \cap L_z$. Since $\rho_y|_L$ is a bijection, there exists $x \in L$ such that $z = x\rho_y|_L = xy \in LR$. Hence $D \subseteq LR$. Let $x \in L$ and $y \in R$. Since $L \cap R$ contains the idempotent e, we have $xy \in L_y \cap R_x \subseteq D$ by Proposition 3.16.

3.11 a) Let $x \in S$. Since S is right simple, $xS = S$. So there exists $e \in S$ such that $xe = x$. Thus $xe^2 = xe = x$ and by left-cancellativity, $e^2 = e$. So S contains an idempotent.

b) Let $e \in S$ be an idempotent. Let $y \in S$. Then $y \in S = eS = ez$ for some $z \in S$, and so $ey = e^2 z = ez = y$ and so e is a left identity for S. In particular, the set of idempotents E forms a right zero subsemigroup.

Let $y \in Se$. Then $y = ze$ for some $z \in S$ and so $ye = ze^2 = ze = y$ and so e is both a right and left identity for Se. Let $y \in Se$. Since $yS = S$, there exists $y' \in S$ with $yy' = e$. Then $y'e \in Se$ and $y(y'e) = e^2 = e$, so $y'e$ is a right inverse of y in Se. Finally, $(y'e)y(y'e)y = y'e^2y = (y'e)y$ and so $(y'e)y = e$ by left-cancellativity in $Se \subseteq S$. So $(y'e)$ is a left inverse of y and so Se is a subgroup.

To see that the map $\varphi : G \times E \to S$ is a homomorphism, note that since every element of E is a left identity for S, we have $((g,e)\varphi)((g',e')\varphi) = geg'e' = gg'e' = (gg',e')\varphi = ((g,e)(g',e'))\varphi$. Suppose $(g,e)\varphi = (g',e')\varphi$. Then $ge = g'e'$, and so $g = g1_G = ge1_G = g'e'1_G = g'1_G = g'$, since E is a right zero subsemigroup. By left-cancellativity, $e = e'$. Hence φ is injective. Finally, let $x \in S$. We have already shown that there is an idempotent e with $xe = x$. Then $(x1_G, e)\varphi = x1_G e = xe = x$, again since E is a right zero subsemigroup. So φ is surjective. Hence φ is an isomorphism.

c) Let $(g,x),(h,y),(i,z) \in G \times Z$. Then

$$\begin{aligned} & (i,z)(g,x) = (i,z)(h,y) \\ \Rightarrow\ & (ig,x) = (ih,y) \\ \Rightarrow\ & ig = ih \wedge x = y \\ \Rightarrow\ & g = h \wedge x = y \\ \Rightarrow\ & (g,x) = (h,y). \end{aligned}$$

So $G \times Z$ is left-cancellative. Furthermore, $(g,x)(g^{-1}h,y) = (h,y)$ and so $(g,x)(G \times Z) = G \times Z$ for all $(g,x) \in G \times Z$. Hence $G \times Z$ is right simple. Thus $G \times Z$ is a right group. Combining parts a) and b) shows that every right group is isomorphic to $G \times Z$ for some group G and right zero semigroup Z.

3.12 Let R be a right ideal of S. Let $r \in R$ and $\ell \in G$. Then $r\ell \in R \cap G$ since R is a right ideal and G is a left ideal. So $R \cap G \neq \varnothing$. Then $R \cap G$ is a right ideal of G, since R is a right ideal and G is a subgroup. But G is a group, and thus its only right ideal is G itself. Hence $R \cap G = G$, and so $G \subseteq R$. In particular, $1_G \in R$. Let $x \in S$. Then $1_G x = 1_G 1_G x$ since 1_G is idempotent, and so $x = 1_G x$ since S is left-cancellative. Therefore $x = 1_G x \in 1_G S \subseteq RS = R$. Hence $S \subseteq R$ and so $S = R$. Therefore S does not contain any proper right ideals and so is right simple. Since it is also left-cancellative, S is a right group.

3.13 a) Let L be a minimal left ideal of S. Let $x \in S$. Then Lx is a left ideal. Let K be a left ideal contained in Lx. Let $J = \{y \in L : yx \in K\}$. Then J is a left ideal and $J \subseteq L$. Since L is minimal, $J = L$. So $K = Jx = Lx$. So Lx is minimal. Let $M = \bigcup\{Lx : x \in S\}$. Then M is a union of left ideals and thus itself a left ideal. Let $m \in M$ and $z \in S$. Then $m \in Lx$ for some $x \in S$. So $mz \in Lxz \subseteq M$. So M is a right ideal and therefore an ideal. Since S is simple, $S = M$.

b) The idempotent e lies in Lx for some x. Since Lx is a left ideal, $Se \subseteq Lx$. Since Lx is minimal, $Se = Lx$. So Se is a minimal left ideal of S. Suppose K is a left ideal of Se. Then $SK \subseteq SeK \subseteq K$ and so K is a left ideal of S. Since Se is a minimal left ideal of S, we have $K = Se$. Therefore Se is left simple.

Let $f \in Se$ be idempotent. Then $Sef = Se$ since Se is minimal. Let $y \in Se$. Then $y \in Sef = Se$ and so $y = y'f$ for some $y' \in Se$. So $yf = y'f^2 = y'f = y$. So every idempotent in Se is a right identity for Se.

Suppose that $xz = yz$ for $x,y,z \in Se$. Now $Sez = Se$ since Se is minimal and so $z'z = e$ for some $z' \in Se$. Let $f = zz'$. Then $f^2 = zz'zz' = zez' = zz' = f$ since e is a right identity for Se. Since $f \in Se$ is idempotent, it is also a right identity for z. Then $x = xf = xzz' = yzz' = yf = y$. Therefore Se is right-cancellative. Hence Se is a left group.

c) Let $z \in eSe$. Then $z = epe$ for some $p \in S$ and so $ez = e^2pe = epe = z$. So e is a left identity for eSe. It is a right identity for $Se \supseteq eSe$, and so a (two-sided) identity for eSe. As noted above, there exists $z' \in Se$ such that $z'z = e$. Then $ez' \in eSe$ and $(ez')z = e^2 = e$. Finally, $z(ez')z(ez') = ze(ez') = z(ez')$ and so $z(ez') = e$ by right-cancellativity in $sSe \subseteq Se$. So ez' is a left and right inverse of z in eSe and so eSe is a group.

d) Let K be a right ideal of S with $K \subseteq eS$. Let $x \in K$. Then $x = ey$ for some $y \in S$. Let $ey'e$ be the inverse of eye in the subgroup eSe. Then $x(ey'e) = eyey'e = (eye)(ey'e) = e$. Hence $e \in K$ since K is a right ideal. Therefore $eS \subseteq K$ and so $K = eS$. Therefore eS is a minimal right ideal.

EXERCISES FOR CHAPTER 4

[See pages 63–64 for the exercises.]

4.1 Clearly $\operatorname{im}\varphi$ is a semigroup; we have to show it is inverse. Let $x \in \operatorname{im}\varphi$. Then there exists $y \in S$ with $y\varphi = x$. Since S is regular, there exists an inverse y^{-1} for y. Let $x' = y^{-1}\varphi$. Then $xx'x = (y\varphi)(y^{-1}\varphi)(y\varphi) = (yy^{-1}y)\varphi = y\varphi = x$ and similarly $x'xx' = x$. So x' is an inverse for x. Therefore $\operatorname{im}\varphi$ is regular. Let $g = fxf$. Since x is an inverse of f^2, we have $xf^2x = x$ and $f^2xf^2 = f^2$. Then $g^2 = f(xf^2x)f = fxf = g$ and so g is idempotent. Furthermore

$$\begin{aligned}
g\varphi &= (fxf)\varphi && \text{[by choice of } g\text{]}\\
&= (f\varphi)(x\varphi)(f\varphi) && \text{[since } \varphi \text{ is a homomorphism]}\\
&= e(x\varphi)e && \text{[since } e = f\varphi\text{]}\\
&= e^2(x\varphi)e^2 && \text{[since } e \text{ is idempotent]}\\
&= (f\varphi)^2(x\varphi)(f\varphi)^2 && \text{[since } e = f\varphi\text{]}\\
&= (f^2xf^2)\varphi && \text{[since } \varphi \text{ is a homomorphism]}\\
&= (f^2\varphi) && \text{[since } f^2xf^2 = f^2\text{]}\\
&= (f\varphi)^2 && \text{[since } \varphi \text{ is a homomorphism]}\\
&= e^2 && \text{[since } f\varphi = e\text{]}\\
&= e. && \text{[since } e \text{ is idempotent]}
\end{aligned}$$

4.2 a) Define $\varphi : G \to \mathcal{M}[G; I, \Lambda; P]$ by $x \mapsto (1, xp_{11}^{-1}, 1)$. Then

$$\begin{aligned}
(x\varphi)(y\varphi) &= (1, xp_{11}^{-1}, 1)(1, yp_{11}^{-1}, 1)\\
&= (1, xp_{11}^{-1}p_{11}yp_{11}^{-1}, 1)\\
&= (1, xyp_{11}^{-1}, 1)\\
&= (xy)\varphi.
\end{aligned}$$

So φ is a homomorphism. Furthermore,

$$x\varphi = y\varphi \Rightarrow (1, xp_{11}^{-1}, 1)(1, yp_{11}^{-1}, 1) \Rightarrow xp_{11}^{-1} = yp_{11}^{-1} \Rightarrow x = y.$$

So φ is injective. Finally, since G is a group, $(1, xp_{11}^{-1}, 1)$ will range over $\mathcal{M}[G; I, \Lambda, P]$ as x ranges over G. So φ is surjective. Hence φ is an isomorphism.

b) Let $M = \{e, z\}$ be a semilattice with $e > z$. Let $p_{\lambda i} = z$. Let (i, x, λ) and (i, y, λ) be arbitrary elements of $\mathcal{M}[M; I, \Lambda; P]$. Then

$$(i, x, \lambda)(i, y, \lambda) = (i, xp_{\lambda i}y, \lambda) = (i, xzy, \lambda) = (i, z, \lambda).$$

So $\mathcal{M}[M; I, \Lambda; P]$ is a null semigroup and so not isomorphic to M.

4.3 a) Let $(i, x, \lambda)\ \mathcal{L}\ (j, x, \mu)$. Then there exists $s \in S^1$ such that $s(i, x, \lambda) = (j, x, \mu)$. If $s = 1$, then $(i, x, \lambda) = (j, x, \mu)$ and in particular $\lambda = \mu$. If $s = (k, z, v) \in S$, then $(j, x, \mu) = s(i, x, \lambda) = (k, zp_{vi}x, \lambda)$ and so $\lambda = \mu$. Hence $L_{(i,x,\lambda)} \subseteq I \times G \times \{\lambda\}$. On the other hand, let $(i, x, \lambda), (j, y, \lambda) \in I \times G \times \{\lambda\}$. Let $s = (i, xy^{-1}p_{\lambda j}^{-1}, \lambda)$ and $t = (j, yx^{-1}p_{\lambda i}^{-1}, \lambda)$. Then

$$s(j, y, \lambda) = (i, xy^{-1}p_{\lambda j}^{-1}, \lambda)(j, y, \lambda) = (i, xy^{-1}p_{\lambda j}^{-1}p_{\lambda j}y, \lambda) = (i, x, \lambda)$$

and similarly $t(i, x, \lambda) = (j, y, \lambda)$. Hence $I \times G \times \{\lambda\} \subseteq L_{(i,x,\lambda)}$. So the $\mathcal{L}$-classes are subsets of the form $I \times G \times \{\lambda\}$.

b) The reasoning is dual to part a).

c) For $(i, x, \lambda) \in S$, we have $H_{(i,x,\lambda)} = L_{(i,x,\lambda)} \cap R_{(i,x,\lambda)} = (I \times G \times \{\lambda\}) \times (\{i\} \times G \times \Lambda) = \{i\} \times G \times \{\lambda\}$.

