Chapter I.

ELEMENTARY PROPERTIES.

This chapter contains basic first properties of commutative semigroups: idempotents, subsemigroups, homomorphisms and congruences, ideals, ideal extensions, $\mathcal{H}$-classes and Schützenberger groups, free commutative semigroups, presentations. It is written for readers who are not familiar with semigroups and can therefore expect a few surprises.

Many results in this chapter are stated for commutative semigroups but extend to all semigroups (with suitable modifications); interested readers should consult Clifford & Preston [1961], Howie [1976], [1995], or Grillet [1995].

1. FIRST RESULTS.

1. A **semigroup** is a set S together with an associative binary operation on S. (This is the only axiom.)

The name "semigroup" suggests a generalization of groups. To disabuse the reader of this erroneous belief we compare the number of distinct (not isomorphic) groups of order n with the number of distinct (not isomorphic or antiisomorphic) semigroups of order n, which has been determined for $n \leqq 8$ (Jürgensen & Wick [1977]; Sato, Yama, & Tokizawa [1991]):

All Semigroups

n	Groups	Semigroups
2	1	4
3	1	18
4	2	126
5	1	1160
6	2	15,973
7	1	836,021
8	5	1,843,120,128

P. A. Grillet, *Commutative Semigroups*

The number of semigroups of order 9 has not been determined; it is known to exceed 52,952,000,000,000, but probably not by much (Jürgensen, Migliorini, & Szép [1991]).

A semigroup is **commutative** when its operation is commutative. (Commutative groups are called *abelian.*) Commutative semigroups are not as numerous as general semigroups but are still much more numerous than abelian groups:

Commutative Semigroups

n	Groups	Semigroups
2	1	3
3	1	12
4	2	58
5	1	325
6	1	2143
7	1	17,291
8	3	221,805
9	2	11,545,843

The number of commutative semigroups of order 9 is from Grillet [1996N].

These large numbers suggest that even commutative semigroups are quite unlike groups and constitute a wholly different kind of algebraic object.

2. There are some natural examples of commutative semigroups.

We denote by $\mathbb{N} = \{0, 1, 2, \ldots, n, \ldots\}$ the additive semigroup of natural numbers. $\mathbb{N}$ is a commutative semigroup under multiplication as well. We also denote by $\mathbb{N}^+ = \{1, 2, \ldots, n, \ldots\}$ the additive semigroup of all positive natural numbers, by $\mathbb{Q}^+$ the additive semigroup of all positive rational numbers, and by $\mathbb{R}^+$ the additive semigroup of all positive real numbers.

Abelian groups are commutative semigroups.

A **semilattice** (short for **lower semilattice**) is a partially ordered set in which any two elements a and b have a greatest lower bound (or meet, or infimum) $a \wedge b$. Every lower semilattice is a commutative semigroup under the binary operation $\wedge$.

Groups and semilattices lie wholly outside semigroup theory. By well-established tradition, we regard as solved any problem which can be stated in terms of groups or semilattices (we dump it onto other unsuspecting mathematicians).

Every commutative ring or algebra is a commutative semigroup under multiplication. In fact, many arithmetic properties of rings are now studied in purely multiplicative terms. (Constructing rings from semigroups is even more fruitful; semigroup algebras are a major employer of commutative semigroups.)

3. The operation $S \times S \longrightarrow S$ on a semigroup S is usually written like a multiplication $(x,y) \longmapsto xy$; sometimes (for instance, in $\mathbb{N}$) like an addition $(x,y) \longmapsto x+y$. In the multiplicative notation, **associativity** is the property

$$x(yz) \;=\; (xy)z \text{ for all } x,y,z \in S;$$

commutativity is the property

$$xy \;=\; yz \text{ for all } x,y \in S.$$

Associativity and commutativity have a number of consequences which we hope are well known to the reader. Associativity allows products of three or more elements to be written without parentheses. Commutativity implies that a product does not depend on the order of its terms:

$$x_{\sigma 1}\, x_{\sigma 2} \cdots x_{\sigma n} \;=\; x_1\, x_2 \cdots x_n$$

for every permutation σ of $\{1,2,\dots,n\}$.

Powers are particular cases of products. When a is an element of a semigroup S and n is a positive integer, then a^n is the product of n elements of S all equal to a (with $a^n = a$ if $n = 1$). If S has an identity element 1 one can also define $a^0 = 1$. In a commutative semigroup S, the equalities

$$x^m\, x^n \;=\; x^{m+n}, \quad (x^m)^n \;=\; x^{mn}, \quad x^n\, y^n \;=\; (xy)^n$$

hold for all $x,y \in S$ and $m,n > 0$ ($m,n \geqq 0$ if S has an identity element). In the additive notation, products $x_1\, x_2 \cdots x_n$ become sums $x_1 + x_2 + \cdots + x_n$ and powers x^n become positive integer multiples nx.

4. An **identity element** of a semigroup S is an element e of S such that $ea = ae = a$ for all $a \in S$. When an identity element exists, it is unique, and we normally denote it by 1 (by 0 in the additive notation). A semigroup with an identity element is a **monoid**.

In a monoid, **empty** products (= products $a_1\, a_2 \cdots a_n$ of elements of S in which $n = 0$) are, by definition, equal to the identity element; for instance, zero powers $a^0 = 1$.

An identity element can be adjoined to any semigroup S: given $1 \notin S$, define an operation on $S \cup \{1\}$ as follows: 1 is an identity element and xy is the same in S and $S \cup \{1\}$ for all $x,y \in S$. Then $S \cup \{1\}$ is a monoid, which is commutative if S is commutative.

The identity element of $S \cup \{1\}$ is not the same as the identity element of S

in case the latter exists. Hence the following construction:

$$S^1 = \begin{cases} S & \text{if } S \text{ has an identity element,} \\ S \cup \{1\} & \text{if } S \text{ does not have an identity element,} \end{cases}$$

which adjoins an identity element only when necessary.

A **zero element** of a semigroup S is an element z of S such that $za = az = z$ for all $a \in S$. When a zero element exists, it is unique, and we normally denote it by 0 (by ∞ in the additive notation).

A zero element can be adjoined to any semigroup S: given $0 \notin S$, define an operation on $S \cup \{0\}$ as follows: 0 is a zero element and xy is the same in S and $S \cup \{0\}$ for all $x, y \in S$. Then $S \cup \{0\}$ is a semigroup with zero, which is commutative if S is commutative.

5. More generally, an **idempotent** of a semigroup S is an element e of S such that $e^2 = e$; then $e^n = e$ for all $n > 0$. We denote by $E(S)$ the set of all idempotents of S.

When S is commutative the **Rees order** on $E(S)$ is defined for all $e, f \in E(S)$ by:

$$e \leqq f \text{ if and only if } ef = e.$$

If an identity element (a zero element) exists, then it is the greatest (the least) element of $E(S)$ under the Rees order.

Proposition 1.1. *When S is a commutative semigroup, then $E(S)$ is a (possibly empty) semilattice under the Rees order, in which $e \wedge f = ef$ for all e and f.*

Proof. First the Rees order is a partial order relation: for all $e, f, g \in E(S)$, $e \leqq e$ since e is idempotent; $e \leqq f \leqq e$ implies $e = ef = fe = f$; and $e \leqq f \leqq g$ implies $e = ef = efg = eg$ and $e \leqq g$. Also $e(ef) = ef$ and $(ef)f = ef$, so that $ef \leqq e, f$. If conversely $g \leqq e$ and $g \leqq f$, then $efg = ef$ and $g \leqq ef$. Thus ef is the infimum of e and f in $E(S)$. □

The Rees order can be defined in any semigroup S and is always a partial order relation on $E(S)$ (Rees [1940]); but then $E(S)$ is not necessarily a semilattice. It was generalized to arbitrary elements by Mitsch [1986], [1994].

Corollary 1.2. *Let S be a commutative semigroup. If every element of S is idempotent, then S is a semilattice under the Rees order, in which $a \wedge b = ab$ for all a and b. If conversely Y is a semilattice, then $(Y, \wedge)$ is a commutative semigroup in which every element is idempotent, and the Rees order on $(Y, \wedge)$ is the given partial order on Y.*

Accordingly, commutative semigroups in which every element is idempotent may be identified with (lower) semilattices, and are, in fact, called semilattices.

6. Subsets $A, B \subseteq S$ of a semigroup S are multiplied by:

$$AB = \{ab \mid a \in A, b \in B\}.$$

In particular,

$$Ac = \{ac \mid a \in A\} \text{ and } cB = \{cb \mid b \in B\}$$

for all $A, B \subseteq S$ and $c \in S$. Multiplication of subsets inherits associativity and commutativity from S.

A **subsemigroup** of a semigroup S is a subset T of S which is closed under the operation on S ($xy \in T$ for all $x, y \in T$); equivalently, such that $TT \subseteq T$. For instance, S and the empty set are subsemigroups of S.

Every subsemigroup T of S inherits a semigroup operation $T \times T \longrightarrow T$ from S; this semigroup T is also called a subsemigroup of S. If S is commutative, then so is T.

Every intersection of subsemigroups of S is a subsemigroup of S. Hence there is for every subset X of S a smallest subsemigroup T of S which contains X; T is the intersection of all the subsemigroups of S which contain X, and is the subsemigroup (sometimes denoted by $\langle X \rangle$ or by X^*) **generated by** X.

Proposition 1.3. *The subsemigroup generated by a subset X is the set of all products of one or more elements of X. In a commutative semigroup, the subsemigroup generated by a subset X is the set of all products of positive powers of one or more distinct elements of X.*

Proof. A subsemigroup which contains X must by induction contain all nonempty products of elements of X. Conversely the set T of all nonempty products of elements of X is closed under multiplication and contains all products of one element of X, i.e. contains X.

Every sequence $x_1, x_2, \dots, x_n$ of elements of X can be permuted into a sequence $y_1, \dots, y_1, y_2, \dots, y_2, \dots, y_k, \dots, y_k$, where $y_1, y_2, \dots, y_k$ are the distinct elements of $\{x_1, x_2, \dots, x_n\}$. In a commutative semigroup, the products $x_1 x_2 \cdots x_n$ and $y_1 \cdots y_1 y_2 \cdots y_2 \cdots y_k \cdots y_k$ are equal; the latter is a product of positive powers of distinct elements of X. □

For example, the **cyclic** subsemigroup generated by $X = \{x\}$ consists of all the positive powers of x.

If the subsemigroup generated by X is S itself, then X **generates** S and the elements of X are **generators** of S; this means that every element of S is the product of one or more elements of X. A semigroup is **finitely generated** when it is generated by a finite subset, **cyclic** when it is generated by a single element.

Proposition 1.3 has an analogue for monoids. When S is a monoid, a **submonoid** of S is a subsemigroup T of S which contains the identity element of S; then T is a monoid in its own right, with the same identity element as S.

Proposition 1.4. *In a monoid, the submonoid generated by a subset X is the set of all products of elements of X. In a commutative monoid, the submonoid generated by a subset X is the set of all products of positive powers of distinct elements of X.*

This works since empty products yield the identity element.

2. HOMOMORPHISMS AND CONGRUENCES.

1. Let S and T be semigroups. A **homomorphism** of semigroups of S into T is a mapping $\varphi : S \longrightarrow T$ such that $\varphi(ab) = \varphi(a)\,\varphi(b)$ for all $a,b \in S$. Semigroup homomorphisms preserve all nonempty products:

$$\varphi\left(a_1 a_2 \cdots a_n\right) = \varphi(a_1)\,\varphi(a_2)\,\cdots\,\varphi(a_n)$$

and preserve positive powers: $\varphi(a^n) = \varphi(a)^n$.

The identity mapping 1_S on a semigroup S is a homomorphism of S onto S. If $\varphi : S \longrightarrow T$ and $\psi : T \longrightarrow U$ are homomorphisms, then so is $\psi \circ \varphi : S \longrightarrow U$. An **isomorphism** of semigroups is a bijective homomorphism; the inverse bijection is also an isomorphism.

When T is commutative, the pointwise product

$$(\varphi.\psi)(a) = \varphi(a)\,\psi(a)$$

of two homomorphisms $\varphi, \psi : S \longrightarrow T$ is a homomorphism $\varphi.\psi : S \longrightarrow T$. With this operation the set $\mathrm{Hom}\,(S,T)$ of all homomorphisms of S into T becomes a commutative semigroup.

2. Semigroup homomorphisms share a number of basic properties with mappings and with homomorphisms of algebraic systems in general.

When S and T are sets, a mapping $\varphi : S \longrightarrow T$ has a **range** or **image** $\mathrm{im}\,\varphi = \varphi(S) \subseteq T$ and induces an equivalence relation $\ker\varphi$ on S,

$$\ker\varphi = \{\,(a,b) \in S \times S \mid \varphi(a) = \varphi(b)\,\}.$$

This provides a quotient set $S/\ker\varphi$ (the set of all equivalence classes) and a **projection** or canonical mapping $S \longrightarrow S/\ker\varphi$, which sends $x \in S$ to its equivalence class. Then φ induces a bijection $S/\ker\varphi \longrightarrow \operatorname{im}\varphi$, which sends the equivalence class of $x \in S$ to $\varphi(x)$, and φ can be reconstructed by composing the projection $S \longrightarrow S/\ker\varphi$, the bijection $S/\ker\varphi \longrightarrow \operatorname{im}\varphi$, and the inclusion mapping $\operatorname{im}\varphi \longrightarrow T$.

$$\begin{tikzcd}
S \arrow[r, "\varphi"] \arrow[d] & T \\
S/\ker\varphi \arrow[r] & \operatorname{im}\varphi \arrow[u]
\end{tikzcd}$$

Homomorphisms of groups have similar properties, with the important difference that quotient groups are constructed from subgroups. As we shall see, semigroups are more like sets than like groups in that, in general, quotient semigroups cannot be constructed from subsets and must be constructed from equivalence relations.

3. First, given a semigroup S and an equivalence relation $\mathcal{E}$ on S, how can we induce an operation on the quotient set $S/\mathcal{E}$? The answer is:

Proposition 2.1. *Let S be a semigroup and $\mathcal{E}$ be an equivalence relation on S. The following conditions are equivalent:*

(1) *there exists an associative operation on $S/\mathcal{E}$ such that the projection $S \longrightarrow S/\mathcal{E}$ is a homomorphism;*

(2) *for all $a,b,c,d \in S$, if $a \mathcal{E} c$ and $b \mathcal{E} d$, then $ab \mathcal{E} cd$.*

When either condition holds, there is only one associative operation on $S/\mathcal{E}$ such that the projection $a \longmapsto E_a$ is a homomorphism; the product of E_a and E_b in $S/\mathcal{E}$ is the equivalence class which contains their product as subsets of S, namely E_{ab}. If S is commutative, then so is $S/\mathcal{E}$.

E_a denotes the $\mathcal{E}$-class of a (= the equivalence class of a modulo $\mathcal{E}$).

Proof. If $a \longmapsto E_a$ is a homomorphism, then $E_a = E_b$, $E_c = E_d$ implies $E_{ac} = E_a.E_c = E_b.E_d = E_{bd}$; thus (1) implies (2).

Conversely let (2) hold. By (2), $c \in E_a$, $d \in E_b$ implies $cd \in E_{ab}$; thus the product $E_a E_b$ of E_a and E_b as subsets of S is contained in the single equivalence class E_{ab}. If the projection $a \longmapsto E_a$ is a homomorphism, then the product $E_a.E_b = E_{ab}$ of E_a and E_b in $S/\mathcal{E}$ is the equivalence class which contains their product $E_a E_b$ as subsets of S; there is only one operation on $S/\mathcal{E}$ with this property, and it is the operation described in the statement. With this operation, $E_a.E_b = E_{ab}$ holds in $S/\mathcal{E}$; hence $S/\mathcal{E}$ is a semigroup:

$$E_a.(E_b.E_c) = E_a.E_{bc} = E_{a(bc)} = E_{(ab)c} = E_{ab}.E_c = (E_a.E_b).E_c$$

and the projection $S \longrightarrow S/\mathcal{E}$ is a homomorphism. Thus (2) implies (1). If S is commutative, then

$$E_b.E_a = E_{ba} = E_{ab} = E_a.E_b$$

and $S/\mathcal{E}$ is commutative. □

A **congruence** on a semigroup S is an equivalence relation $\mathcal{E}$ on S which satisfies condition (2) in Proposition 2.1; then the **quotient semigroup** of S by $\mathcal{E}$ is the semigroup $S/\mathcal{E}$ in Proposition 2.1, such that the projection $S \longrightarrow S/\mathcal{E}$ is a homomorphism. The equivalence relation on S induced by the projection $S \longrightarrow S/\mathcal{E}$ is $\mathcal{E}$ itself.

A congruence on a group is completely determined by the equivalence class of the identity element, so that quotient groups can be constructed from normal subgroups. This nice property does not extend to semigroups; not even to commutative monoids with a zero element. For instance let S be the semilattice (also a monoid) $S = \{0, e, 1\}$ in which $0 < e < 1$. The equivalence relation whose classes are $\{e, 0\}$ and $\{1\}$ is a congruence; so is the equality (whose classes are $\{0\}$, $\{e\}$, and $\{1\}$); thus a congruence on S is not determined by the class of the identity element. Similarly, the equivalence relation whose classes are $\{1, e\}$ and $\{0\}$ is a congruence; hence a congruence on S is not determined by the class of the zero element.

4. Armed with quotient semigroups we can now state the **Homomorphism Theorem** (also known as the **First Isomorphism Theorem**):

Theorem 2.2. *When $\varphi : S \longrightarrow T$ is a homomorphism of semigroups:*

(1) $\operatorname{Im}\varphi = \varphi(S)$ *is a subsemigroup of T;*

(2) $\ker\varphi$ *is a congruence on S;*

(3) *there exists an isomorphism $S/\ker\varphi \longrightarrow \operatorname{Im}\varphi$ such that the diagram*

$$\begin{tikzcd} S \arrow[r, "\varphi"] \arrow[d] & T \\ S/\ker\varphi \arrow[r] & \operatorname{Im}\varphi \arrow[u] \end{tikzcd}$$

commutes; in particular $S/\ker\varphi \cong \operatorname{Im}\varphi$. If S and T are commutative, then so are $\operatorname{Im}\varphi$ and $S/\ker\varphi$.

Proof. When $\varphi : S \longrightarrow T$ is a homomorphism, $\operatorname{Im}\varphi = \varphi(S)$ is a subsemigroup of T, since $\varphi(a)\,\varphi(b) = \varphi(ab)$ for all $a, b \in S$; $\mathcal{E} = \ker\varphi$ is a congruence on S, since $\varphi(a) = \varphi(b)$, $\varphi(c) = \varphi(d)$ implies $\varphi(ac) = \varphi(a)\,\varphi(c) =$

$\varphi(b)\,\varphi(d) = \varphi(bd)$; and the bijection $E_a \longmapsto \varphi(a)$ is a homomorphism, since it sends $E_a{\cdot}E_b = E_{ab}$ to $\varphi(ab) = \varphi(a)\,\varphi(b)$. □

Let S and T be semigroups. By Theorem 2.2, S is isomorphic to a subsemigroup of T if and only if there exists an injective homomorphism (an **embedding**) of S into T; then S can be **embedded** into T. Similarly, T is isomorphic to a quotient semigroup of S if and only if there exists a surjective homomorphism of S onto T; then T is a **homomorphic image** of S.