4.4 A completely simple semigroup is isomorphic to $\mathcal{M}[G; I, \Lambda; P]$ for some group G, index sets I and Λ, and matrix P. Suppose that we have $(i_1, g_1, \lambda_1)(i_2, g_2, \lambda_2) = (j_1, h_1, \mu_1)(j_2, h_2, \mu_2)$. Then $(i_1, g_1p_{\lambda_1 i_2}g_2, \lambda_2) = (j_1, h_1p_{\mu_1 j_2}h_2, \mu_2)$, and so

$$i_1 = j_1, \tag{S.7}$$
$$\lambda_2 = \mu_2, \tag{S.8}$$
$$g_1p_{\lambda_1 i_2}g_2 = h_1p_{\mu_1 j_2}h_2. \tag{S.9}$$

Let $q = (j_2, p_{\mu_1 j_2}^{-1}h_1^{-1}g_1, \lambda_1)$. Then

$$\begin{aligned}
(j_1, h_1, \mu_1)q &= (j_1, h_1, \mu_1)(j_2, p_{\mu_1 j_2}^{-1}h_1^{-1}g_1, \lambda_1) && \text{[by definition of } q\text{]} \\
&= (j_1, h_1p_{\mu_1 j_2}p_{\mu_1 j_2}^{-1}h_1^{-1}g_1, \lambda_1) \\
&= (j_1, g_1, \lambda_1) \\
&= (i_1, g_1, \lambda_1) && \text{[by (S.7)]}
\end{aligned}$$

and

$$\begin{aligned} q(i_2,g_2,\lambda_2) &= (j_2, p^{-1}_{\mu_1 j_2} h_1^{-1} g_1, \lambda_1)(i_2,g_2,\lambda_2) && \text{[by definition of } q\text{]} \\ &= (j_2, p^{-1}_{\mu_1 j_2} h_1^{-1} g_1 p_{\lambda_1 i_2} g_2, \lambda_2) \\ &= (j_2, p^{-1}_{\mu_1 j_2} h_1^{-1} h_1 p_{\mu_1 j_2} h_2, \mu_2) && \text{[by (S.8) and (S.9)]} \\ &= (j_2, h_2, \mu_2). \end{aligned}$$

Hence $\mathcal{M}[G;I,\Lambda;P]$ is equidivisible.

4.5 a) Let $x,y \in S \simeq \mathcal{M}[G;I,\Lambda;P]$ with $x \mathcal{L} y$. Then by Exercise 4.3, $x = (i,g,\lambda)$, $y = (j,h,\lambda)$ for some $i,j \in I$, $g,h \in G$, $\lambda \in \Lambda$.. Let $z = (k,f,\mu) \in S$. Then $zx = (k, fp_{\mu i} g, \lambda)$ and $zy = (k, fp_{\mu j} h, \lambda)$. Since $zx, zy \in I \times G \times \{\lambda\}$, we have $zx \mathcal{L} zy$. Hence $\mathcal{L}$ is left compatible. We already know $\mathcal{L}$ is a right congruence by Proposition 3.3(a). So $\mathcal{L}$ is a congruence. Similarly, $\mathcal{R}$ is a congruence and so $\mathcal{H} = \mathcal{L} \cap \mathcal{R}$ is a congruence.

b) Let $[(i,g,\lambda)]_{\mathcal{L}}, [(j,j,\mu)]_{\mathcal{L}} \in S/\mathcal{L}$. Then $[(i,g,\lambda)]_{\mathcal{L}}[(j,h,\mu)]_{\mathcal{L}} = [(i, gp_{\lambda j} h, \mu)]_{\mathcal{L}} = [(j,h,\mu)]_{\mathcal{L}}$ (since $(i,gp_{\lambda j}h,\mu)\,\mathcal{L}\,(j,h,\mu)$). Hence $S/\mathcal{L}$ is a right zero semigroup. Similarly $S/\mathcal{R}$ is a left zero semigroup.

c) Define a map $\varphi : S/\mathcal{H} \to S/\mathcal{R} \times S/\mathcal{L}$ by

$$[(i,g,\lambda)]_{\mathcal{H}}\varphi = \big([(i,g,\lambda)]_{\mathcal{R}}, [(i,g,\lambda)]_{\mathcal{L}}\big).$$

This map is well-defined and injective since $\mathcal{H} = \mathcal{L} \cap \mathcal{R}$. It is clearly surjective, and is a homomorphism by definition. So $S/\mathcal{H} \simeq S/\mathcal{R} \times S/\mathcal{L}$.

4.6 Since S is completely simple, $S \simeq \mathcal{M}[G;I,\Lambda,P]$. Hence $|S| = |I| \times |G| \times |\Lambda|$.

a) Since $p = |I| \times |G| \times |\Lambda|$, one of the following three cases must hold:

i) $|I| = p$, $|G| = 1$, and $|\Lambda| = 1$. Since G is trivial and $|\Lambda| = 1$, the $\mathcal{R}$-classes of S are single elements by Exercise 4.3(b). Thus $S \simeq S/\mathcal{R}$ is a left zero semigroup by Exercise 4.5(b).

ii) $|I| = 1$, $|G| = 1$, and $|\Lambda| = p$. This is similar to case i), and shows that S is a right zero semigroup.

iii) $|I| = 1$, $|G| = p$, and $|\Lambda| = 1$. Then S is a group by Exercise 4.2.

b) Since $pq = |I| \times |G| \times |\Lambda|$, one of the following cases must hold (interchanging p and q if necessary):

i) $|I| = pq$, $|G| = 1$, and $|\Lambda| = 1$. As in part a)i), $S \simeq S/\mathcal{R}$ is a left zero semigroup and so a left group.

ii) $|I| = p$, $|G| = q$, and $|\Lambda| = 1$. Then $S = I \times G \times \{\lambda\}$. Thus

$$\begin{aligned} &(i,x,\lambda)(k,z,\lambda) = (j,y,\lambda)(k,z,\lambda) \\ \Rightarrow &(i, xp_{\lambda k} z, \lambda) = (j, yp_{\lambda k} z, \lambda) \end{aligned}$$

$\Rightarrow i = j \wedge xp_{\lambda k}z = yp_{\lambda k}z$
$\Rightarrow i = j \wedge x = y$ [by cancellation in G]
$\Rightarrow (i,x,\lambda) = (j,y,\lambda)$.

So S is right-cancellative. Since S consists of a single $\mathcal{L}$-class, $S = Sx$ for all $x \in S$ and so S does not contain a proper left ideal. So S is left simple and right-cancellative and so a left group.

iii) $|I| = p$, $|G| = 1$, and $|\Lambda| = q$. Then the $\mathcal{H}$-classes of S are single elements by Exercise 4.3(c). So $S \simeq S/\mathcal{H}$ is a rectangular band by Exercise 4.5(c)

iv) $|I| = 1$, $|G| = pq$, and $|\Lambda| = 1$. As in part a)iii), S is a group (and thus both a left and a right group).

v) $|I| = 1$, $|G| = p$, and $|\Lambda| = q$. This is similar to case ii), and shows that S is a right group.

vi) $|I| = 1$, $|G| = 1$, and $|\Lambda| = pq$. As in part a)ii), $S \simeq S/\mathcal{L}$ is a right zero semigroup and so a right group.

4.7 a) Let $z \in S$. Then $zz^{-1}\,\mathcal{R}\,z$ and $z^{-1}z\,\mathcal{L}\,z$. So $zz^{-1} = z^{-1}z\,\mathcal{H}\,z$. Similarly $zz^{-1} = z^{-1}z\,\mathcal{H}\,z^{-1}$. So $z\,\mathcal{H}\,z^{-1}$. Since every $\mathcal{H}$-class of S is a subgroup, z^{-1} is the unique group inverse of z in this subgroup. The $\mathcal{H}$-class of $z\varphi$ is also a subgroup and $(z\varphi)^{-1}$ is the unique group inverse of $z\varphi$ in this subgroup. Then $\varphi|_H$ is a group homomorphism into the subgroup $H_{z\varphi}$ and so $z^{-1}\varphi = (z\varphi)^{-1}$.

b) There are many possible examples. Let $S = \{s_1, s_2\}$ and $T = \{t_1, t_2\}$ be left zero semigroups. Define $^{-1}$ on S by $s_1^{-1} = s_2$ and $s_2^{-1} = s_1$. Define $^{-1}$ on T by $t_i^{-1} = t_i$. In both cases, $^{-1}$ satisfies $(x^{-1})^{-1} = x$ and $xx^{-1}x = x$. Define $\varphi : S \to T$ by $s_i\varphi = t_i$. Then $(s_1\varphi)^{-1} = t_1^{-1} = t_1$ but $s_1^{-1}\varphi = s_2\varphi = t_2$.

4.8 a) i) The isomorphism φ maps non-zero $\mathcal{R}$-classes bijectively onto non-zero $\mathcal{R}$-classes. Since the $\mathcal{R}$-classes of $\mathcal{M}_0[G;I,\Lambda;P]$ are sets of the form $\{i\}\times G\times\Lambda$ and the $\mathcal{R}$-classes of $\mathcal{M}_0[H;J,\mathrm{M};Q]$ are sets of the form $\{j\} \times G \times \mathrm{M}$, there must be a bijection $\alpha : I \to J$ such that $(i,a,\lambda)\varphi \in \{i\alpha\} \times H \times \mathrm{M}$. Similarly there is a bijection $\beta : \Lambda \to \mathrm{M}$ such that $(i,a,\lambda)\varphi \in I \times H \times \{\lambda\beta\}$. Combining these statements shows that $(i,a,\lambda)\varphi \in \{i\alpha\}\times H\times \{\lambda\beta\}$. Since φ must map group $\mathcal{H}$-classes to group $\mathcal{H}$-classes, we have $p_{\lambda i} \neq 0$ if and only if $p_{(\lambda\beta)(i\alpha)} \neq 0$.

ii) Let $\gamma : G \to \{1\} \times G \times \{1\}$ be defined by $x\gamma = (1, p_{11}^{-1}x, 1)$. Then $(x\gamma)(y\gamma) = (1,p_{11}^{-1}x,1)(1,p_{11}^{-1}y,1) = (1,p_{11}^{-1}xp_{11}p_{11}^{-1}y,1) = (1,p_{11}^{-1}xy,1) = (xy)\gamma$, so γ is a homomorphism. Furthermore, γ is injective since $x\gamma = y\gamma \Rightarrow (1,p_{11}^{-1}x,1) = (1,p_{11}^{-1}y,1) \Rightarrow p_{11}^{-1}x = p_{11}^{-1}y \Rightarrow x = y$. Finally, γ is surjective since for any $(1,x,1) \in \{1\} \times G \times \{1\}$, we have $(p_{11}x)\gamma = (1,x,1)$. So γ is an isomorphism.

Similarly, the map $\eta : H \to \{1\alpha\} \times H \times \{1\beta\}$ defined by $x\eta = (1\alpha, p_{(1\beta)(1\alpha)}^{-1} x, 1\beta)$ is an isomorphism.