5. Theorem 2.2 can be deduced from more general results which allow one homomorphism to factor through another and help construct diagrams of semigroups and homomorphisms.

Proposition 2.3. *Let $\varphi : S \longrightarrow T$ and $\psi : U \longrightarrow T$ be homomorphisms of semigroups. If φ is injective, then ψ factors through φ ($\psi = \varphi \circ \xi$ for some homomorphism $\xi : U \longrightarrow S$) if and only if* $\operatorname{Im}\psi \subseteq \operatorname{Im}\varphi$*; and then ψ factors uniquely through φ (ξ is unique). If φ and ψ are injective and* $\operatorname{Im}\psi = \operatorname{Im}\varphi$*, then ξ is an isomorphism.*

$$\begin{tikzcd}
S \arrow[r, "\varphi"] & T \\
& U \arrow[ul, "\xi"] \arrow[u, "\psi"']
\end{tikzcd}$$

This is clear.

Proposition 2.4. *Let $\varphi : S \longrightarrow T$ and $\psi : S \longrightarrow U$ be homomorphisms of semigroups. If φ is surjective, then ψ factors through φ ($\psi = \xi \circ \varphi$ for some homomorphism $\xi : T \longrightarrow U$) if and only if* $\ker\varphi \subseteq \ker\psi$*; and then ψ factors uniquely through φ (ξ is unique). If φ and ψ are surjective and* $\ker\varphi = \ker\psi$*, then ξ is an isomorphism.*

$$\begin{tikzcd}
S \arrow[r, "\varphi"] \arrow[d, "\psi"'] & T \arrow[dl, "\xi"] \\
U &
\end{tikzcd}$$

Proof. If $\psi = \xi \circ \varphi$, then $\varphi(a) = \varphi(b)$ implies $\psi(a) = \xi(\varphi(a)) = \xi(\varphi(b)) = \psi(b)$, and $\ker\varphi \subseteq \ker\psi$.

Conversely, assume that φ is surjective and that $\ker\varphi \subseteq \ker\psi$. Let ξ be the set of ordered pairs

$$\xi \;=\; \{\,(\varphi(a), \psi(a)) \in T \times U \;\big|\; a \in S\}.$$

For every $t \in T$, there exists $u \in U$ such that $(t,u) \in \xi$, since φ is surjective; if moreover $(t,u) \in \xi$, $(t',u') \in \xi$, and $t = t'$, then $u = u'$, since $\ker\varphi \subseteq \ker\psi$.

Thus ξ is a mapping of T into U. Also $\xi\,(\varphi(a)) = \psi(a)$ for all $a \in S$ by definition and

$$\xi\big(\varphi(a)\,\varphi(b)\big) \;=\; \xi\big(\varphi(ab)\big) \;=\; \psi(ab) \;=\; \psi(a)\,\psi(b) \;=\; \xi\,(\varphi(a))\,\xi\,(\varphi(b))$$

for all $a,b \in S$, so that ξ is a homomorphism. Thus ψ factors through φ; ψ factors uniquely through φ since any mapping χ such that $\psi = \chi \circ \varphi$ must contain all ordered pairs $\big(\varphi(a), \psi(a)\big)$ and must coincide with ξ. If moreover ψ is surjective and $\ker\varphi = \ker\psi$, then ξ is injective, since $\xi\,(\varphi(a)) = \xi\,(\varphi(b))$ implies $\psi(a) = \psi(b)$ and $\varphi(a) = \varphi(b)$, is surjective, since $\operatorname{Im}\xi = \operatorname{Im}(\xi \circ \varphi) = \operatorname{Im}\psi$, and is an isomorphism. □

Analogues of the (other) two Isomorphism Theorems also hold for semigroups. The most useful employ the following constructions. Let $\varphi : S \longrightarrow T$ be a semigroup homomorphism. The **direct image** under φ of a subsemigroup S' of S is the subset $\varphi(S') = \{\varphi(x) \mid s \in S'\}$ of T. The **inverse image** under φ of a subsemigroup T' of T is

$$\varphi^{-1}(T') \;=\; \{x \in S \mid \varphi(x) \in T\}$$

Proposition 2.5. *Let $\varphi : S \longrightarrow T$ be a homomorphism of semigroups and* $\mathcal{C} = \ker\varphi$.

If S' is a subsemigroup of S, then $\varphi(S')$ is a subsemigroup of T.

If T' is a subsemigroup of T, then $\varphi^{-1}(T')$ is a subsemigroup of S and a union of $\mathcal{C}$-classes.

If φ is surjective this defines an order preserving one-to-one correspondence between subsemigroups of T and subsemigroups of S that are unions of $\mathcal{C}$-classes.

Proof. If S' is a subsemigroup of S, then $\varphi(S')$ is a subsemigroup of T, since $\varphi(x)\,\varphi(y) = \varphi(xy) \in \varphi(S')$ for all $x,y \in S'$.

If T' is a subsemigroup of T, then $\varphi^{-1}(T')$ is a union of $\mathcal{C}$-classes and is a subsemigroup of S since $\varphi(x)$, $\varphi(y) \in T'$ implies $\varphi(xy) = \varphi(x)\,\varphi(y) \in T'$.

If φ is surjective, then $\varphi(\varphi^{-1}(T')) = T'$ for every $T' \subseteq T$. Also $S' \subseteq \varphi^{-1}(\varphi(S'))$ for every $S' \subseteq S$; conversely, $x \in \varphi^{-1}(\varphi(S'))$ implies $\varphi(x) = \varphi(s)$ for some $s \in S'$ and $x \in S'$ if $S' \subseteq S$ is a union of $\mathcal{C}$-classes. □

Similarly, the **direct image** under a semigroup homomorphism $\varphi : S \longrightarrow T$ of a congruence $\mathcal{E}$ on S is the binary relation

$$\varphi(\mathcal{E}) \;=\; \{\big(\varphi(a), \varphi(b)\big) \in T \times T \mid (a,b) \in \mathcal{E}\};$$

equivalently, the direct image of $\mathcal{E} \subseteq S \times S$ under $\varphi \times \varphi : S \times S \longrightarrow T \times T$. The **inverse image** under φ of a congruence $\mathcal{F}$ on T is the binary relation

$$\varphi^{-1}(\mathcal{F}) = \{(a,b) \in S \times S \mid (\varphi(a), \varphi(b)) \in \mathcal{F}\};$$

equivalently, the inverse image of $\mathcal{F}$ under $\varphi \times \varphi$. We also say that $\varphi(\mathcal{E})$, $\varphi^{-1}(\mathcal{F})$ are **induced** by $\mathcal{E}$ and $\mathcal{F}$.

Proposition 2.6. *Let $\varphi : S \longrightarrow T$ be a homomorphism of semigroups and* $\mathcal{C} = \ker \varphi$.

If $\mathcal{F}$ is a congruence on T, then $\varphi^{-1}(\mathcal{F})$ is a congruence on S which contains $\mathcal{C}$; if φ is surjective, then $S/\varphi^{-1}(\mathcal{F}) \cong T/\mathcal{F}$.

If φ is surjective and $\mathcal{E}$ is a congruence on S which contains $\mathcal{C}$, then $\varphi(\mathcal{E})$ is a congruence on T, and $T/\varphi(\mathcal{E}) \cong S/\mathcal{E}$.

If φ is surjective this defines an order preserving one-to-one correspondence between congruences on T and congruences on S that contain $\mathcal{C}$.

Proof. Let $\mathcal{F}$ be a congruence on T and $\rho : T \longrightarrow T/\mathcal{F}$ be the projection, so that $\mathcal{F} = \ker \rho$. We see that $\varphi^{-1}(\mathcal{F}) = \ker(\rho \circ \varphi)$. Therefore $\varphi^{-1}(\mathcal{F})$ is a congruence on S. If φ is surjective, then $S/\varphi^{-1}(\mathcal{F}) \cong \operatorname{Im}(\rho \circ \varphi) = \operatorname{Im} \rho = T/\mathcal{F}$ by Theorem 2.2.

Now let φ be surjective and $\mathcal{E}$ be a congruence on S which contains $\mathcal{C}$. Let $\rho : S \longrightarrow S/\mathcal{E}$ be the projection. By Proposition 2.4, ρ factors through φ: $\rho = \xi \circ \varphi$ for some homomorphism $\xi : T \longrightarrow S/\mathcal{E}$. We have $\varphi(\mathcal{E}) = \ker \xi$: indeed $(a,b) \in \mathcal{E}$ implies $\xi(\varphi(a)) = \rho(a) = \rho(b) = \xi(\varphi(b))$ and $(\varphi(a), \varphi(b)) \in \ker \xi$; if conversely $(t,u) \in \ker \xi$, then $t = \varphi(a)$, $u = \varphi(b)$ for some $a, b \in S$, $(a,b) \in \mathcal{E}$ since $\rho(a) = \xi(t) = \xi(u) = \rho(b)$, and $(t,u) = (\varphi(a), \varphi(b)) \in \varphi(\mathcal{E})$. Therefore $\varphi(\mathcal{E})$ is a congruence; by Theorem 2.2, $T/\varphi(\mathcal{E}) \cong \operatorname{Im} \xi = \operatorname{Im} \rho = S/\mathcal{E}$, since φ is surjective.