By part a), $\varphi|_{\{1\}\times G\times\{1\}} : \{1\}\times G\times\{1\} \to \{1\alpha\}\times H\times\{1\beta\}$ is an isomorphism, so the composition $\theta = \gamma\varphi\eta^{-1} = \gamma\varphi|_{\{1\}\times G\times\{1\}}\eta^{-1}$ is an isomorphism from G to H.

iii) First,

$$(i,x,\lambda) = (i, 1_G p_{11} p_{11}^{-1} x p_{11} p_{11}^{-1}) = (i,1_G,1)(1,p_{11}^{-1}x,1)(1,p_{11}^{-1},1).$$

Now, for all $x \in G$,

$$(1,p_{11}^{-1}x,1)\varphi = x\gamma\varphi_{\{1\}\times H\times\{1\}} = x\theta\eta = (1\alpha, q_{(1\beta)(1\alpha)}^{-1}(x\theta), 1\beta)$$

Therefore for any $x \in G$,

$$\begin{aligned}
&= (i,x,\lambda)\varphi \\
&= \big((i,1_G,1)(1,p_{11}^{-1}x,1)(1,p_{11}^{-1},\lambda)\big)\varphi \\
&= (i,1_G,1)\varphi(1,p_{11}^{-1}x,1)\varphi(1,p_{11}^{-1},\lambda)\varphi \\
&= (i\alpha,u_i,1\beta)(1\alpha,q_{(1\beta)(1\alpha)}^{-1}(x\theta),1\beta)(1\alpha,q_{(1\beta)(1\alpha)}^{-1}v_\lambda,\lambda\beta)\varphi \\
&= (i\alpha,u_i q_{(1\beta)(1\alpha)} q_{(1\beta)(1\alpha)}^{-1}(x\theta) q_{(1\beta)(1\alpha)} q_{(1\beta)(1\alpha)}^{-1} v_\lambda,\lambda\beta)\varphi \\
&= (i\alpha,u_i(x\theta)v_\lambda,\lambda\beta)\varphi.
\end{aligned}$$

Hence

$$\begin{aligned}
&(i\alpha,u_i p_{\lambda i}\theta v_\lambda,\lambda\beta) \\
&= (i,p_{\lambda i},\lambda)\varphi \\
&= \big((i,1_G,\lambda)(i,1_G,\lambda)\big)\varphi \\
&= (i,1_G,\lambda)\varphi(i,1_G,\lambda)\varphi \\
&= (i\alpha,u_i v_\lambda,\lambda)(i\alpha,u_i v_\lambda,\lambda\beta) \\
&= (i\alpha,u_i v_\lambda q_{(\lambda\beta)(i\alpha)} u_i v_\lambda,\lambda\beta);
\end{aligned}$$

thus $p_{\lambda i} = v_\lambda q_{(\lambda\beta)(i\alpha)} u_i$.

b) Define a map $\varphi : \mathcal{M}_0[G;I,\Lambda;P] \to \mathcal{M}_0[H;J,\mathrm{M};Q]$ by $(i,x,\lambda)\varphi = (i\alpha,u_i(x\theta)v_\lambda,\lambda\beta)$ and $0\varphi = 0$. Then φ is a homomorphism since

$$\begin{aligned}
&(i,x,\lambda)\varphi(i',y,\lambda')\varphi \\
&= (i\alpha,u_i(x\theta)v_\lambda,\lambda\beta)(i'\alpha,u_{i'}(y\theta)v_{\lambda'},\lambda') \\
&= (i\alpha,u_i(x\theta)v_\lambda q_{(\lambda\beta)(i'\alpha)} u_{i'}(y\theta)v_{\lambda'},\lambda') \\
&= (i\alpha,u_i(x\theta)(p_{\lambda i'}\theta)(y\theta)v_{\lambda'},\lambda') \\
&= (i\alpha,u_i((xp_{\lambda i'}y)\theta)v_{\lambda'},\lambda') \\
&= (i,xp_{\lambda i'}y,\lambda')\varphi \\
&= \big((i,x,\lambda)(i',y,\lambda')\big)\varphi.
\end{aligned}$$

Furthermore, φ is a bijection since α, β, and θ are all bijections. So φ is an isomorphism from $\mathcal{M}_0[G;I,\Lambda;P]$ to $\mathcal{M}_0[H;J,\mathrm{M};Q]$.

4.9 Suppose P is regular. Then $S = \mathcal{M}_0[G; I, \Lambda; P]$ is completely simple and so regular by the proof of Proposition 4.3. [Alternatively: Since P contains some non-zero element $p_{\lambda i}$, the element $(i, p_{\lambda i}^{-1}, \lambda)$ is idempotent and thus regular. Thus the $\mathcal{D}$-class $I \times G \times \Lambda$ is regular by Proposition 3.17.]

Suppose P is not regular. Then P has a row of a column all of whose entries are 0. Suppose all the entries in the row indexed by λ are 0; the reasoning for columns is similar. Let $(i, x, \lambda) \in \mathcal{M}_0[G; I, \Lambda; P] - \{0\}$. Then for any $(j, y, \mu) \in \mathcal{M}_0[H; I, \Lambda; P] - \{0\}$, we have $(i, x, \lambda)(j, y, \mu) = 0$ since $p_{\lambda j} = 0$. Hence there is no element $z \in \mathcal{M}_0[H; I, \Lambda; P]$ with $(i, x, \lambda)z(i, x, \lambda) = (i, x, \lambda)$. Thus S is not regular.

EXERCISES FOR CHAPTER 5

[See page 78 for the exercises.]

5.1 Let $\tau = \begin{pmatrix} 1 & 2 \\ 2 & * \end{pmatrix}$ and $\zeta = \begin{pmatrix} 1 & 2 \\ * & * \end{pmatrix}$. Then $\tau\tau = \tau\zeta = \zeta\tau = \zeta\zeta = \zeta$. So $T = \{\tau, \zeta\}$ is a null semigroup and τ does not have an inverse in T. [Of course, τ does have an inverse in $\mathcal{I}_X$; indeed $\tau^{-1} = \begin{pmatrix} 1 & 2 \\ * & 1 \end{pmatrix}$.]

5.2 By Exercise 4.1, $\operatorname{im}\varphi$ is regular and $y^{-1}\varphi$ is an inverse for $y\varphi$ for any $y \in S$. Let $e, f \in \operatorname{im}\varphi$ be idempotents. Again by Exercise 4.1, there are idempotents $g, h \in S$ with $g\varphi = e$ and $h\varphi = f$. Since S is inverse, $gh = hg$. Thus $ef = (g\varphi)(h\varphi) = (gh)\varphi = (hg)\varphi = (h\varphi)(g\varphi) = fe$. Hence idempotents commute in $\operatorname{im}\varphi$ and so $\operatorname{im}\varphi$ is an inverse subsemigroup. Since inverses are unique in inverse semigroups, it follows that $(y\varphi)^{-1} = y^{-1}\varphi$.

5.3 Let S be a Clifford semigroup. By Theorem 5.11, S is regular and its idempotents are central. Thus its idempotents certainly commute. So S is inverse by Theorem 5.1.

5.4 a) Let S be a Clifford semigroup. Then $S \simeq \mathcal{S}[Y; G_\alpha; \varphi_{\alpha,\beta}]$, for some semilattice Y, groups G_α, and homomorphisms $\varphi_{\alpha,\beta} : G_\alpha \to G_\beta$. Let e and f be idempotents in S. Then $e \in G_\alpha$ and $f \in G_\beta$ for some $\alpha, \beta \in Y$. Thus $e = 1_\alpha$ and $f = 1_\beta$, where 1_α and 1_β are the identities of G_α and G_β. So $ef = 1_\alpha 1_\beta = (1_\alpha\varphi_{\alpha,\alpha\wedge\beta})(1_\beta\varphi_{\beta,\alpha\wedge\beta}) = 1_{\alpha\wedge\beta}1_{\alpha\wedge\beta} = 1_{\alpha\wedge\beta}$. So the idempotents of S form a subsemigroup and so S is orthodox.

b) Let S be completely simple and orthodox. So $S \simeq \mathcal{M}[G; I, \Lambda; P]$ for some group G, index sets I and Λ and matrix P over G. Then $I \times \Lambda$ is a rectangular band. Without loss of generality, assume that there is a symbol 1 in $I \cap \Lambda$. Now, $(1, p_{\lambda 1}^{-1}\lambda)$ and $(j, p_{1j}^{-1}, 1)$ are idempotents, and so, since S is orthodox, their product $(1, p_{\lambda 1}^{-1}\lambda)(j, p_{1j}^{-1}, 1) =$

$(1, p_{\lambda 1}^{-1} p_{\lambda j} p_{1j}^{-1}, 1)$ is also an idempotent; hence $p_{\lambda 1}^{-1} p_{\lambda j} p_{1j}^{-1} = p_{11}^{-1}$. Define a map $\varphi : G \times (I \times \Lambda) \to S$ by $(g,(i,\lambda))\varphi = (i, p_{1i}^{-1} g p_{11} p_{\lambda 1}^{-1}, \lambda)$. Then

$$\begin{aligned}
&(g,(i,\lambda))\varphi(h,(j,\mu))\varphi \\
&= (i, p_{1i}^{-1} g p_{11} p_{\lambda 1}^{-1}, \lambda)(j, p_{1j}^{-1} h p_{11} p_{\mu 1}^{-1}, \mu) \\
&= (i, p_{1i}^{-1} g p_{11} p_{\lambda 1}^{-1} p_{\lambda j} p_{1j}^{-1} h p_{11} p_{\mu 1}^{-1}, \mu) \\
&= (i, p_{1i}^{-1} g p_{11} p_{11}^{-1} h p_{11} p_{\mu 1}^{-1}, \mu) \\
&= (i, p_{1i}^{-1} g h p_{11} p_{\mu 1}^{-1}, \mu) \\
&= (gh,(i,\mu))\varphi;
\end{aligned}$$

thus φ is a homomorphism. It is clearly injective and surjective and thus an isomorphism.

5.5 Let S be a completely 0-simple inverse semigroup. By Theorem 4.7, then $S \simeq \mathcal{M}_0[G; I, \Lambda; P]$ for some group G, index sets I and Λ, and matrix P over G^0. Since S is inverse every $\mathcal{L}$-class and every $\mathcal{R}$-class contains exactly one idempotent. Non-zero idempotents of $\mathcal{M}_0[G; I, \Lambda; P]$ are elements of the form $(i, p_{\lambda i}^{-1}, \lambda)$ where $i \in I$ and $\lambda \in \Lambda$ are such that $p_{\lambda i} \neq 0$. The non-zero $\mathcal{R}$-classes of $\mathcal{M}_0[G; I, \Lambda; P]$ are the sets $\{i\} \times G \times \Lambda$; the non-zero $\mathcal{R}$-classes of $\mathcal{M}_0[G; I, \Lambda; P]$ are the sets $I \times G \times \{\lambda\}$. So for each i, there is a unique λ such that $p_{\lambda i}$ is non-zero, and vice versa. Hence there is a bijection $\psi : I \to \Lambda$ so that $i\psi$ is the unique element of Λ with $p_{(i\psi)i} \neq 0$. Hence $|I| = |\Lambda|$ Since Λ an abstract index set, we can reorder it and the rows of P so that P becomes diagonal. Now we can simply replace the index set Λ with I.

Now suppose that $S \simeq \mathcal{M}_0[G; I, I; P]$, where P is diagonal. Then S is completely 0-simple and so regular. The idempotents of $\mathcal{M}_0[G; I, I; P]$ are the elements (i, p_{ii}^{-1}, i). If $i \neq j$, then $p_{ij} = 0$ (since P is diagonal) and so $(i, p_{ii}^{-1}, i)(j, p_{jj}^{-1}, j) = 0$. So idempotent of S commute and so S is inverse.

5.6 a) Let $x \in \operatorname{im} \tau$. Then $x = z\tau$ for some $z \in S^1$. Let $y \in S^1$. Since τ is a partial right translation, $\operatorname{dom} \tau$ is a left ideal and so $yz \in \operatorname{dom} \tau$; furthermore, $(yz)\tau = y(z\tau) = yx$ and so $yx \in \operatorname{im} \tau$. Thus $\operatorname{im} \tau$ is a left ideal of S^1.

b) Let $\tau, \sigma \in \mathcal{I}_{S^1}$ be partial right translations. Let $x, y \in S^1$. Suppose $x\tau\sigma$ is defined. Then both $x \in \operatorname{dom} \tau$ and $x\tau \in \operatorname{dom} \sigma$. Since $\operatorname{dom} \tau$ is a left ideal, $yx \in \operatorname{dom} \tau$ and $(yx)\tau = y(x\tau)$. Since $\operatorname{dom} \sigma$ is a left ideal, $y(x\tau) \in \operatorname{dom} \sigma$ and $(y(x\tau))\sigma = y(x\tau\sigma)$. Hence $yx \in \operatorname{dom}(\tau\sigma)$ and $(yx)\tau\sigma = y(x\tau\sigma)$. So $\tau\sigma$ is a partial right translation.

Suppose $x\tau^{-1}$ is defined. Let $z = x\tau^{-1}$. Then $z \in \operatorname{dom} \tau$ and $z\tau = x$. Since $\operatorname{dom} \tau$ is a left ideal, $yz \in \operatorname{dom} \tau$ and $(yz)\tau = y(z\tau) = yx$.

So $yx \in \operatorname{dom}\tau^{-1}$ and $(yx)\tau^{-1} = yz = y(x\tau^{-1})$. So τ^{-1} is a partial right translation.