If φ is surjective, then $\varphi \times \varphi$ is surjective; therefore $\varphi(\varphi^{-1}(\mathcal{F})) = \mathcal{F}$ for all $\mathcal{F} \subseteq T \times T$. Similarly $\mathcal{E} \subseteq \varphi^{-1}(\varphi(\mathcal{E}))$ for all $\mathcal{E} \subseteq S \times S$. If $\mathcal{E}$ is a congruence on S and $\mathcal{C} \subseteq \mathcal{E}$, and $(a,b) \in \varphi^{-1}(\varphi(\mathcal{E}))$, then $(\varphi(a), \varphi(b)) \in \varphi(\mathcal{E})$, $(\varphi(a), \varphi(b)) = (\varphi(c), \varphi(d))$ for some $(c,d) \in \mathcal{E}$, and, as above, $(a,c) \in \mathcal{E}$ and $(b,d) \in \mathcal{E}$; hence $(a,b) \in \mathcal{E}$, so that $\varphi^{-1}(\varphi(\mathcal{E})) = \mathcal{E}$. □

It follows from Propositions 2.5, 2.6 that the subsemigroups of a quotient semigroup $S/\mathcal{C}$ are precisely the sets of $\mathcal{C}$-classes whose unions are subsemigroups of S; and that the congruences on $S/\mathcal{C}$ are precisely the congruences induced on $S/\mathcal{C}$ by congruences on S that contain $\mathcal{C}$.

6. Similar results hold for monoids. When S and T are monoids, a **homomorphism** of monoids of S into T is a homomorphism of semigroups $\varphi : S \longrightarrow T$ such that $\varphi(1) = 1$. Then φ preserves all products and nonnegative powers.

When S is a monoid and $\mathcal{E}$ is a congruence on S, then

$$E_1.E_a \;=\; E_{1a} \;=\; E_a \;=\; E_{a1} \;=\; E_a.E_1$$

for all $a \in S$, so that $S/\mathcal{E}$ is a monoid and the projection $S \longrightarrow S/\mathcal{E}$ is a homomorphism of monoids. If therefore $\varphi : S \longrightarrow T$ is a homomorphism of monoids, then, as in Theorem 2.2, $\operatorname{Im}\varphi$ is a submonoid of T, $\ker\varphi$ is a congruence on S, and there is an isomorphism $S/\ker\varphi \longrightarrow \operatorname{Im}\varphi$ such that the diagram

$$\begin{tikzcd}
S \arrow[r, "\varphi"] \arrow[d] & T \\
S/\ker\varphi \arrow[r] & \operatorname{Im}\varphi \arrow[u]
\end{tikzcd}$$

commutes; in particular $S/\ker\varphi \cong \operatorname{Im}\varphi$.

Results similar to Propositions 2.3, 2.4, 2.5, and 2.6 also hold for monoids; this is left to the reader.

7. We complete this section with some properties of congruences.

Proposition 2.7. *An equivalence relation $\mathcal{C}$ on a commutative semigroup S is a congruence if and only if, for all $a, b, c \in S$, $a \;\mathcal{C}\; b$ implies $ac \;\mathcal{C}\; bc$.*

Proof. If this condition holds, then $a \;\mathcal{C}\; b$, $c \;\mathcal{C}\; d$ implies $ac \;\mathcal{C}\; bc = cb \;\mathcal{C}\; db = bd$, and $\mathcal{C}$ is a congruence. The converse is clear. □

For instance the equality $=$ on a semigroup S is a congruence, and so is the **universal** congruence $\mathcal{U}$, of which S is the only equivalence class; $S/{=} \cong S$, whereas $S/\mathcal{U}$ is trivial.

Since congruences on a given semigroup S are subsets of $S \times S$, we can form their unions and intersections in $S \times S$. The following result is straightforward.

Proposition 2.8. *Let S be a semigroup. Every intersection of congruences on S is a congruence on S. The union of a chain of congruences on S is a congruence on S.*

In particular, the **empty intersection** $\bigcap_{i\in\emptyset} \mathcal{C}_i$ of congruences on S can be defined as the universal congruence on S; the **empty union** $\bigcup_{i\in\emptyset} \mathcal{C}_i$ of congruences on S can be defined as the equality on S.

By Proposition 2.8 there is for every binary relation $\mathcal{R} \subseteq S \times S$ a smallest congruence $\mathcal{C}$ on S which contains $\mathcal{R}$; $\mathcal{C}$ is the intersection of all the congruences which contain $\mathcal{R}$ and is the congruence **generated by** $\mathcal{R}$.

Proposition 2.9. *Let S be a commutative semigroup. The congruence $\mathcal{C}$ generated by $\mathcal{R} \subseteq S \times S$ can be constructed as follows. Let*

$$\mathcal{S} = \{ (xu, yu) \mid x, y \in S,\ u \in S^1,\ \textit{and}\ x\ \mathcal{R}\ y\ \ \textit{or}\ \ y\ \mathcal{R}\ x \}.$$

Then $a\ \mathcal{C}\ b$ if and only if there exist $n \geqq 1$ and $s_1, \dots, s_n \in S$ such that $a = s_1$, $s_n = b$, and $s_i\ \mathcal{S}\ s_{i+1}$ for all $1 \leqq i < n$.

Proof. We see that $\mathcal{S}$ contains $\mathcal{R}$ (let $u = 1 \in S^1$ in the definition of $\mathcal{S}$), is symmetric ($a\ \mathcal{S}\ b$ implies $b\ \mathcal{S}\ a$), and admits multiplication ($a\ \mathcal{S}\ b$ implies $ac\ \mathcal{S}\ bc$). Hence $\mathcal{C}$ is symmetric (reverse the sequence $s_1, \dots, s_n$ in the definition of $\mathcal{C}$) and admits multiplication. Moreover $\mathcal{C}$ contains the equality on S (let $n = 1$ in the definition), contains $\mathcal{S}$ (let $n = 2$), and is transitive. Thus $\mathcal{C}$ is a congruence and contains $\mathcal{R}$.

Conversely, a congruence which contains $\mathcal{R}$ must contain $\mathcal{S}$, since a congruence is symmetric and admits multiplication; and a congruence which contains $\mathcal{S}$ must contain $\mathcal{C}$, since a congruence is reflexive and transitive. □

Proposition 2.9 can be stated more simply as follows: every relation $a\ \mathcal{C}\ b$ follows from relations $x\ \mathcal{R}\ y$ by finitely many applications of the following inference rules: $a\ \mathcal{R}\ b$ implies $a\ \mathcal{C}\ b$; $a\ \mathcal{C}\ b$ implies $au\ \mathcal{C}\ bu$, for all $u \in S$; $a \in S$ implies $a\ \mathcal{C}\ a$; $a\ \mathcal{C}\ b$ implies $b\ \mathcal{C}\ a$; $a\ \mathcal{C}\ b$, $b\ \mathcal{C}\ c$ implies $a\ \mathcal{C}\ c$.

3. IDEALS.

1. An **ideal** of a semigroup S is a subset I of S such that $a \in I$ implies $ax \in I$ and $xa \in I$ for all $x \in S$; equivalently, such that $IS \subseteq I$ and $SI \subseteq I$. For instance, S and the empty set are ideals of S. If S is commutative, the condition $SI \subseteq I$ is sufficient.

Proposition 3.1. *Every union of ideals of S is an ideal of S. Every intersection of ideals of S is an ideal of S.*

By Proposition 3.1 there exists, for every subset X of S, an ideal of S which contains X and is contained in every ideal of S which contains X; this is the ideal of S **generated by** X.

Proposition 3.2. *In a commutative semigroup S, the ideal generated by a subset X is the set S^1X of all multiples of elements of X.*

Proof. S^1X is the product in S^1, which is contained in S since either $S^1X = SX$ or $S^1X = SX \cup 1X = SX \cup X \subseteq S$; contains $1X = X$; and is an ideal of S since $SS^1X \subseteq S^1X$. Conversely, an ideal which contains X also contains SX and S^1X. □

In particular (when S is commutative) the ideal generated by one element $a \in S$ is the set S^1a of all multiples of a; such ideals are called **principal**.

Proposition 3.3. *Let S be a commutative semigroup. If K is a minimal nonempty ideal of S, then K is a smallest nonempty ideal of S, and K is a group.*

Proof. Let I be a nonempty ideal. Since I and K are ideals, $IK \subseteq I \cap K$ and $I \cap K$ is a nonempty ideal. Since $I \cap K \subseteq K$ it follows that $K \subseteq I$.

When $a \in K$, then $Ka \subseteq K$ is an ideal of S; hence $Ka = K$. In particular $ea = a$ for some $e \in K$. Since every element of K has the form ax for some $x \in K$ it follows that e is an identity element of K. Then every element a of K has an inverse in K, since $ab = e$ for some $b \in K$, and K is a group. □

The smallest nonempty ideal of S, when it exists, is the **kernel** of S. Every finite commutative semigroup has a kernel; $\mathbb{N}$ does not.

Proposition 3.4. *Let $\varphi : S \longrightarrow T$ be a homomorphism of semigroups and* $\mathcal{C} = \ker \varphi$.

If φ is surjective and I is an ideal of S, then $\varphi(I)$ is an ideal of T.

If J is an ideal of T, then $\varphi^{-1}(J)$ is an ideal of S and a union of $\mathcal{C}$-classes.

If φ is surjective this defines an order preserving one-to-one correspondence between ideals of T and ideals of S that are unions of $\mathcal{C}$-classes.

Proof. If φ is surjective and I is an ideal of S, then $\varphi(I)$ is an ideal of T, since $\varphi(x)\,\varphi(y) = \varphi(xy) \in \varphi(I)$ for all $x \in S$ and $y \in I$.

If J is an ideal of T, then $\varphi^{-1}(J)$ is a union of $\mathcal{C}$-classes and is an ideal of S since $\varphi(y) \in J$ implies $\varphi(xy) = \varphi(x)\,\varphi(y) \in J$ for all $x \in S$.

If φ is surjective, then $\varphi(\varphi^{-1}(J)) = J$ for every $J \subseteq T$, and $\varphi^{-1}(\varphi(I)) = I$ for every $I \subseteq S$ that is a union of $\mathcal{C}$-classes, as in the proof of Proposition 2.5. □

2. Congruences on a group are determined by normal subgroups. In a semigroup, congruences are most easily constructed from ideals. The resulting quotient semigroups, discovered by Rees [1940], are peculiarly different from quotient groups and from quotient rings.

Proposition 3.5. *When I is an ideal of a semigroup S, the relation* $\mathcal{J}$

defined by

$$a \mathfrak{I} b \iff a = b \ \text{or} \ a,b \in I$$

is a congruence on S, the **Rees congruence** *of the ideal I.*

Proof. $\mathfrak{I}$ is an equivalence relation, and is a congruence since $a = b$ and $c,d \in I$ implies $ac, bd \in I$; $a,b \in I$ and $c = d$ implies $ac, bd \in I$; and $a,b,c,d \in I$ implies $ac, bd \in I$. □

The quotient semigroup $S/I = S/\mathfrak{I}$ is the **Rees quotient** of S by I. It is standard practice to identify the $\mathfrak{I}$-class $\{x\} \in S/I$ of each $x \notin I$ with $x \in S$. If $I = \varnothing$, then $S/I = S$. If $I \neq \varnothing$, the $\mathfrak{I}$-class $I \in S/I$ is a zero element and is denoted by 0; then $S/I = (S \backslash I) \cup \{0\}$ with the multiplication $.$ in which 0 is a zero element and

$$x \,.\, y = \begin{cases} xy \in S & \text{if } xy \notin I \\ 0 & \text{if } xy \in I \end{cases}$$

for all $x,y \in S \backslash I$. Thus the Rees quotient is obtained by squeezing I to a zero element (if $I \neq \varnothing$) and leaving $S \backslash I$ untouched.

3. The Rees quotient can be viewed as the completion of a partial semigroup into an authentic semigroup. In general a **partial binary operation** on a set P is a mapping $\mu : D \longrightarrow P$ whose domain D is a subset of $P \times P$: when $x,y \in P$, $\mu(x,y)$ is defined when $(x,y) \in D$ and is undefined otherwise. In the multiplicative notation, $\mu(x,y)$ is denoted by xy. A **partial semigroup** is a set P together with a partial binary operation on P which is **associative** in the sense that $x(yz) = (xy)z$ holds whenever $x,y,z \in P$ and both $x(yz)$ and $(xy)z$ are defined. (Other associativity conditions have been considered; see the book by Lyapin & Evseev [1997].)

When P and Q are partial semigroups, a **partial homomorphism** of P into Q is a mapping $\varphi : P \longrightarrow Q$ which preserves existing products: $\varphi(xy) = \varphi(x)\,\varphi(y)$ whenever xy is defined in P. If Q is a commutative semigroup, then the set $\mathrm{PHom}(P,Q)$ of all partial homomorphisms of P into Q is closed under pointwise addition and is a commutative semigroup; if P is an actual semigroup, then $\mathrm{PHom}(P,Q) = \mathrm{Hom}(P,Q)$.

Every subset A of a semigroup S is a partial semigroup for the partial operation $.$ induced by S in the obvious way: when $x,y \in A$, then $x \,.\, y$ is defined in A if and only if $xy \in A$, and then $x \,.\, y = xy$. When I is a nonempty ideal of S, the Rees quotient S/I is obtained from the partial semigroup $S \backslash I$ by adjoining a zero element and setting all undefined products to 0.

4. An **ideal extension** of a semigroup S by a semigroup Q with zero is a

semigroup E such that S is an ideal of E and Q is the Rees quotient $Q = E/S$. Ideal extensions were first studied by Clifford [1950].

The **ideal extension problem**, first considered by Clifford [1950], consists in constructing all ideal extensions of a given semigroup S by a given semigroup Q with zero; one may assume $S \cap Q = \emptyset$. This difficult problem is discussed in some detail in Clifford & Preston [1961], Grillet [1995], and especially Petrich [1973]. The particular case of monoids has a very nice solution, due to Clifford [1950]; another case will be seen in Chapter II. More general results are known but have had few applications to commutative semigroups.

When S is a subsemigroup of E, a **retraction** of E onto S is a homomorphism of E into S which is the identity on S.

Proposition 3.6. *Every ideal extension of a monoid S has a retraction $a \longmapsto ea = ae$, where e is the identity element of S.*

Proof. Let e be the identity element of S. In E we have $ea = (ea)e = e(ae) = ae$ for all $a \in E$, since ea and ae are in S. Let

$$\psi(a) \;=\; ea \;=\; eae \;=\; ae \;\in\; S$$

for all $a \in E$. Then $\psi(a) = a$ when $a \in S$, and $\psi(ab) = eabe = \psi(a)\,\psi(b)$ for all $a,b \in E$. □

An ideal extension E of S by Q is a **retract** ideal extension when there exists a retraction ψ of E onto S. Then the restriction $\varphi : Q\backslash 0 \longrightarrow S$ of ψ to $Q\backslash 0 = E\backslash S$ is a partial homomorphism, and the operation on E is determined as follows by the operation on S, the partial operation on $Q\backslash 0$, and the partial homomorphism φ. If $a,b \in Q\backslash 0$ and $ab \neq 0$ in Q, then ab is the same in Q and E. If $a,b \in Q\backslash 0$ and $ab = 0$ in $Q = E/S$, then, in E, $ab \in S$ and $ab = \psi(ab) = \varphi(a)\,\varphi(b)$. If $a \in Q\backslash 0$ and $x \in S$, then, in E, $ax = \psi(ax) = \varphi(a)\,x$ and $xa = \psi(xa) = x\,\varphi(a)$. If $x,y \in S$, then xy is the same in S and E.

Lemma 3.7. *Let S be a semigroup and Q be a semigroup with zero such that $S \cap Q = \emptyset$. If φ is a partial homomorphism of $Q\backslash 0$ into S, then the disjoint union $E = S \cup (Q\backslash 0)$, with the multiplication $*$ defined by*

$$\begin{cases} a*b = ab \in Q & \textit{if } ab \neq 0 \textit{ in } Q, \\ a*b = \varphi(a)\,\varphi(b) & \textit{if } ab = 0 \textit{ in } Q, \\ a*y = \varphi(a)\,y, \\ x*b = x\,\varphi(b), \\ x*y = xy \in S \end{cases}$$

for all $a, b \in Q\backslash 0$ and $x, y \in S$, is a retract ideal extension of S by Q, and every retract ideal extension of S by Q can be constructed in this fashion. Moreover, E is commutative if and only if S and Q are commutative.

Proof. Associativity in E follows in a long but straightforward manner from associativity in S, associativity in Q, and the hypothesis that φ is a partial homomorphism. Then it is clear that S is an ideal of E and that $E/S = Q$. Moreover the mapping $\psi : E \longrightarrow S$ defined by

$$\psi(a) = \varphi(a) \text{ for all } a \in Q\backslash\{0\},\ \psi(x) = x \text{ for all } x \in S,$$

is a retraction of E onto S. Conversely we saw that every retract ideal extension can be constructed as in the statement. □

The ideal extension constructed in Lemma 3.7 is **determined by** the partial homomorphism φ. Thus, an ideal extension is a retract ideal extension if and only if it is determined by a partial homomorphism:

Proposition 3.8. *Every ideal extension of a monoid S by a semigroup Q with zero is a retract ideal extension and is therefore determined by a partial homomorphism of $Q\backslash\{0\}$ into S, namely $a \longmapsto ea = ae$, where e is the identity element of S.*

This follows from Lemma 3.7 and Proposition 3.6.

4. DIVISIBILITY.

1. A **preorder** (also called **quasiorder**) is a binary relation which is reflexive and transitive; thus, a preorder which is also antisymmetric is an order relation.

On a commutative semigroup S the **Green's preorder** $\leqq_{\mathcal{H}}$ (also called the **divisibility preorder**) is defined by

$$a \leqq_{\mathcal{H}} b \iff a = tb \text{ for some } t \in S^1 \iff S^1 a \subseteq S^1 b.$$

if for example e and f are idempotents, then $e \leqq_{\mathcal{H}} f$ if and only if $e \leqq f$ in the Rees order: indeed $ef = e$ implies $e \leqq_{\mathcal{H}} f$; conversely, $e = tf$ implies $ef = tff = tf = e$.

Green's relation $\mathcal{H}$ is one of several relations introduced for semigroups in general by Green [1951]:

$$a \,\mathcal{H}\, b \iff a \leqq_{\mathcal{H}} b \text{ and } b \leqq_{\mathcal{H}} a \iff S^1 a = S^1 b.$$

Proposition 4.1. *In a commutative semigroup, $\mathcal{H}$ is a congruence.*

Proof. If $a \mathcal{H} b$, then $a = tb$ and $b = ua$ for some $t, u \in S^1$, $ac = tbc$ and $bc = uac$ for some $t, u \in S^1$, and $ac \mathcal{H} bc$. □

In a sense, $\mathcal{H}$ measures the extent of group-like behavior in semigroups. Thus, multiplication by elements of a semigroup induces permutations of its $\mathcal{H}$-classes:

Lemma 4.2. *Let H be an $\mathcal{H}$-class and $t \in S^1$. If $tH \subseteq H$, then the mapping $g_t : x \longmapsto tx$ of H into H is bijective.*

Proof. Let $h \in H$. Then $th \in H$, $h = uth$ for some $u \in S^1$, and $uH \subseteq H$, since $\mathcal{H}$ is a congruence. If $a \in H$, then $a = hv$ for some $v \in S^1$ and $tua = uta = uthv = hv = a$; thus g_t and g_u are mutually inverse bijections of H onto H. □

2. Actual groups arise from $\mathcal{H}$ in two ways. A **subgroup** of a semigroup S is a subsemigroup G of S which happens to be a group. Necessarily the identity element of G is an idempotent of S. Conversely, every idempotent e of S yields a trivial subgroup $\{e\}$ of S. Less trivially:

Proposition 4.3. *For an $\mathcal{H}$-class H of a commutative semigroup S the following conditions are equivalent:*

(1) *$ab \in H$ for some $a, b \in H$;*

(2) *H is a subsemigroup of S;*

(3) *H contains an idempotent;*

(4) *H is a subgroup of S.*

Proof. (1) implies (2) since $\mathcal{H}$ is a congruence: if a, b, and $ab \in H$, then $x, y \in H$ implies $x \mathcal{H} a$, $y \mathcal{H} b$, $xy \mathcal{H} ab$, and $xy \in H$.