Hence the set of partial right translations forms an inverse subsemigroup of $\mathcal{I}_{S^1}$. Since every ρ_x is a partial right transformation, T is a subsemigroup of the set of partial right transformations.

5.7 a) Let $p = c^\beta w^{-1} u b^\zeta$ and $q = c^\zeta u^{-1} w b^\delta$. Then $c^\gamma w b^\beta p =_S c^\gamma u b^\zeta$ and $c^\gamma u b^\zeta q =_S c^\gamma w b^\beta$ and so if $\gamma = \delta$, we have $c^\gamma w b^\beta \mathcal{R}\, c^\delta u b^\zeta$. For the converse, suppose that $c^\gamma w b^\beta \mathcal{R}\, c^{\gamma+\eta} u b^\zeta$ for $\eta > 0$. Since $\mathcal{R}$ is a left congruence, $wb^\beta =_S b^\gamma c^\gamma w b^\beta \mathcal{R}\, b^\gamma c^{\gamma+\eta} u b^\zeta = c^\eta u b^\zeta$. Let $p \in S$ be such that $c^\eta u b^\zeta p = wb^\beta$. So $c^\eta u b^\zeta p c^\beta w^{-1} =_S \varepsilon$ and so c is right invertible. Let $c^\vartheta x b^\iota$ be the right inverse of c. Then $c(c^\vartheta x b^\iota) = c^{\vartheta+1} x b^\iota =_S \varepsilon$, which is a contradiction since each element of S is represented by a word of the form $c^{\gamma'} w' b^{\beta'}$, where γ' and β' are uniquely determined. So $c^\gamma w b^\beta \mathcal{R}\, c^\delta u b^\zeta \Leftrightarrow \gamma = \delta$.

A dual argument proves the result for $\mathcal{L}$. Combining the results for $\mathcal{R}$ and $\mathcal{L}$ gives the result for $\mathcal{D}$.

b) This is immediate from Proposition 5.14.

c) First, $c^\gamma b^\gamma c^\gamma b^\gamma =_S c^\gamma b^\gamma$ and so $c^\gamma b^\gamma$ is an idempotent.

Suppose $c^\gamma w b^\beta$ is idempotent. Assume that $\beta \geq \gamma$; the other case is similar. Then $c^\gamma w b^\beta =_S c^\gamma w b^\beta c^\gamma w b^\beta =_S c^\gamma w b^{\beta-\gamma} w b^\beta =_S c^\gamma w(w\varphi^{\beta-\gamma}) b^{2\beta-\gamma}$. Hence $\beta = 2\beta - \gamma$ and so $\beta = \gamma$. Thus $c^\gamma w b^\beta =_S c^\gamma w(w\varphi^0) b^\gamma = c^\gamma w^2 b^\gamma$. Hence $w = 1_G$ and so $c^\gamma w b^\beta =_S c^\gamma b^\gamma$.

EXERCISES FOR CHAPTER 6

[See page 86 for the exercises.]

6.1 Fix $x \in I$. For $s \in S - I$. Define $s\hat{\varphi}$ to be $(x\varphi)^{-1}((xs)\varphi)$; notice that $xs \in I$ since I is an ideal. Now, for $s' \in S$ and $i \in I$,

$$\begin{aligned}
&(s\hat{\varphi})(i\hat{\varphi}) \\
&= (x\varphi)^{-1}((xs)\varphi)(i\varphi) && \text{[by definition of } \hat{\varphi}] \\
&= (x\varphi)^{-1}((xsi)\varphi) && \text{[since } \varphi \text{ is a homomorphism]} \\
&= (si)\hat{\varphi}; && \text{[by definition of } \hat{\varphi}]
\end{aligned}$$

furthermore, $(s\hat{\varphi})(i\hat{\varphi}) = (si)\hat{\varphi}$ by commutativity of S and G. For $s, s' \in$

S,

$$\begin{aligned}
&(s\hat{\varphi})(s'\hat{\varphi}) \\
&= (x\varphi)^{-1}((xs)\varphi)(x\varphi)^{-1}((xs')\varphi) && \text{[by definition of } \hat{\varphi}] \\
&= (x\varphi)^{-1}(x\varphi)^{-1}((xs)\varphi)((xs')\varphi) && \text{[since } G \text{ is abelian]} \\
&= (x\varphi)^{-1}(x\varphi)^{-1}((xsxs')\varphi) && \text{[since } \varphi \text{ is a homomorphism]} \\
&= (x\varphi)^{-1}(x\varphi)^{-1}((xxss')\varphi) && \text{[since } S \text{ is commutative]} \\
&= (x\varphi)^{-1}(x\varphi)^{-1}(x\varphi)((xss')\varphi) && \text{[since } \varphi \text{ is a homomorphism and } x, xss' \in I] \\
&= (x\varphi)^{-1}((xss')\varphi) && \text{[since } (x\varphi)^{-1}(x\varphi) = 1_G] \\
&= (ss')\hat{\varphi}. && \text{[by definition of } \hat{\varphi}]
\end{aligned}$$

Together with the fact that φ is a homomorphism, this shows that $\hat{\varphi}$ is a homomorphism.

Finally, suppose $\psi : S \to G$ is a homomorphism extending φ. Then $(xs)\psi = (x\psi)(s\psi)$ for any $s \in S - I$. Hence $(xs)\varphi = (x\varphi)(s\psi)$ since $x, xs \in I$, and so $s\psi = (x\varphi)^{-1}((xs)\varphi) = s\hat{\varphi}$. Hence $\psi = \hat{\varphi}$ and so $\hat{\varphi}$ is the unique extension of φ to S.

6.2 a) From the definition, $\sim$ is clearly reflexive and symmetric. Suppose $\alpha \sim \beta$ and $\beta \sim \gamma$. Then there exist δ and ζ with $\delta \subseteq \alpha$, $\delta \subseteq \beta$, $\zeta \subseteq \alpha$, and $\zeta \subseteq \beta$. Let $\eta = \zeta\zeta^{-1}\delta$. Then $\operatorname{dom}\eta \subseteq \operatorname{dom}\zeta$ and for any $x \in \operatorname{dom}\eta$, we have

$$x\eta = x\zeta\zeta^{-1}\delta = x\delta = x\beta = x\zeta$$

and so $\eta \subseteq \delta \subseteq \alpha$ and $\eta \subseteq \zeta \subseteq \gamma$. Hence $\alpha \sim \gamma$. Therefore $\sim$ is transitive.

Suppose $\alpha_1 \sim \beta_1$ and $\alpha_2 \sim \beta_2$. Then there exist δ_1 and δ_2 with $\delta_1 \subseteq \alpha_1$, $\delta_1 \subseteq \beta_1$, $\delta_2 \subseteq \alpha_2$ and $\delta_2 \subseteq \beta_2$. Hence $\delta_1\delta_2 \subseteq \alpha_1\alpha_2$ and $\delta_1\delta_2 \subseteq \beta_1\beta_2$. Hence $\alpha_1\alpha_2 \sim \beta_1\beta_2$. Therefore $\sim$ is a congruence.

b) Let $\alpha, \beta \in T$. Let $\zeta = \alpha^{-1}\beta$ and $\eta = \beta\alpha^{-1}$. Then $\alpha\zeta = \alpha\alpha^{-1}\beta \subseteq \beta$ and so $\alpha\zeta \sim \beta$; similarly $\eta\alpha = \beta\alpha^{-1}\alpha \subseteq \beta$ and so $\eta\alpha \sim \beta$. Thus for any $[\alpha]_\sim, [\beta]_\sim \in G$, there exist $[\zeta]_\sim, [\eta]_\sim \in G$ with $[\alpha]_\sim[\zeta]_\sim = [\eta]_\sim[\alpha]_\sim = [\beta]_\sim$; hence $[\alpha]_\sim G = G[\alpha]_\sim = G$ for any $[\alpha]_\sim \in G$. Thus G is a group.

c) Let $\alpha, \beta \in T$. Then $\operatorname{im}\alpha$ is a left ideal of S by Exercise 5.6(a) and $\operatorname{dom}\beta$ is a left ideal of S since β is a partial right transformation. Since S is right reversible, $\operatorname{im}\alpha \cap \operatorname{dom}\beta \neq \varnothing$. Hence $\alpha\beta \neq \varnothing$.

Since T is generated by the non-empty elements ρ_x and ρ_x^{-1}, we see that T does not contain the empty relation.

d) Suppose $x\psi = y\psi$; then $[\rho_x]_\sim = [\rho_y]_\sim$ and so $\rho_x \sim \rho_y$. Then there exists $\delta \in T$ such that $\delta \subseteq \rho_x$ and $\delta \subseteq \rho_y$. By the previous paragraph, δ is not the empty relation. So let $z \in \operatorname{dom}\delta$. Then $z\rho_x = z\rho_y$. Thus $zx = zy$ and so $x = y$ by cancellativity. Hence $\psi : S \to G$ is a monomorphism and so S is group-embeddable.

6.3 Let $(m,n),(p,q),(r,s) \in S$. Then

$$\begin{aligned}(m,n)\big((p,q)(r,s)\big) &= (m,n)(p+r, 2^r q+s)\\ &= (m+p+r, 2^{p+r}n + 2^r q + s)\\ &= (m+p+r, 2^r(2^p n+q)+s)\\ &= (m+p, 2^p n+q)(r,s)\\ &= \big((m,n)(p,q)\big)(r,s);\end{aligned}$$

thus the multiplication is associative.

Let $(m_1,n_1),(m_2,n_2) \in S$. Let $p_1 = m_2$, $q_1 = 2^{m_1}n_2$, $p_2 = m_1$, and $q_2 = 2^{m_2}n_2$. Then

$$(m_1,n_1)(p_1,q_1) = (m_1+p_1, 2^{p_1}n_1+q_1) = (m_1+m_2, 2^{m_2}n_2 + 2^{m_1}n_2)$$

and

$$(m_2,n_2)(p_2,q_2) = (m_2+p_2, 2^{p_2}n_2+q_2) = (m_2+m_1, 2^{m_1}n_2 + 2^{m_2}n_2);$$

so $(m_1,n_1)(p_1,q_1) = (m_2,n_2)(p_2,q_2)$. Since (m_1,n_1) and (m_2,n_2) were arbitrary, S is left-reversible.

Suppose S is right-reversible. Then $(1,0)$ and $(1,1)$ have a common left multiple. Thus there exist (p_1,q_1) and (p_2,q_2) with $(p_1,q_1)(1,0) = (p_2,q_2)(1,1)$. Hence $(p_1+1, 2q_1) = (p_2+1, 2q_2+1)$, which is a contradiction, since $2q_1$ is even and $2q_2+1$ is odd. Thus S is not right-reversible.

EXERCISES FOR CHAPTER 7

[See page 103 for the exercises.]

7.1 In finite semigroups, $\mathcal{J} = \mathcal{D}$, so $J_x = D_x$. Since D_x is non-trivial, it contains some element $z \neq x$ such that $z \mathcal{R} x$. That is, there exist $p, q \in S^1$ such that $xp = z$ and $zq = x$; notice that $p, q \in S$ since $x \neq z$. Hence $xpq = x$, and so $x(pq)^k = x$ for all $k \in \mathbb{N}$. Since S is finite, there is some $\ell \in \mathbb{N}$ such that $(pq)^\ell$ is idempotent. Let $y = (pq)^\ell$; then $y^2 = y$ and $xy = x$. By the ordering of $\mathcal{J}$-classes, $J_x = J_{xy} \leq J_y$. Since y is idempotent and thus regular, every element of $D_y = J_y$ is regular by Proposition 3.17.