Assume that H is a subsemigroup and let $a \in H$. Then $aH \subseteq H$; by Lemma 4.2, $g_a : x \longmapsto ax$ is a permutation of H. In particular $ae = a$ for some $e \in H$. Then $a = ae = aee$ and $e^2 = e$, since g_a is injective. Thus (2) implies (3).

Now assume that H contains an idempotent e. Then $a, b \in H$ implies $a \mathcal{H} e$, $b \mathcal{H} e$, $ab \mathcal{H} ee = e$ since $\mathcal{H}$ is a congruence, and $ab \in H$; thus H is a subsemigroup of S. For every $a \in H$ we have $a = te$ for some $t \in S^1$ and $ae = tee = te = a$. Moreover $aH \subseteq H$, $g_a : x \longmapsto ax$ is a permutation of H by Lemma 4.2, and $ab = e$ for some $b \in H$. Hence H is a group. Thus (3) implies (4); and (4) implies (1). □

If for instance S is a monoid, then the elements of H_1 are the **units** of S and H_1 is the **group of units** of S.

Proposition 4.4. *In a commutative monoid S, $S \backslash H_1$ is an ideal.*

Proof. If $y \in S$ is not a unit, then there cannot exist $u \in S$ such that $uxy = 1$, and xy is not a unit. □

In general:

Corollary 4.5. *The maximal subgroups of a commutative semigroup S coincide with the $\mathcal{H}$-classes of S which contain idempotents. They are pairwise disjoint. Every subgroup of S is contained in exactly one maximal subgroup.*

Proof. If G is a subgroup of S and e is the identity element of G, then every $x \in G$ satisfies $ex = x$ and $xy = e$ for some $y = x^{-1} \in G \subseteq S$; hence $G \subseteq H_e$. □

The history of Corollary 4.5 goes back to Schwarz [1943] for torsion semigroups and to Wallace [1953] and Kimura [1954] for semigroups in general.

3. In fact Lemma 4.2 yields a group for every $\mathcal{H}$-class H. Let

$$\mathrm{St}(H) \;=\; \{t \in S^1 \mid tH \subseteq H\}$$

denote the (left) stabilizer of H. For every $t \in \mathrm{St}(H)$, Lemma 4.2 provides a bijection $g_t : H \longrightarrow H$, $x \longmapsto tx$.

Proposition 4.6. *For every $\mathcal{H}$-class H, $\Gamma(H) = \{g_t \mid t \in \mathrm{St}(H)\}$ is a simply transitive group of permutations of H, and $t \longmapsto g_t$ is a homomorphism of $\mathrm{St}(H)$ onto $\Gamma(H)$. If $H = H_e$ is a maximal subgroup of S, then $\Gamma(H) \cong H$.*

Proof. First $g_t(g_u(x)) = tux = g_{tu}(x)$ for all $t, u \in \mathrm{St}(H)$ and $x \in H$; thus $t \longmapsto g_t$ is a homomorphism and $\Gamma(H)$ is a semigroup (under composition). Also $1 \in \mathrm{St}(H) \subseteq S^1$ and $g_1 = 1_H$ is the identity mapping on H.

Let $g_t \in \Gamma(H)$ and $a \in H$. As in the proof of Lemma 4.2, $a \,\mathcal{H}\, ta$ and $a = uta$ for some $u \in S^1$; in fact $u \in \mathrm{St}(H)$, since $\mathcal{H}$ is a congruence. For every $x \in H$ we now have $x = av$ and $utx = utav = av = x$ for some $v \in S^1$; thus g_t has an inverse in $\Gamma(H)$, namely g_u.

If $a, b \in H$, then $b = ta$ for some $t \in S^1$, $t \in \mathrm{St}(H)$ since $\mathcal{H}$ is a congruence, and $g_t(a) = b$; thus $\Gamma(H)$ is transitive. In fact $\Gamma(H)$ is simply transitive: if $g_t(a) = g_u(a)$, then $ta = ua$, $tx = tav = uav = ux$ for every $x = av \in H$, and $g_t = g_u$.

If finally $H = H_e$ is a maximal subgroup of S, with identity element e, then $H \subseteq \mathrm{St}(H)$ and the homomorphism $h \longmapsto g_h$ of H into $\Gamma(H)$ is bijective, since $g_h(e) = h$ and $\Gamma(H)$ is simply transitive. □

$\Gamma(H)$ is the (left) **Schützenberger group** of H; it was discovered by Schützenberger [1957].

5. FREE COMMUTATIVE SEMIGROUPS.

1. When a commutative semigroup S is generated by a subset X, every element of S is a product of positive powers of one or more distinct elements of X (Proposition 1.3) but can in general be written in this form in several ways. For example $X = S$ generates S, and then every equality $ab = c$ in S equates two distinct products of positive powers of one or more distinct elements of S.

A commutative semigroup S is **free** on a subset X when every element of S can be written uniquely (up to the order of the terms) as a product of positive powers of one or more distinct elements of X. For example, the multiplicative semigroup $\{2,3,\dots,n,\dots\} \subseteq \mathbb{N}$ is free (as a commutative semigroup) on the set of all prime numbers. In the additive notation, powers become positive integer multiples; the additive semigroup $\mathbb{N}^+$ is free on $\{1\}$.

2. For every set X we now construct a commutative semigroup F_X which is free on X.

F_X is one of the few commutative semigroups that we prefer to denote additively. Then products of positive powers of distinct elements of X become sums of positive integer multiples of distinct elements of X, that is, (finite) linear combinations of elements of X with coefficients in $\mathbb{N}^+$. This suggests that we retrieve F_X from the free abelian group G_X on X, which consists of all linear combinations $a = \sum_{x \in X} a_x x$ with integer coefficients $a_x \in \mathbb{Z}$ that are almost all zero (that is, $\{x \in X \mid a_x \neq 0\}$ is finite). (Linear combinations $\sum_{x \in X} a_x x$ can be defined more formally as suitable families $(a_x)_{x \in X}$ of integers.) Addition on G_X is coordinatewise:

$$\textstyle\sum_{x \in X} a_x x \; + \; \sum_{x \in X} b_x x \; = \; \sum_{x \in X} (a_x + b_x) x \, .$$

G_X is a partially ordered group, as the coordinatewise partial order

$$\textstyle\sum_{x \in X} a_x x \leqq \sum_{x \in X} b_x x \text{ if and only if } a_x \leqq b_x \text{ for all } x \in X$$

is compatible with the operation (if $a \leqq b$, then $a + c \leqq b + c$).

F_X is the positive cone of G_X, which is a subsemigroup of G_X:

$$F_X \; = \; \{a \in G_X \mid a > 0\};$$

equivalently, F_X is the set of all linear combinations $a = \sum_{x \in X} a_x x$ with integer coefficients a_x such that $a_x = 0$ for almost all x, $a_x \geqq 0$ for all x, and $a_x > 0$ for some x. Note that $a \leqq_{\mathcal{H}} b$ in F_X if and only if $a \geqq b$ in the coordinatewise partial order.

Every $y \in X$ can be written as a linear combination $y = \sum_{x \in X} a_x x \in F_X$ in which $a_y = 1$ and $a_x = 0$ for all $x \neq y$; thus $X \subseteq F_X$. Now every element of F_X can be written uniquely (up to the order of the terms) as a nonempty sum of positive integer multiples of distinct elements of X; hence

Proposition 5.1. *For every set X, F_X is a commutative semigroup which is free on X.*

Sometimes it is better to denote F_X multiplicatively; then every element of F_X is uniquely (up to the order of the terms) a nonempty product $a = \prod_{x \in X} x^{ax}$ of positive integer powers of distinct elements of X (with $a_x = 0$ for almost all x, $a_x \geqq 0$ for all x, and $a_x > 0$ for some x).

3. The most important property of F_X is its universal property:

Theorem 5.2. *Every mapping f of X into a commutative semigroup S extends uniquely to a homomorphism φ of F_X into S, namely*

$$\varphi(\textstyle\sum_{x \in X} a_x x) \;=\; \prod_{x \in X} f(x)^{ax} \;.$$

The image of φ is the subsemigroup of S generated by $f(X)$. If S is generated by $f(X)$, then φ is surjective. If S is free on X, then S is isomorphic to F_X.

$$\begin{tikzcd}
X \arrow[r, "\subseteq"] \arrow[dr, "f"'] & F_X \arrow[d, "\varphi"] \\
& S
\end{tikzcd}$$

If F_X is denoted multiplicatively, then $\varphi\left(\prod_{x \in X} x^{ax}\right) = \prod_{x \in X} f(x)^{ax}$.

Proof. A homomorphism φ transforms sums into products and transforms linear combinations into products of powers:

$$\varphi(a_1 x_1 + a_2 x_2 + \cdots + a_n x_n) \;=\; \varphi(x_1)^{a_1}\, \varphi(x_2)^{a_2} \,\cdots\, \varphi(x_n)^{a_n} \;.$$

If $\varphi : F_X \longrightarrow S$ extends f (if $\varphi(x) = f(x)$ for all i), then, for every $a = \sum_{x \in X} a_x x \in F_X$,

$$\varphi(\textstyle\sum_{x \in X} a_x x) \;=\; \prod_{x \in X} \varphi(x)^{ax} \;=\; \prod_{x \in X} f(x)^{ax}$$

$(= \prod_{x \in X, a_x \neq 0} f(x)^{ax}$, which is a finite product). Hence φ is unique.

Conversely define a mapping $\varphi : F_X \longrightarrow S$ by

$$\varphi(\textstyle\sum_{x \in X} a_x x) = \prod_{x \in X} f(x)^{a_x} .$$

Then φ extends f and is a homomorphism:

$$\varphi(\textstyle\sum_{x \in X} a_x x + \sum_{x \in X} b_x x) = \prod_{x \in X} f(x)^{a_x + b_x}$$
$$= \textstyle\prod_{x \in X} f(x)^{a_x} f(x)^{b_x} = \left(\prod_{x \in X} f(x)^{a_x}\right)\left(\prod_{x \in X} f(x)^{b_x}\right).$$

By Proposition 1.3,

$$\operatorname{Im} \varphi = \{\textstyle\prod_{x \in X} f(x)^{a_x} \mid a \in F_X\}$$

is the subsemigroup of S generated by $f(X)$. If S is free on X and $f : X \longrightarrow S$ is the inclusion mapping, then φ is an isomorphism. □

It follows from Theorem 5.2 that all commutative semigroups that are generated by a set X are homomorphic images of F_X. Since every semigroup S is generated by some subset $X \subseteq S$ (for instance, by $X = S$), we have:

Corollary 5.3. *Every commutative semigroup is a homomorphic image of a free commutative semigroup. Every finitely generated commutative semigroup is a homomorphic image of a finitely generated free commutative semigroup.*

Commutative semigroups can thus be explored by means of congruences on free commutative semigroups. This approach was pioneered by Rédei [1956] and will be explored in later chapters, and in Proposition 5.8 below.

4. Free commutative semigroups have certain finiteness properties:

Proposition 5.4. *Every free commutative semigroup F satisfies the descending chain condition. If F is finitely generated, then every antichain of F is finite.*

An **antichain** is a subset A which does not contain elements $a < b$.

Proof. By the last part of Theorem 5.2 it suffices to prove these properties for F_X.

When $a = \sum_{x \in X} a_x x \in F$ the positive integer $|a| = \sum_{x \in X} a_x$ is the **length** of a. If $a < b$ in F, then $a_x \leqq b_x$ for all $x \in X$, $a_x < b_x$ for some $x \in X$, and $|a| < |b|$. There cannot exist an infinite descending sequence $a_1 > a_2 > \cdots > a_n > a_{n+1} > \cdots$ of elements of F, for then $|a_1| > |a_2| > \cdots > |a_n| > |a_{n+1}| > \cdots$ would be an infinite descending sequence of positive integers.

Now assume that X is finite. We prove by induction on the number of elements of X that every antichain of F_X is finite. If X is empty, then F_X is empty and so is every antichain of F_X. If X has just one element, then $F_X \cong \mathbb{N}^+$ is a chain and an antichain of F_X has at most one element.

Let X have more than one element and A be an antichain of F_X. For every $y \in X$ and $n \geqq 0$ let $A_{y,n} = \{a \in A \mid a_y = n\}$. Then

$$\{\textstyle\sum_{x \in X \setminus \{y\}} a_x x \mid a \in A_{y,n}\}$$

is an antichain of $F_{X\setminus\{y\}}$ and $A_{y,n}$ is finite by the induction hypothesis.

For every $x \in X$ let $m(x) = \min\,(a_x \mid a \in A)$ and $M_x = \{a \in A \mid a_x = m(x)\}$. By the above, $M = \bigcup_{x \in X} M_x$ is finite. Let $n(x) = \max\,(a_x \mid a \in M)$. Then $n(x) \geqq m(x)$, since $a_x = m(x)$ for some $a \in M$. If $a \in A$, then $a_x \geqq m(x)$ for all $x \in X$ and $a_x \leqq n(x)$ for some $x \in X$, otherwise $a_x > n(x)$ for all $x \in X$, $a > b$ for all $b \in M \subseteq A$, and A is not an antichain. Hence $A \subseteq \bigcup_{x \in X,\, m(x) \leqq n \leqq n(x)} A_{x,n}$ is finite. □

The second half of Proposition 5.4 is known as **Dickson's Theorem**, after Dickson [1913] who proved it for the free multiplicative subsemigroups of $\mathbb{N}$ generated by finitely many primes. A different proof will be given in Chapter VI along with additional finiteness properties.

5. A commutative monoid S is **free** on a subset X (as a monoid) when every element of S can be written uniquely (up to the order of the terms) as a product of positive powers of distinct elements of X (Proposition 1.4).

The nonnegative cone of G_X is

$$F_X \cup \{0\} \;=\; \{a \in G_X \mid a \geqq 0\};$$

equivalently, $F_X \cup \{0\}$ is the set of all linear combinations $a = \sum_{x \in X} a_x x$ with integer coefficients a_x such that $a_x = 0$ for almost all x and $a_x \geqq 0$ for all x. Every element of $F_X \cup \{0\}$ can be written uniquely (up to the order of the terms) as a sum of positive integer multiples of distinct elements of X; hence $F_X \cup \{0\}$ is a free commutative monoid on X. If X is finite, with n elements, then F_X is isomorphic to the direct product $\mathbb{N}^n$. The universal property of $F_X \cup \{0\}$ is:

Proposition 5.5. *Every mapping f of X into a commutative monoid S extends uniquely to a monoid homomorphism φ of $F_X \cup \{0\}$ into S.*

Corollary 5.6. *Every (finitely generated) commutative monoid is a homomorphic image of a (finitely generated) free commutative monoid.*

In later chapters it will be more convenient to denote the free commutative monoid by F_X; then the free commutative semigroup on X is $F_X \backslash \{0\}$.

Similarly we call $F_X \cup \{\infty\}$ the **free** commutative semigroup with zero on the set X, since every element of $F_X \cup \{\infty\}$ is either the zero element ∞ or uniquely a nonempty sum of positive integer multiples of distinct elements of X. Every mapping f of X into a commutative semigroup S with zero extends uniquely to a semigroup homomorphism $\varphi : F_X \cup \{\infty\} \longrightarrow S$ such that $\varphi(\infty) = 0$.

In the multiplicative notation, $F_X \cup \{0\}$ and $F_X \cup \{\infty\}$ become $F_X \cup \{1\}$ and $F_X \cup \{0\}$, respectively.

6. As an application of free commutative semigroups we construct all cyclic semigroups. By Proposition 1.3, a cyclic semigroup S consists of all the powers of its generator x, and is necessarily commutative; hence S is isomorphic to the quotient of $F_{\{x\}}$ by some congruence. Now every element of $F_{\{x\}}$ can be written uniquely in the form nx with $n \in \mathbb{N}^+$; hence $F_{\{x\}} \cong \mathbb{N}^+$. Thus a cyclic semigroup is isomorphic to the quotient of $\mathbb{N}^+$ by some congruence.

Let $\mathcal{C}$ be a congruence on $\mathbb{N}^+$. If $\mathcal{C}$ is not the equality on $\mathbb{N}^+$, the least integer $r > 0$ such that $r \; \mathcal{C} \; t$ for some $t \neq r$ is the **index** of $\mathcal{C}$. Then the least integer $s > 0$ such that $r \; \mathcal{C} \; r + s$ is the **period** of $\mathcal{C}$.

Lemma 5.7. *When $\mathcal{C}$ is a congruence on $\mathbb{N}^+$ of index r and period s, then $a \; \mathcal{C} \; b$ if and only if either $a = b < r$, or $a, b \geqq r$ and $a \equiv b \bmod s$.*

Proof. Since $\mathcal{C}$ is a congruence, $r \; \mathcal{C} \; r + s$ implies $r \; \mathcal{C} \; r + s \; \mathcal{C} \; r + 2s \; \mathcal{C} \; \dots \; \mathcal{C} \; r + ks$ for all $k > 0$, $u + r \; \mathcal{C} \; u + r + ks$ for all $k > 0$, $u \geqq 0$, and $a \; \mathcal{C} \; b$ whenever $r \leqq a \leqq b$ and $a \equiv b \bmod s$.

Conversely assume $a \; \mathcal{C} \; b$ with $a < b$. Then $a \geqq r$ by the choice of r. There is an integer $u \geqq 0$ such that $u + a \equiv r \bmod s$, and an integer $k \geqq 0$ such that $a + ks < b \leqq a + ks + s$. Then $t = b - a - ks$ satisfies $0 < t \leqq s$ and $a + ks \; \mathcal{C} \; a \; \mathcal{C} \; b = a + ks + t$; hence

$$r \; \mathcal{C} \; u + a \; \mathcal{C} \; u + a + ks \; \mathcal{C} \; u + a + ks + t \; \mathcal{C} \; r + t.$$

Since $0 < t \leqq s$ it follows from the choice of s that $t = s$. Then $b = a + ks + s \equiv a \bmod s$. □

Proposition 5.8. *Let S be a cyclic semigroup, generated by $x \in S$. Either $S \cong \mathbb{N}^+$, or S is finite and there exist integers $r, s > 0$ (the* **index** *and* **period** *of x) such that $x^i = x^j$ if and only if either $i = j < r$, or $i, j \geqq r$ and $i \equiv j \bmod s$; then every element of S can be written uniquely in the form x^i with $1 \leqq i < r + s$ and*

$$x^i x^j = \begin{cases} x^{i+j} & \text{if } i+j < r+s, \\ x^k & \text{if } i+j \geqq r+s, \text{ where} \\ & \quad r \leqq k < r+s \text{ and } k \equiv i+j \bmod s; \end{cases}$$

and $\{x^r, x^{r+1}, \ldots, x^{r+s-1}\}$ *is a cyclic subgroup of* S.