7.2 a) Let S be a finite nilsemigroup. Let $n = |S|$. Let $x_1, \ldots, x_{n+1} \in S$. Consider the $n+1$ products

$$x_1, x_1x_2, \ldots, x_1\cdots x_n, x_1\cdots x_{n+1}.$$

Since $|S| = n$, two of these products must be equal: that is, $x_1\cdots x_k = x_1\cdots x_{k+\ell}$ for some $k \in \{1,\ldots,n\}$ and $\ell \in \{1,\ldots,n+1-k\}$. Hence

$$x_1\cdots x_k = x_1\cdots x_k x_{k+1}\cdots x_{k+\ell} = x_1\cdots x_k(x_{k+1}\cdots x_{k+\ell})^m$$

for all $m \in \mathbb{N}$. Since S is a nilsemigroup, there is some $m \in \mathbb{N}$ with $(x_{k+1}\cdots x_{k+\ell})^m = 0$. Thus $x_1\cdots x_k = x_1\cdots x_k(x_{k+1}\cdots x_{k+\ell})^m = 0$ and so $x_1\cdots x_n = 0$ (since $k \leq n$). Therefore $S^n = \{0\}$ and so S is nilpotent.

b) Let $S = \{0\} \cup \{x_{i,j} : i \in \mathbb{N}, j \leq i\}$. Define a product on S as follows:

$$x_{i,j}x_{k,\ell} = \begin{cases} x_{i,j+\ell} & \text{if } i = k \text{ and } j + \ell \leq i, \\ 0 & \text{otherwise,} \end{cases}$$

$$x_{i,j}0 = 0x_{i,j} = 00 = 0.$$

It is easy to check that this operation is associative. For any $x_{i,j} \in S$, we have $x_{i,j}^{i+1} = 0$ since $j(i+1) > i$. Thus S is a nilsemigroup. However, for any $n \in \mathbb{N}$, we have $x_{n,1}^n = x_{n,n} \neq 0$, so $S^n \neq \{0\}$. Thus S is not nilpotent.

7.3 a) Let $x', y' \in J\varphi$. Then $x' = x\varphi$ and $y' = y\varphi$ for some $x, y \in J$. Thus there exist $p, q, r, s \in S^1$ such that $pxq = y$ and $rys = x$. Then $(p\varphi)x'(q\varphi) = y'$ and $(r\varphi)y'(s\varphi) = x'$ (where we view 1φ as the identity of $(S')^1$) and so $x' \mathcal{J} y'$. So all elements of $J\varphi$ are contained within a single $\mathcal{J}$-class of S'.

b) Let $x' \in J'$. Then $x' = x\varphi$ for some $x \in S$. Let $J = J_x$. Since all elements of $J\varphi$ are $\mathcal{J}$-related by part a), we see that $J\varphi \subseteq J'$.

Let J be minimal such that $J\varphi \subseteq J'$. Let $I = S^1JS^1$. Then $I = S^1xS^1$ for any $x \in J$, by the definition of $\mathcal{J}$. Let $y' \in J'$. Then $y' \mathcal{J} x\varphi$ and so there exist $p', q' \in (S')^1$ with $y' = p'(x\varphi)q'$. So $y' \in (S')^1(x\varphi)(S')^1 = (S^1xS^1)\varphi = I\varphi$ since φ is surjective. So $J' \subseteq I\varphi$.

Let $y \in I$ and let $K = J_y$. By part a), there exists some $\mathcal{J}$-class K' of S' such that $K\varphi \subseteq K'$. Suppose that $y \notin J$. Then $K = J_y < J$. Therefore $K\varphi \nsubseteq J'$ since J was chosen to be minimal such that $J\varphi \subseteq J'$. Hence $K' \neq J'$. Suppose $y\varphi \in J'$. Then there exists $p', q', r', s' \in (S')^1$ with $p'(y\varphi)q' = x\varphi$ and $r'(x\varphi)s' = y\varphi$ for some $x \in J$. Since φ is surjective, this shows that $y \mathcal{J} x$ and so $y \in J$, which is a contradiction. Therefore $y\varphi \notin J'$.

Thus for any $y \in I$, we have $y \notin J$ implies $y\varphi \notin J'$. Hence $y\varphi \in J'$ implies $y \in J$, which implies $y\varphi \in J\varphi$. Since φ is surjective, this shows that $J' \subseteq J\varphi$. Thus $J\varphi = J'$.

7.4 It suffices to prove this when T is a subsemigroup of S and when T is a homomorphic image of S. In both cases, T is finite because S is, and thus for both S and T the property of having $\mathcal{H}$ being the equality relation is equivalent to aperiodic. Let T be a subsemigroup of S. Let $x \in T$. Since $x \in S$ and S is aperiodic, there exists $k \in \mathbb{N}$ such that $x^k = x^{k+1}$. Since this is true for all $x \in T$, the subsemigroup T is aperiodic. Now let $\varphi : S \to T$ be an epimorphism. Let $y \in T$. Then there exists $x \in S$ such that $x\varphi = y$. Since S is aperiodic, $x^k = x^{k+1}$ for some $k \in \mathbb{N}$. Hence $y^k = (x\varphi)^k = x^k\varphi = x^{k+1}\varphi = (x\varphi)^{k+1} = y^{k+1}$. Since this is true for all $y \in T$, the semigroup T is aperiodic. This completes the proof.

In the free semigroup $\{a\}^+$, the relation $\mathcal{H}$ is the equality relation, but any finite non-trivial cyclic group is a homomorphic image of $\{a\}^+$.

7.5 Let $(s_1, t_1), (s_2, t_2), (s_3, t_3) \in S \rtimes_\varphi T$. Then

$$\begin{aligned}
&\big((s_1,t_1)(s_2,t_2)\big)(s_3,t_3)\\
&= (s_1\,{}^{t_1}s_2, t_1t_2)(s_3,t_3) && \text{[by (7.1)]}\\
&= (s_1\,{}^{t_1}s_2\,{}^{t_1t_2}s_3, t_1t_2t_3) && \text{[by (7.1)]}\\
&= (s_1\,{}^{t_1}s_2\,{}^{t_1}({}^{t_2}s_3), t_1t_2t_3) && \text{[by the definition of a left action]}\\
&= (s_1\,{}^{t_1}(s_2\,{}^{t_2}s_3), t_1t_2t_3) && \text{[since the action is by endomorphisms]}\\
&= (s_1,t_1)(s_2\,{}^{t_2}s_3, t_2t_3) && \text{[by (7.1)]}\\
&= (s_1,t_1)\big((s_2,t_2)(s_3,t_3)\big); && \text{[by (7.1)]}
\end{aligned}$$

thus the multiplication (7.1) is associative.

7.6 a) Suppose M and N are monoids. Let $e : N \to M$ be the constant map with $(x)e = 1_M$ for all $x \in N$. Then for any $(f, n) \in M \wr N$, we have

$$\begin{aligned}
&(e,1_N)(f,n)\\
&= (e\,{}^{1_N}f, 1_Nn)\\
&= (f,n) && \text{[since } (x)e\,{}^{1_N}f = (x)e(x1_N)f = 1_M(x)f = (x)f\text{]}
\end{aligned}$$

and

$$\begin{aligned}
&(f,n)(e,1_N)\\
&= (f^ne, n1_N)\\
&= (f,n); && \text{[since } (x)f^ne = (x)f(xn)\,{}^ne = (x)f1_M = (x)f\text{]}
\end{aligned}$$

hence $(e, 1_N)$ is an identity for the monoid $M \wr N$.

b) Suppose M and N are groups. Let $(f, n) \in M \wr N$. Define $f' \in N \to M$ by $(x)f' = ((xn^{-1})f)^{-1}$. Then

$$\begin{aligned}
&(f,n)(f',n^{-1})\\
&= (f\,{}^nf', nn^{-1})\\
&= (e,1_N) && \text{[since } (x)f\,{}^nf' = (x)f(xn)f' =\\
& && (x)f((xnn^{-1})f)^{-1} = (x)f((x)f)^{-1} = 1_M\text{]}
\end{aligned}$$

and

$$\begin{aligned}
&(f',n^{-1})(f,n)\\
&= (f'\,{}^{n^{-1}}f, n^{-1}n)\\
&= (e,1_N); && \text{[since } (x)f'\,{}^{n^{-1}}f = (x)f'(xn^{-1})f = (x)f'((x)f')^{-1} = 1_M\text{]}
\end{aligned}$$

thus (f', n^{-1}) is a right and left inverse for (f, n). Hence $M \wr N$ is a group.

7.7 The wreath product $S \wr T$ must be right-cancellative but is not necessarily left-cancellative. For $(f, s), (g, t), (h, u) \in S \wr T$,

$$
\begin{aligned}
& (f, s)(h, u) = (g, t)(h, u) \\
\Rightarrow\ & (f\,{}^{s}h, su) = (g\,{}^{t}h, tu) \\
\Rightarrow\ & f\,{}^{s}h = g\,{}^{t}h \wedge su = tu \\
\Rightarrow\ & (\forall x \in T)\big((x)f(xs)h = (x)g(xt)h\big) \wedge su = tu \\
\Rightarrow\ & (\forall x \in T)\big((x)f(xs)h = (x)g(xt)h\big) \wedge s = t \\
& \qquad\qquad\qquad\qquad\qquad\qquad [\text{since } T \text{ is cancellative}] \\
\Rightarrow\ & (\forall x \in T)\big((x)f(xs)h = (x)g(xs)h\big) \wedge s = t \quad [\text{substituting } s = t] \\
\Rightarrow\ & (\forall x \in T)\big((x)f = (x)g\big) \wedge s = t \qquad [\text{since } S \text{ is cancellative}] \\
\Rightarrow\ & f = g \wedge s = t.
\end{aligned}
$$

Now let $S = T = \mathbb{N} \cup \{0\}$ (under $+$) and define a map $f : S \to T$ by $(0)f = 1$ and $(x)f = 0$ for all $x \in T - \{0\}$ and a map $g : S \to T$ by $(x)g = 0$ for all $x \in T$. Then

$$(g, 1)(f, 1) = (g\,{}^{1}f, 2) = (g\,{}^{1}g, 2) = (g, 1)(g, 1)$$

since $(x)g\,{}^{1}f = (x)g + (x+1)f = 0 + 0 = (x)g + (x+1)g = (x)g\,{}^{1}g$ for all $x \in T$. Hence $S \wr T$ is not left-cancellative.

7.8 This is a tedious analysis of products of three elements in $C(S)$. Each element is either in S or S'; there are thus eight cases. Let $x, y, z \in S$. Then:

- $(xy)z = x(yz)$, since S is a subsemigroup of $S \cup S'$;
- $(xy)z' = z' = xz' = x(yz')$;
- $(xy')z = y'z = (yz)' = x(yz)' = x(y'z)$;
- $(xy')z' = z' = xz' = x(y'z')$;
- $(x'y)z = (xy)'z = ((xy)z)' = (x(yz))' = x'(yz)$, using associativity in S for the third step;
- $(x'y)z' = z' = x'z' = x'(yz')$;
- $(x'y')z = y'z = (yz)' = x'(yz)' = x'(y'z)$;
- $(x'y')z' = z' = x'z' = x'(y'z')$.

Therefore the product defined by (7.3) is associative.

7.9 Define a map $\psi : C(M) \to \mathcal{T}_M$ by $x\psi = \rho_x$ and $x'\psi = \tau_x$ for $x \in M$. Clearly $\operatorname{im}\varphi = \{\rho_x, \tau_x : x \in M\}$. We cannot have $x\psi = y'\psi$, for $x\psi$ is a non-constant map and $y'\psi$ is a constant map. So to check injectivity, we simply check that $\psi|_M$ and $\psi_{M'}$ are injective:

$$
\begin{aligned}
x\psi = y\psi \Rightarrow \rho_x = \rho_y \Rightarrow 1\rho_x = 1\rho_y \Rightarrow x = y, \\
x'\psi = y'\psi \Rightarrow \tau_x = \tau_y \Rightarrow 1\tau_x = 1\tau_y \Rightarrow x = y.
\end{aligned}
$$

Finally, to check that ψ is a homomorphism, we must check the various cases of multiplication in the definition of $C(M)$:

$$\begin{aligned}(x\varphi)(y'\varphi) &= \rho_x\tau_y = \tau_y = y'\varphi = (xy')\varphi\\ (x'\varphi)(y'\varphi) &= \tau_x\tau_y = \tau_y = y'\varphi = (x'y')\varphi\\ (x'\varphi)(y\varphi) &= \tau_x\rho_y = \tau_{xy} = (xy)'\varphi.\end{aligned}$$

So ψ is an isomorphism.