Proof. We have $S \cong \mathbb{N}^+/\mathcal{C}$ for some congruence $\mathcal{C}$ on $\mathbb{N}^+$. If $\mathcal{C}$ is the equality, then $S \cong \mathbb{N}^+$. Now assume that $\mathcal{C}$ is not the equality. As before, $\mathcal{C}$ has index $r > 0$ and period $s > 0$. By Lemma 5.7, the $\mathcal{C}$-class of $a < r$ is $\{a\}$; the $\mathcal{C}$-classes of $r, r+1, \ldots, r+s-1$ are distinct (and infinite); and these are all the $\mathcal{C}$-classes. Since $a \equiv b \bmod s$ implies $a \;\mathcal{C}\; b$ when $a, b \geqq r$ the operation on S is as described in the statement.

Finally, $G = \{x^r, x^{r+1}, \ldots, x^{r+s-1}\}$ is a subsemigroup of S and we see from the multiplication on S that $G \cong \mathbb{Z}/s\mathbb{Z}$, the additive group of integers modulo s. □

Proposition 5.8 was first stated (for cyclic semigroups of subsets of a group) by Frobenius [1895], and its Corollary 5.9 below, in its present form, by Moore [1902]. Lemma 5.7 was rediscovered by Chacron [1982]. Tamura [1963] determined all congruences on $\mathbb{Q}^+$.

Corollary 5.9. *Every nonempty finite semigroup contains an idempotent.*

Proof. If S is finite nonempty, then S contains a finite cyclic subsemigroup, which by Proposition 5.8 contains a subgroup and its identity element. □

6. PRESENTATIONS.

Corollary 5.4 suggests that commutative semigroups can be constructed by presentations (= by generators and relations).

1. For this it is more convenient to denote free commutative semigroups multiplicatively. Formally, a commutative semigroup **relation** between elements of a set X is an ordered pair (u, v), normally written as an equality $u = v$, of elements of F_X. (Relations are readily distinguished from actual equalities in F_X, since the latter are all trivial.)

When f is a mapping of X into a commutative semigroup S, we say that the relation $u = v$ **holds in** S **via** f in case the equality $\varphi(u) = \varphi(v)$ holds in S, where $\varphi : F_X \longrightarrow S$ is the homomorphism which extends f.

These somewhat abstract definitions make most sense when X is a subset of S and $f : X \longrightarrow S$ is the inclusion mapping; then φ sends a product $\prod_{x \in X} x^{a_x}$ of elements of X as calculated in F_X to the same product $\prod_{x \in X} x^{a_x}$ calculated in S; hence the relation $\prod_{x \in X} x^{u_x} = \prod_{x \in X} x^{v_x}$ holds in S if and only if the products $\prod_{x \in X} x^{u_x} = \prod_{x \in X} x^{v_x}$ are equal in S.

2. When X is a set and $\mathcal{R} \subseteq F_X \times F_X$ is a set of relations between the elements of X, we denote by $\langle X \,|\, \mathcal{R} \rangle$ the quotient of the free commutative semigroup F_X by the congruence $\mathcal{C}$ generated by $\mathcal{R}$. By Proposition 2.9, $\mathcal{C}$ consists of all the "obvious consequences" of the relations in $\mathcal{R}$.

$\langle X \,|\, \mathcal{R} \rangle$ comes with a canonical mapping $\iota : X \longrightarrow \langle X \,|\, \mathcal{R} \rangle$ which is the composition

$$\iota : \; X \xrightarrow{\subseteq} F_X \longrightarrow F_X/\mathcal{C} = \langle X \,|\, \mathcal{R} \rangle .$$

Proposition 6.1. *$\langle X \,|\, \mathcal{R} \rangle$ is generated by $\iota(X)$ and every relation $(u,v) \in \mathcal{R}$ holds in $\langle X \,|\, \mathcal{R} \rangle$ via ι.*

Proof. $\langle X \,|\, \mathcal{R} \rangle$ is generated by $\iota(X)$, since F_X is generated by X. Moreover the projection $F_X \longrightarrow F_X/\mathcal{C} = \langle X \,|\, \mathcal{R} \rangle$ is the only homomorphism which extends ι; since $\mathcal{R} \subseteq \mathcal{C}$, every relation $(u,v) \in \mathcal{R}$ holds in $\langle X \,|\, \mathcal{R} \rangle$ via ι. □

Accordingly $\langle X \,|\, \mathcal{R} \rangle$ is known as the commutative semigroup **generated by X subject to $\mathcal{R}$**. This is somewhat misleading since X is not a subset of $\langle X \,|\, \mathcal{R} \rangle$ (in fact, ι need not even be injective) and every homomorphic image of $\langle X \,|\, \mathcal{R} \rangle$ has the properties in Proposition 6.1. However, $\langle X \,|\, \mathcal{R} \rangle$ is the "largest" semigroup with these properties:

Proposition 6.2. *Let X be a set and $\mathcal{R}$ be a set of relations between the elements of X. Let S be a commutative semigroup and $f : X \longrightarrow S$ be a mapping such that every relation $u = v$ in $\mathcal{R}$ holds in S via f. There is a unique homomorphism $\varphi : \langle X \,|\, \mathcal{R} \rangle \longrightarrow S$ such that $f = \varphi \circ \iota$. If S is generated by $f(X)$, then φ is surjective.*

$$\begin{tikzcd}
X \arrow[r, "\iota"] \arrow[dr, "f"'] & \langle X \,|\, \mathcal{R} \rangle \arrow[d, "\varphi"] \\
& S
\end{tikzcd}$$

Proof. Let $\mathcal{C}$ be the congruence on F_X generated by $\mathcal{R}$ and $\pi : F_X \longrightarrow F_X/\mathcal{C} = \langle X \,|\, \mathcal{R} \rangle$ be the projection. Let $\psi : F_X \longrightarrow S$ be the homomorphism which extends f. Then $\psi(u) = \psi(v)$ for every relation $u = v$ in $\mathcal{R}$, since $u = v$ holds in S via f; hence $\mathcal{R} \subseteq \ker \psi$ and $\mathcal{C} \subseteq \ker \psi$. By Proposition 2.4, ψ factors through π: $\psi = \varphi \circ \pi$ for some homomorphism $\varphi : \langle X \,|\, \mathcal{R} \rangle \longrightarrow S$.

Then $\varphi \circ \iota = f$.

$$\begin{tikzcd}
X \arrow[r, "\subseteq"] \arrow[dr, "f"'] & F_X \arrow[r, "\pi"] \arrow[d, "\psi"] & \langle X \,|\, \mathcal{R} \rangle \arrow[dl, "\varphi"] \\
& S &
\end{tikzcd}$$

Let $\varphi' : \langle X \,|\, \mathcal{R} \rangle \longrightarrow S$ be another homomorphism such that $\varphi' \circ \iota = f$. Then $T = \{ a \in \langle X \,|\, \mathcal{R} \rangle \mid \varphi(a) = \varphi'(a) \}$ is a subsemigroup of $\langle X \,|\, \mathcal{R} \rangle$ which contains $\iota(X)$; since $\iota(X)$ generates $\langle X \,|\, \mathcal{R} \rangle$ it follows that $\varphi = \varphi'$. □

3. A **presentation** of a commutative semigroup S consists of a set X, a set $\mathcal{R}$ of commutative semigroup relations between the elements of X, and an isomorphism $S \cong \langle X \,|\, \mathcal{R} \rangle$. By Corollary 5.4, every commutative semigroup S has a presentation, in which X can be any subset of S which generates S, and $\mathcal{R}$ can be any binary relation which generates the congruence induced by $F_X \longrightarrow S$.

For example let $\mathcal{C}$ be the congruence on $\mathbb{N}^+$ of index r and period s. By Lemma 5.7, $\mathcal{C}$ is generated by $(r, r+s)$. Therefore a finite cyclic semigroup S of index r and period s has the presentation $S \cong \langle\, x \mid x^r = x^{r+s} \,\rangle$.

Presentations are associated with a number of logical and computational problems: the **word problem** (deciding when two products of generators are equal); the **isomorphism problem** (deciding when two presentations yield isomorphic semigroups); and recognition problems (recognizing additional properties from a presentation). Algorithms in Rosales & García-Sánchez [1999] solve a number of these problems.

4. Similar definitions apply to commutative monoids and to commutative semigroups with zero. A commutative monoid relation between the elements of a set X is an ordered pair (u, v) (normally written as an equality $u = v$) of elements of the free commutative monoid $F_X \cup \{1\}$ (written multiplicatively); the identity element of $F_X \cup \{1\}$ may appear as u or v. When S is a commutative monoid, a commutative monoid presentation of S consists of a set X, a set $\mathcal{R}$ of commutative monoid relations between the elements of X, and an isomorphism $S \cong \langle X \,|\, \mathcal{R} \rangle$, where $\langle X \,|\, \mathcal{R} \rangle$ now denotes the quotient of $F_X \cup \{1\}$ by the congruence generated by $\mathcal{R}$.

A commutative relation with zero between the elements of a set X is an ordered pair (u, v) (normally written as an equality $u = v$) of elements of the free commutative semigroup with zero $F_X \cup \{0\}$ (written multiplicatively); the zero element of $F_X \cup \{0\}$ may appear as u or v. When S is a commutative semigroup with zero, a presentation of S as a commutative semigroup with zero consists of a set X, a set $\mathcal{R}$ of commutative relations with zero between the elements of X, and an isomorphism $S \cong \langle X \mid \mathcal{R} \rangle$, where $\langle X \mid \mathcal{R} \rangle$ now denotes the quotient of $F_X \cup \{0\}$ by the congruence generated by $\mathcal{R}$.