7.10 Ley $x \in M$ and $y \in C(M)$. Then

$$\begin{aligned}&(x)[(y)(f^m g)_{\mathrm{con}}]\\ &= ((x)f^m g)' && [\text{by definition of } {}_{\mathrm{con}}]\\ &= ((x)f)'(xm)g && [\text{by definition of the product and action}]\\ &= (x)[(y)f_{\mathrm{con}}](x)[(m')g_{\mathrm{ext}}] && [\text{by definition of } {}_{\mathrm{ext}} \text{ and } {}_{\mathrm{con}}]\\ &= (x)[(y)f_{\mathrm{con}}](x)[(ym')g_{\mathrm{ext}}]\\ &&& [\text{by definition of the product in } C(M)]\\ &= (x)[(y)f_{\mathrm{con}}(y)\,{}^{m'}g_{\mathrm{ext}}] && [\text{by multiplication in } C(S)^M]\\ &= (x)[(y)f_{\mathrm{con}}\,{}^{m'}g_{\mathrm{ext}}]; && [\text{by multiplication in } (C(S)^M)^{C(M)}]\end{aligned}$$

this proves (7.5). Next,

$$\begin{aligned}&(x)[(y)g_{\mathrm{con}}]\\ &= ((x)g)' && [\text{by definition of } {}_{\mathrm{con}}]\\ &= (xy)f((x)g)' && [\text{by definition of the product in } C(S)]\\ &= (x)[(y)f_{\mathrm{ext}}](x)[(ym)g_{\mathrm{con}}] && [\text{by definition of } {}_{\mathrm{ext}} \text{ and } {}_{\mathrm{con}}]\\ &= (x)[(y)f_{\mathrm{ext}}(y)\,{}^{m}g_{\mathrm{con}}] && [\text{by multiplication in } C(S)^M]\\ &= (x)[(y)f_{\mathrm{ext}}\,{}^{m}g_{\mathrm{con}}]; && [\text{by multiplication in } (C(S)^M)^{C(M)}]\end{aligned}$$

this proves (7.6). Finally,

$$\begin{aligned}&(x)[(y)g_{\mathrm{con}}]\\ &= ((x)g)' && [\text{by definition of } {}_{\mathrm{con}}]\\ &= ((x)f)'((x)g)' && [\text{by definition of the product in } C(S)]\\ &= (x)[(y)f_{\mathrm{con}}](x)[(ym)g_{\mathrm{con}}] && [\text{by definition of } {}_{\mathrm{con}}]\\ &= (x)[(y)f_{\mathrm{con}}(y)\,{}^{m}g_{\mathrm{con}}] && [\text{by multiplication in } C(S)^M]\\ &= (x)[(y)f_{\mathrm{con}}\,{}^{m}g_{\mathrm{con}}]; && [\text{by multiplication in } (C(S)^M)^{C(M)}]\end{aligned}$$

this proves (7.7).

EXERCISES FOR CHAPTER 8

[See pages 127–128 for the exercises.]

8.1 a) Let $\mathcal{N}$ be the class of finite nilpotent semigroups. Let $S \in \mathcal{N}$. So $S^n = \{0\}$ for some $n \in \mathbb{N}$. First, let T be a subsemigroup of S. Then $T^n \subseteq S^n = \{0\}$; hence $T \in \mathcal{N}$. So $\mathcal{N}$ is closed under Sub. Second, let $\varphi : S \to U$ be an epimorphism. Then $U^n = (S\varphi)^n = S^n\varphi \subseteq \{0_S\}\varphi = \{0_U\}$. So $U \in \mathcal{N}$. Thus $\mathcal{N}$ is closed under Hom. Third, let $S_1, \ldots, S_k$ be nilpotent; then $S_i^{n_i} = \{0_{S_i}\}$ for some $n_i \in \mathbb{N}$ for each $i = 1, \ldots, k$. Let n be the maximum of the various n_i. Then

$$(S_1 \times \ldots \times S_k)^n \subseteq S_1^n \times \ldots S_k^n = \{0_{S_1}\} \times \ldots \{0_{S_k}\} = \{(0_{S_1}, \ldots, 0_{S_k})\};$$

hence $S_1 \times \ldots \times S_k \in \mathcal{N}$. Thus $\mathcal{N}$ is closed under $\mathrm{Prod}_{\mathrm{fin}}$. Therefore $\mathcal{N}$ is a pseudovariety.

b) Let $A = \{a\}$. For each $k \in \mathbb{N}$, let $I_k = \{w \in A^+ : |w| \geq k\}$. Then I_k is an ideal of A^+. Let $S_k = A^+/I_k$; then $S_k^k = \{0_{S_k}\}$. So each S_k is nilpotent. Let $S = \prod_{i=1}^{\infty} S_k$. Let $s \in S$ be such that $(k)s = a \in S_k$ for all $k \in \mathbb{N}$. Then for any $n \in \mathbb{N}$, we have $(n+1)s^n = a^n \in S_{n+1}$; hence $(n+1)s^n \neq 0_{S_{n+1}}$, and so $s^n \neq 0_S$ for any $n \in \mathbb{N}$. Thus $S^n \neq \{0_S\}$ for any $n \in \mathbb{N}$. Hence S is not nilpotent. Therefore the class of nilpotent semigroups is not closed under Prod and so is not a variety.

8.2 Note first that we are working with algebras of type $\{(\circ, 2), ({}^{-1}, 1)\}$. Let S be an orthodox completely regular semigroup. Let $\varphi : S \to T$ be an epimorphism. Then T is regular by Example 4.1, and furthermore $(x\varphi)^{-1} = (x^{-1}\varphi)$ since homomorphisms for algebras of this type must also preserve ${}^{-1}$. Therefore since S is completely regular and thus satisfies the laws (4.3), T also satisfies these laws, so T is completely regular. Finally, if $e, f \in T$ are idempotents, then $e = xx^{-1}$ and $f = yy^{-1}$ for some $x, y \in T$ by Proposition 4.13. Let $p, q \in S$ be such that $p\varphi = x$ and $q\varphi = y$. Then pp^{-1} and qq^{-1} are idempotent. So $pp^{-1}qq^{-1}$ is idempotent (since S is orthodox) and so $(pp^{-1}qq^{-1})\varphi = xx^{-1}yy^{-1} = ef$ is idempotent. So the idempotents of T form a subsemigroup and so T is orthodox.

Now let T be a subalgebra of S. Then T also satisfies the laws (4.3) and is thus completely regular. Finally, the set of idempotents of T is the intersection of the set of idempotents of S, which is a subsemigroup, and T, which is also a subsemigroup. Hence the set of idempotents of T is a subsemigroup.

Finally, let $\{S_i : i \in I\}$ be a collection of orthdox completely regular semigroups. Then each S_i satisfies the laws (4.3) and so their product $\prod_{i \in I} S_i$ does also. The set of idempotents in $\prod_{i \in I} S_i$ is the product of the sets of idempotents in each S_i and hence forms a subsemigroup.

Now let S be an orthodox completely regular semigroup. Then S satisfies the laws (4.3). Let $x, y \in S$. Note that $x^{-1}x$ and yy^{-1} are idempotents, and so their product $x^{-1}xyy^{-1}$ is idempotent since S is orthodox.

Thus

$$\begin{aligned} & xyy^{-1}x^{-1}xy \\ = {} & xx^{-1}xyy^{-1}x^{-1}xyy^{-1}y \\ = {} & xx^{-1}xyy^{-1}y && \text{[since } x^{-1}xyy^{-1} \text{ is idempotent]} \\ = {} & xy. \end{aligned}$$

Therefore S satisfies the law $xyy^{-1}x^{-1}xy = xy$.

Now suppose S satisfies the laws (4.3) and $xyy^{-1}x^{-1}xy = xy$. Then S is completely regular. Let $e, f \in S$ be idempotents; then $e = x^{-1}x$ and $f = yy^{-1}$ for some $x, y \in S$ by Proposition 4.13. Then

$$\begin{aligned} & (ef)^2 \\ = {} & (x^{-1}xyy^{-1})^2 \\ = {} & x^{-1}xyy^{-1}x^{-1}xyy^{-1} \\ = {} & x^{-1}xyy^{-1}; && \text{[since } xyy^{-1}x^{-1}xy = xy\text{]} \\ = {} & ef. \end{aligned}$$

Hence the idempotents of S form a subsemigroup and so S is orthodox.

8.3 a) Let $S = L \times R$ be a rectangular band, where L is a left zero semigroup and R is a right zero semigroup.

Let $\varphi : S \to T$ be an epimorphism. Fix $(\ell, r) \in S$. Let $L_T = (L \times \{r\})\varphi$ and $R_T = (\{\ell\} \times R)\varphi$. Notice that L_T is a left zero semigroup and R_T is a right zero semigroup; hence $L_T \times R_T$ is a rectangular band. Define $\psi : L_T \times R_T \to T$ by $(\ell_t, r_t)\psi = \ell_t r_t$. Let $(\ell_t^{(1)}, r_t^{(1)}), (\ell_t^{(2)}, r_t^{(2)}) \in L_T \times R_T$. Let $\ell^{(1)}, \ell^{(2)} \in L$ and $r^{(1)}, r^{(2)} \in R$ be such that $(\ell^{(i)}, r)\varphi = \ell_t^{(i)}$ and $(\ell, r^{(i)})\varphi = r_t^{(i)}$ for $i = 1, 2$. Then

$$\begin{aligned} & (\ell_t^{(1)}, r_t^{(1)})\psi(\ell_t^{(2)}, r_t^{(2)})\psi \\ = {} & \ell_t^{(1)} r_t^{(1)} \ell_t^{(2)} r_t^{(2)} \\ = {} & (\ell^{(1)}, r)\varphi(\ell, r^{(1)})\varphi(\ell^{(2)}, r)\varphi(\ell, r^{(2)})\varphi \\ = {} & \big((\ell^{(1)}, r)(\ell, r^{(1)})(\ell^{(2)}, r)(\ell, r^{(2)})\big)\varphi \\ = {} & (\ell^{(1)}, r^{(2)})\varphi \\ = {} & \big((\ell^{(1)}, r)(\ell, r^{(2)})\big)\varphi \\ = {} & (\ell^{(1)}, r)\varphi(\ell, r^{(2)})\varphi \\ = {} & \ell_t^{(1)} r_t^{(2)} \\ = {} & (\ell_t^{(1)}, r_t^{(2)})\psi \\ = {} & \big((\ell_t^{(1)}, r_t^{(1)})(\ell_t^{(2)}, r_t^{(2)})\big)\psi; \end{aligned}$$

thus ψ is a homomorphism. Furthermore,

$$\begin{aligned} & (\ell_t^{(1)}, r_t^{(1)})\psi = (\ell_t^{(2)}, r_t^{(2)})\psi \\ \Rightarrow {} & \ell_t^{(1)} r_t^{(1)} = \ell_t^{(2)} r_t^{(2)} \end{aligned}$$

$$
\begin{aligned}
&\Rightarrow (\ell^{(1)}, r)\varphi(\ell, r^{(1)})\varphi = (\ell^{(2)}, r)\varphi(\ell, r^{(2)})\varphi \\
&\Rightarrow \big((\ell^{(1)}, r)(\ell, r^{(1)})\big)\varphi = \big((\ell^{(2)}, r)(\ell, r^{(2)})\big)\varphi \\
&\Rightarrow (\ell^{(1)}, r^{(1)})\varphi = (\ell^{(2)}, r^{(2)})\varphi \\
&\Rightarrow (\ell^{(1)}, r^{(1)})\varphi(\ell, r)\varphi = (\ell^{(2)}, r^{(2)})\varphi(\ell, r)\varphi \\
&\qquad\qquad \wedge (\ell, r)\varphi(\ell^{(1)}, r^{(1)})\varphi = (\ell, r)\varphi(\ell^{(2)}, r^{(2)})\varphi \\
&\Rightarrow \big((\ell^{(1)}, r^{(1)})(\ell, r)\big)\varphi = \big((\ell^{(2)}, r^{(2)})(\ell, r)\big)\varphi \\
&\qquad\qquad \wedge \big((\ell, r)(\ell^{(1)}, r^{(1)})\big)\varphi = \big((\ell, r)(\ell^{(2)}, r^{(2)})\big)\varphi \\
&\Rightarrow (\ell^{(1)}, r)\varphi = (\ell^{(2)}, r)\varphi \wedge (\ell, r^{(1)})\varphi = (\ell, r^{(2)})\varphi \\
&\Rightarrow \ell_t^{(1)} = \ell_t^{(2)} \wedge r_t^{(1)} = r_t^{(2)} \\
&\Rightarrow (\ell_t^{(1)}, r_t^{(1)}) = (\ell_t^{(2)}, r_t^{(2)}),
\end{aligned}
$$

so ψ is injective. Finally, ψ is surjective since

$$
\begin{aligned}
\operatorname{im}\psi &= L_T R_T \\
&= (L \times \{r\})\varphi(\{\ell\} \times R)\varphi \\
&= \big((L \times \{r\})(\{\ell\} \times R)\big)\varphi \\
&= (L \times R)\varphi = T.
\end{aligned}
$$

Hence T is isomorphic to the rectangular band $L_T \times R_T$; thus $T \in \mathcal{RB}$. So $\mathcal{RB}$ is closed under forming homomorphic images.

Now let T be a subsemigroup of S. Let $L_T = \{\ell \in L : (\exists r \in R)((\ell, r) \in T)\}$ and $R_T = \{r \in R : (\exists \ell \in L)((\ell, r) \in T)\}$. Notice that L_T is also a left zero semigroup and R_T is also a right zero semigroup. Clearly $T \subseteq L_T \times R_T$; we now establish the opposite inclusion. Let $(\ell_t, r_t) \in L_T \times R_T$. Then there exist $r \in R$ and $\ell \in L$ such that $(\ell_t, r) \in T$ and $(\ell, r_t) \in T$. Thus $(\ell_t, r_t) \in (\ell_t, r)(\ell, r_t) \in T$. So $T = L_T \times R_T$ is a rectangular band. So $\mathcal{RB}$ is closed under taking subsemigroups.

Finally, let $\{S_i : i \in I\}$ be a collection of rectangular bands. Then $S_i \simeq L_i \times R_i$ for some left zero semigroup L_i and right zero semigroup R_i, for each $i \in I$. Then

$$
\prod_{i\in I} S_i = \prod_{i\in I} (L_i \times R_i) \simeq \Big(\prod_{i\in I} L_i\Big) \times \Big(\prod_{i\in I} R_i\Big).
$$

Since $\prod_{i\in I} L_i$ is a left zero semigroup and $\prod_{i\in I} R_i$ is a right zero semigroup, $\prod_{i\in I} S_i \in \mathcal{RB}$. Hence $\mathcal{RB}$ is closed under forming direct products.

Thus $\mathcal{RB}$ is a variety.

b) Let $S = L \times R$ be a rectangular band. Let $x = (l_1, r_1)$ and $y = (l_2, r_2)$. Then $xyx = (l_1, r_1)(l_2, r_2)(l_1, r_1) = (l_1, r_1) = x$. So S satisfies this law.

Suppose S satisfies the law $xyx = x$. Fix some $t \in S$. Let $L = St$ and $R = tS$. Then for any $pt, p't \in L$, we have $ptp't = pt$ by the law

(with $x = t$ and $y = p'$). So L is a left zero semigroup and similarly R is a right zero semigroup. Furthermore, for any $p, q.r \in S$,

$$\begin{aligned} pr &= pqpr && \text{[by the law with } x = p \text{ and } y = q\text{]} \\ &= pqrqpr && \text{[by the law with } x = q \text{ and } y = r\text{]} \\ &= pqr. && \text{[by the law with } x = r \text{ and } y = qp\text{]} \end{aligned} \tag{S.10}$$

Define $\psi : S \to L \times R$ by $p\psi = (pt, tp)$. Then

$$\begin{aligned} (p\psi)(q\psi) &= (pt, tp)(qt, tq) \\ &= (pt, tq) \\ &= (pqt, tpq) && \text{[using (S.10) in both components]} \\ &= (pq)\psi, \end{aligned}$$

so ψ is a homomorphism. Notice that this also shows that for any $pt \in L$, $tq \in R$, we have $(pq)\psi = (pt, tq)$; thus ψ is surjective. Finally, for any $p, q \in S$,

$$\begin{aligned} & p\psi = q\psi \\ \Rightarrow\ & (pt, tp) = (qt, tq) \\ \Rightarrow\ & pt = qt \wedge tp = tq \\ \Rightarrow\ & ptp = qtp \wedge qtp = qtq \\ \Rightarrow\ & ptp = qtq \\ \Rightarrow\ & p = q, \text{[applying the law on both sides]} \end{aligned}$$

so ψ is injective. So S is [isomorphic to] a rectangular band and so $S \in \mathcal{RB}$.

c) Any rectangular band satisfies the law $xyz = xz$ by (S.10). Every element of a rectangular band is idempotent, so $x^2 = x$ is also satisfied.

Let S satisfy the laws $x^2 = x$ and $xyz = xz$. To prove that S is a rectangular band, follow the reasoning in part b) with the following minor differences: First, L is a left zero semigroup since $ptp't = ptt = pz$ by applying first $xyz = xz$ and then $x^2 = x$; similarlt R is a right zero semigroup. Second, to prove ψ is a homomorphism, apply $xyz = xz$ to both components. Finally, the last step in proving ψ is injective becomes $ptp = qtq \Rightarrow p^2 = q^2 \Rightarrow p = q$, by applying first $xyz = xz$ and then $x^2 = x$.

d) Let S be a non-trivial null semigroup. Then for any $x, y, z \in S$, we have $xyz = 0_S$ and $xz = 0_S$. However, S is not a rectangular band because $x^2 \neq x$ for any $x \neq 0_S$.

8.4 Let $S = G \times L \times R$, where G is a group, L is a left zero semigroup, and R is a right zero semigroup. Let $\varphi : S \to T$ be a homomorphism. Fix $(1_G, \ell, r) \in S$. Let $H = (G \times \{\ell\} \times \{r\})\varphi$, $L_T = (\{1_G\} \times L \times \{r\})\varphi$ and

$R_T = (\{1_G\} \times \{\ell\} \times R)\varphi$. Reasoning parallel to Example 8.3 shows that $T \simeq H \times L_T \times R_T$.

Notice that $(g,\ell,r)^{-1} = (g^{-1},\ell,r)$. Let T be a subalgebra of S. Let $H = \{g \in G : (\exists(\ell,r) \in L \times R)((g,\ell,r) \in T\}$. We first prove that if $(g,\ell,r) \in T$, then $H \times \{(\ell,r)\} \subseteq T$. Let $h \in H$; then $(h,\ell',r') \in T$ for some $\ell' \in L$, $r' \in R$. Hence T contains

$$(g,\ell,r)(g,\ell,r)^{-1}(h,\ell',r')(g,\ell,r)(g,\ell,r)^{-1} = (gg^{-1}hgg^{-1},\ell,r) = (h,\ell,r),$$

and thus $H \times \{(\ell,r)\} \subseteq T$. Now reason as in Example 8.3 to see that $T = H \times L_T \times R_T$ and thus $T \in \mathcal{X}$.

Let $\{S_i : i \in I\}$ be a collection of semigroups in $\mathcal{X}$. Then for all $i \in I$, we have $S_i \simeq G_i \times L_i \times R_i$ for some group G_i, left zero semigroup L_i and right zero semigroup R_i. Hence

$$\prod_{i\in I} S_i \simeq \prod_{i\in I}(G_i \times L_i \times R_i) \simeq \Big(\prod_{i\in I} G_i\Big) \times \Big(\prod_{i\in I} L_i\Big) \times \Big(\prod_{i\in I} R_i\Big);$$

since $\prod_{i\in I} G_i$ is a group, $\prod_{i\in I} L_i$ is a left zero semigroup, and $\prod_{i\in I} R_i$ is a right zero semigroup, we see that $\prod_{i\in I} S_i$ is [isomorphic to] the direct product of a group and a rectangular band. So $\prod_{i\in I} S_i \in \mathcal{X}$.

Let $S = G \times L \times R$, where G is a group, L is a left zero semigroup, and R is a right zero semigroup. Let $x = (g,\ell,r)$ and $y = (g',\ell',r')$. Then $xx^{-1} = (g,\ell,r)(g^{-1},\ell,r) = (1_G,\ell,r) = (g^{-1},\ell,r)(g,\ell,r) = x^{-1}x$ and $x^{-1}yy^{-1}x = (g^{-1},\ell,r)(h,\ell',r')(h^{-1},\ell',r')(g,\ell,r) = (g^{-1}hh^{-1}g,\ell,r) = (1_G,\ell,r) = (g^{-1},\ell,r)(g,\ell,r) = x^{-1}x$. So S satisfies these laws.

Now suppose that S satisfies the given laws. For any $x,y \in S$, we have $x = xx^{-1}x = xx^{-1}yy^{-1}x \in SyS$. So S is simple by the analogy of Lemma 3.5 for simple semigroups. Let $e,f \in S$ be idempotents; then $e = xx^{-1}$ and $f = yy^{-1}$ for some $x,y \in S$. Then $efe = xx^{-1}yy^{-1}xx^{-1} = xx^{-1}xx^{-1} = xx^{-1} = e$. So the idempotents of S form a rectangular band by Example 8.3. Since rectangular bands are completely simple, they contain primitive idempotents. Hence S contains a primitive idempotent. So S is completely simple. Since the idempotents of S form a subsemigroup, S is orthodox. Hence S is a direct product of a rectangular band and a group by Exercise 5.4(b).

8.5 Let $S \in \bigcap_{i\in I} \mathsf{V}_i$. Then $S \in \mathsf{V}_i$ for all $i \in I$. Let T be a homomorphic image (respectively, subalgebra) of S. Since each V_i is a pseudovariety, $T \in \mathsf{V}_i$ for all $i \in I$. Hence $T \in \bigcap_{i\in I} \mathsf{V}_i$. So $\bigcap_{i\in I} \mathsf{V}_i$ is closed under forming homomorphic images and subalgebras. Now let $S_1,\ldots,S_n \in \bigcap_{i\in I} \mathsf{V}_i$. Then $S_j \in \mathsf{V}_i$ for each $i \in I$ and $j = 1,\ldots,n$. So $S_1 \times \ldots \times S_n \in \mathsf{V}_i$ for each $i \in I$ and so $S_1 \times \ldots \times S_n \in \bigcap_{i\in I} \mathsf{V}_i$. So $\bigcap_{i\in I} \mathsf{V}_i$ is closed under forming finitary direct products. Therefore $\bigcap_{i\in I} \mathsf{V}_i$ is a pseudovariety.

8.6 Let S be a completely regular semigroup. Let $s \in S$. By Proposition 4.13, s lies in a subgroup G of S. If $\theta : \overline{\Omega}_{\{x\}}\mathsf{S} \to S$ is such that $x\theta = s$, then $x^\omega\theta$ is the idempotent power of S, which much be the identity

of G. So $x^{\omega+1}\theta = (x^\omega\theta)(x\theta) = 1s = s = x\theta$, so S satisfies the pseudoidentity $x^{\omega+1} = x$.

Now suppose that S satisfies $x^{\omega+1} = x$. Let $s \in S$ and choose $\theta : \overline{\Omega}_{\{x\}}\mathsf{S} \to S$ with $x\theta = s$. Then $x^\omega\theta = s^k$ for some $k \in \mathbb{N}$. So $s^k = x^\omega\theta = x\theta = s$. Thus s lies in the cyclic group $\{s, s^2, \ldots, s^{k-1}\}$. Hence every element of S lies in a subgroup and so S is completely regular by Proposition 4.13.

8.7 Let S be a completely simple semigroup; thus $S = \mathcal{M}[G; I, \Lambda; P]$ for some group G, index sets I and Λ, and matrix P over G. Let (i, g, λ) and (j, h, μ) be elements of S. If $\theta : \overline{\Omega}_{\{x\}}\mathsf{S} \to S$ is such that $x\theta = (i, g, \lambda)$ and $y\theta = (j, h, \mu)$, then $(xy)\theta = (i, g, \lambda)(j, h, \mu) = (i, gp_{\lambda j}h, \mu)$. Now, $(i, gp_{\lambda j}h, \mu)^k = (i, (gp_{\lambda j}hp_{\mu i})^{k-1}gp_{\lambda j}h, \mu)$ for all $k \in \mathbb{N}$. Thus $(xy)^\omega\theta$ is $(i, (gp_{\lambda j}hp_{\mu i})^{k-1}gp_{\lambda j}h, \mu)$ for some k. Since $(xy)^\omega\theta$ is always an idempotent, we have $(xy)^\omega\theta = (i, p_{\mu i}^{-1}, \mu)$. Therefore we have $((xy)^\omega x)\theta = (i, p_{\mu i}^{-1}, \mu)(i, g, h) = (i, p_{\mu i}^{-1}, \mu)(i, g, \lambda) = (i, p_{\mu i}^{-1}p_{\mu i}g, \lambda) = (i, g, \lambda) = x\theta$. Thus S satisfies the pseudoidentity $(xy)^\omega x = x$.

Now suppose that S satisfies $(xy)^{\omega+1} = x$. Let $s, t \in S$ and choose $\theta : \overline{\Omega}_{\{x\}}\mathsf{S} \to S$ with $x\theta = s$ and $y\theta = t$. Then $(xy)^\omega x\theta = (st)^k s$ for some $k \in \mathbb{N}$. Hence $s = (st)^k s \in StS$ and so S is simple by the analogy of Lemma 3.5 for simple semigroups. Arguing as in Exercise 8.6 but with $x\theta = y\theta = s$, we see that s lies in the $\{s, s^2, \ldots, s^{2k}\}$. Hence every element of S lies in a subgroup and so S is completely regular by Proposition 4.13. Since S is completely regular and simple, it is completely simple by Theorem 4.14.

EXERCISES FOR CHAPTER 9

[See page 138 for the exercises.]

9.1 a) It is immediate from the definition that σ_L that is it reflexive, symmetric, and transitive. So σ_L is an equivalence relation. Let $u\ \sigma_L\ v$ and let $s \in A^*$. Then $puq \in L \Leftrightarrow pvq \in L$ for all $p, q \in A^*$. In particular, this holds for all p of the form $p's$; hence $p'suq \in L \Leftrightarrow p'svq \in L$ for all $p', q \in A^*$. Hence $su\ \sigma_L\ sv$. So σ_L is left-compatible; similarly it is right-compatible and is thus a congruence.

b) Let $u \in L$ and let $v\ \sigma_L\ u$. Put $p = q = \varepsilon$ in the definition of σ_L to see that $v \in L$. Thus if any σ_L-class intersects L, it is contained in L. Therefore L is a union of σ_L-classes.

c) Let ρ be a congruence on A^* such that L is a union of ρ-classes. Then

$$\begin{aligned} & (u, v) \in \rho \\ \Rightarrow\ & (\forall p, q \in A^*)((puq, pvq) \in \rho) \qquad \text{[since } \rho \text{ is a congruence]} \end{aligned}$$

$$\Rightarrow (\forall p, q \in A^*)((puq, pvq \in L) \vee (puq, pvq \notin L))$$
[since L is a union of ρ-classes]
$$\Rightarrow (\forall p, q \in A^*)(puq \in L \Leftrightarrow pvq \in L)$$
$$\Rightarrow (u, v) \in \sigma_L;$$

thus $\rho \subseteq \sigma_L$.

9.2 Suppose L is rational. Then it is recognized by a finite semigroup S by Proposition 9.4. By Proposition 9.6, Synt L divides S. Hence Synt L is finite.

Suppose Synt L is finite. The semigroup Synt L recognizes L by Proposition 9.6. Since L is recognized by a finite semigroup, it is rational by Proposition 9.4.

9.3 Let $K, L \in \mathcal{N}(A^+)$. If both K and L are finite, then $K \cup L$ and $K \cap L$ are finite and so $K \cup L, K \cap L \in \mathcal{N}(A^+)$. If one of K or L is finite and the other cofinite, then $K \cup L$ is cofinite and $K \cap L$ is finite and so $K \cup L, K \cap L \in \mathcal{N}(A^+)$. If both K and L are cofinite, then $K \cup L$ and $K \cap L$ are cofinite and so $K \cup L, K \cap L \in \mathcal{N}(A^+)$. So $\mathcal{N}(A^+)$ is closed under union and intersection. If K is finite, $A^+ - K$ is cofinite and so $A^+ - K \in \mathcal{N}(A^+)$; if K is cofinite, $A^+ - K$ is finite and so $A^+ - K \in \mathcal{N}(A^+)$. So $\mathcal{N}(A^+)$ is closed under complementation.

Let $L \in \mathcal{N}(A^+)$ and $a \in A$. If L is finite, it contains only word of length less than n for some fixed $n \in \mathbb{N}$. So $a^{-1}L$ and La^{-1} contain only words of length less than $n-1$. So $a^{-1}L$ and La^{-1} are finite and so $a^{-1}L, La^{-1} \in \mathcal{N}(A^+)$. On the other hand, if L is cofinite, it contains all words in A^+ of length greater than n for some fixed $n \in \mathbb{N}$. So $a^{-1}L$ and La^{-1} contain all words in A^+ of length greater than $n-1$. So $a^{-1}L$ and La^{-1} are cofinite and so $a^{-1}L, La^{-1} \in \mathcal{N}(A^+)$.

Let $L \in \mathcal{N}(B^+)$ and let $\varphi : A^+ \to B^+$ be a homomorphism. If L is finite, it contains only word of length less than n for some fixed $n \in \mathbb{N}$. Let $w \in A^+$ have length greater than n. Then $w\varphi$ has length greater than n and so $w\varphi \notin L$. So $L\varphi^{-1}$ contains only words of length less than n; thus $L\varphi^{-1}$ is finite and so $L\varphi^{-1} \in \mathcal{N}(A^+)$. On the other hand, if L is cofinite, it contains all words in A^+ of length greater than n for some fixed $n \in \mathbb{N}$. Let $w \in A^+$ have length greater than n. Then $w\varphi$ has length greater than n and so $w\varphi \in L$. So $L\varphi^{-1}$ contains all words in A^+ of length greater than n; thus $L\varphi^{-1}$ is cofinite and so $L\varphi^{-1} \in \mathcal{N}(A^+)$.

9.4 The class $\mathcal{V}(A^+)$ consists of all languages recognized by semigroups in 1; that is, recognized by E. Let $\varphi : A^+ \to E$ be a homomorphism. Suppose $L = L\varphi\varphi^{-1}$. Since E contains only one element and $L\varphi \subseteq E$, we have either $L\varphi = \varnothing$ or $L\varphi = E$. In the first case, $L = \varepsilon$; in the second case, $L = A^+$. So L is recognized by E if and only if L is either $\varnothing$ or A^+. Hence $\mathcal{V}(A^+) = \{\varnothing, A^+\}$.

Bibliography

CLIFFORD, A. H. 'Semigroups admitting relative inverses'. In: *Annals of Mathematics*. 2nd ser. 42 (1941), pp. 1037–1049. ISSN: 0003-486X. DOI: 10.2307/1968781.

CLIFFORD, A. H. & PRESTON, G. B. *The Algebraic Theory of Semigroups*. Vol. 1. Mathematical Surveys 7. Providence, R.I.: American Mathematical Society, 1961.

DISTLER, A. 'Classification and Enumeration of Finite Semigroups'. PhD thesis. University of St Andrews, 2010. URL: hdl.handle.net/10023/945.

GALLAGHER, P. 'On the Finite Generation and Presentability of Diagonal Acts, Finitary Power Semigroups and Schützenberger Products'. PhD thesis. University of St Andrews, 2005. URL: www-circa.mcs.st-and.ac.uk/Theses/pgphd.pdf.

GREEN, J. A. 'On the structure of semigroups'. In: *Annals of Mathematics*. 2nd ser. 54 (1951), pp. 163–172. ISSN: 0003-486X. DOI: 10.2307/1969317.

GRILLET, P.-A. 'A short proof of Rédei's theorem'. In: *Semigroup Forum* 46, no. 1 (1993), pp. 126–127. ISSN: 0037-1912. DOI: 10.1007/BF02573555.

——— *Semigroups: An Introduction to the Structure Theory*. Monographs and Textbooks in Pure and Applied Mathematics 193. New York: Marcel Dekker Inc., 1995. ISBN: 0-8247-9662-4.

HOWIE, J. M. *Fundamentals of Semigroup Theory*. London Mathematical Society Monographs (New Series) 12. New York: Clarendon Press, Oxford University Press, 1995. ISBN: 0-19-851194-9.

KROHN, K. & RHODES, J. 'Algebraic theory of machines I. Prime decomposition theorem for finite semigroups and machines'. In: *Transactions of the American Mathematical Society* 116 (1965), pp. 450–464. ISSN: 0002-9947. DOI: 10.2307/1994127.

LALLEMENT, G. *Semigroups and Combinatorial Applications*. New York, Chichester and Brisbane: John Wiley & Sons, 1979. ISBN: 0-471-04379-6.

——— 'Augmentations and wreath products of monoids'. In: *Semigroup Forum* 21, no. 1 (1980), pp. 89–90. ISSN: 0037-1912. DOI: 10.1007/BF02572539.

MALCEV, A. I. 'On the immersion of an algebraic ring into a field'. In: *Mathematische Annalen* 113 (1937), pp. 686–691. DOI: 10.1007/BF01571659.

MILLER, D. D. & CLIFFORD, A. H. 'Regular $\mathcal{D}$-classes in semigroups'. In: *Transactions of the American Mathematical Society* 82 (1956), pp. 270–280. ISSN: 0002-9947. DOI: 10.2307/1992989.

ORE, Ø. 'Linear equations in non-commutative fields'. In: *Annals of Mathematics*. 2nd ser. 32, no. 3 (July 1931), pp. 463–477. DOI: 10.2307/1968245.

PRESTON, G. B. 'Inverse semi-groups with minimal right ideals'. In: *Journal of the London Mathematical Society*. 1st ser. 29 (1954), pp. 404–411. ISSN: 0024-6107. DOI: 10.1112/jlms/s1-29.4.404.

——— 'Representations of inverse semi-groups'. In: *Journal of the London Mathematical Society*. 1st ser. 29 (1954), pp. 411–419. ISSN: 0024-6107. DOI: 10.1112/jlms/s1-29.4.411.

RÉDEI, L. *Theorie der Endlich Erzeugbaren Kommutativen Halbgruppen*. Vol. 41. Hamburger Mathematische Einzelschriften. Würzburg: Physica-Verlag, 1963. See Rédei, *The Theory of Finitely Generated Commutative Semigroups* for a translation.

——— *The Theory of Finitely Generated Commutative Semigroups*. Ed. by N. Reilly. Oxford: Pergamon Press, 1965.

REES, D. 'On semi-groups'. In: *Proceedings of the Cambridge Philosophical Society* 36, no. 4 (1940), pp. 387–400. DOI: 10.1017/S0305004100017436.

——— 'On the group of a set of partial transformations'. In: *Journal of the London Mathematical Society*. 1st ser. 22 (1947), 281–284 (1948). ISSN: 0024-6107. DOI: 10.1112/jlms/s1-22.4.281.

SCHÜTZENBERGER, M.-P. '$\overline{\mathcal{D}}$ représentation des demi-groupes'. In: *Comptes rendus hebdomadaires des séances de l'Académie des Sciences* 244 (1957), pp. 1994–1996.

SUSCHKEWITSCH, A. 'Über die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit'. In: *Mathematische Annalen* 99 (1928), pp. 30–51. DOI: 10.1007/BF01459084.

TAMURA, T. & KIMURA, N. 'On decompositions of a commutative semigroup'. In: *Kōdai Mathematical Seminar Reports* 6, no. 4 (1954), pp. 109–112. ISSN: 0023-2599. DOI: 10.2996/kmj/1138843534.

VAGNER, V. V. 'Generalized groups'. In: *Doklady Akademii Nauk SSSR* 84 (1952), pp. 1119–1122.

COLOPHON

These notes were typeset by the author using XeLaTeX, with a custom style utilizing the packages *fontspec*, *xunicode*, *xltxtra*, *titlesec*, *titletoc*, *booktabs*, *amsthm*, and *amsmath*. Diagrams were created using PGF/Ti*k*Z.

The main text is set in Minion Pro; many mathematical symbols in MnSymbol; shell letters in DejaVu Sans.

The bibliography and citations were compiled using the *biblatex* package and *Biber* backend.