Notes on Semigroups and Related Structures

Bilal Ahmad Kalas

Contents

Part I.

Core Foundations

1. Elemantary Concepts

1.1. Sets and Relations

1.1.1. Relations

Definition 1.1.1 (Binary relation). Let X be a set. Every subset ρ of the Cartesian product $X \times X$ is called a *(binary) relation* on X. If $(x, y) \in \rho$, we also write $x\rho y$, where $x, y \in X$.

Definition 1.1.2 (Domain and range). For a relation $\rho \subseteq X \times X$, the *domain* and *range* of R are defined by

$$\operatorname{dom} \rho = \{x \in X \,:\, \exists\, y \in X \text{ with } (x, y) \in R\},$$

and

$$\operatorname{ran} \rho = \{y \in X \,:\, \exists\, x \in X \text{ with } (x, y) \in R\}.$$

The word *image* is also used sometimes as a synonym of range.

Notation 1.1.3. The set of all binary relations on X is denoted by $\mathfrak{B}(X)$.

Remark 1.1.4. If $\rho, \tau \in \mathfrak{B}(X)$, then $\rho \subseteq \tau$ means that $x\rho y \Rightarrow x\tau y$ for all $x, y \in X$. We shall often write $\rho \leq \tau$ for $\rho \subseteq \tau$.

Definition 1.1.5 (Complement). The complement of a relation $\rho \in B(X)$ is the relation $\overline{\rho} \in B(X)$ defined by

$$(x, y) \in \overline{\rho} \iff (x, y) \notin \rho.$$

Definition 1.1.6 (Properties of a relation). A relation $\rho \in (X)$ is called

1. *reflexive*, if $x\rho x$ for all $x \in X$;
2. *symmetric*, if $x\rho y$ implies yRx;
3. *antisymmetric*, if $x\rho y$ and $y\rho x$ together imply $x = y$;
4. *transitive*, if $x\rho y$ and $y\rho z$ imply $x\rho z$;
5. *right unique*, if ρy and $x\rho z$ imply $y = z$;
6. *left unique*, if $x\rho y$ and $z\rho y$ imply $x = z$;
7. *right total*, if for every $y \in X$ there exists $x \in X$ such that $x\rho y$;
8. *left total*, if for every $x \in X$ there exists $y \in X$ such that $x\rho y$.

The last four notions also apply to relations $\rho \subseteq X \times Y$ for two possibly different sets X and Y.

1.1.2. Mappings

Definition 1.1.7 (Mapping). Let X and Y be sets. A mapping $\varphi : X \to Y$ is a relation $\varphi \subseteq X \times Y$ which is right unique and left total; that is, for every $x \in X$ there exists exactly one $y \in Y$ such that $(x, y) \in \varphi$.

Remark 1.1.8. As usual, we write $\varphi(x) = y$. Sometimes we also write $x\varphi = y$. The set of all mappings from X to Y is denoted by $\mathrm{Map}(X, Y)$ or Y^X. We also use $\mathcal{T}(X)$ for $\mathrm{Map}(X, X)$. The elements of $\mathcal{T}(X)$ are called *transformations* of X.

Definition 1.1.9 (Injective, surjective, bijective). A mapping $\varphi : X \to Y$ is called

1. *injective*, if $\varphi(x) = \varphi(x') \Rightarrow x = x'$ for all $x, x' \in X$;
2. *surjective*, if for every $y \in Y$ there exists $x \in X$ such that $\varphi(x) = y$;
3. *bijective*, if it is both injective and surjective.

Equivalently, injectivity means that the relation is left unique, and surjectivity means that the relation is right total.

Remark 1.1.10. The subset of all bijective transformations in $\mathcal{T}(X)$ is denoted by $\mathcal{S}(X)$, and its elements are called permutations or bijections of X.

Definition 1.1.11 (Identity map). The identity map $\mathrm{id}_X : X \to X$ is defined by

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

Definition 1.1.12 (Constant mapping). For $y \in Y$, the constant mapping $c_y : X \to Y$ is defined by

$$c_y(x) = y \qquad \forall\, x \in X.$$

Definition 1.1.13 (Restriction). If $\varphi : X \to Y$ is a mapping and $A \subseteq X$, then the restriction of φ to A is defined by $\varphi|_A : A \to Y$ such that

$$\varphi|_A(a) = \varphi(a) \qquad \forall\, a \in A.$$

Conversely, we say that φ extends $\varphi|_A$.

Definition 1.1.14 (Partial mapping). A partial mapping $\varphi : X \to Y$ is defined to be a right unique relation; that is, $\varphi : \operatorname{dom}\varphi \to Y$ is a mapping, where $\operatorname{dom}\varphi \subseteq X$. The set $\operatorname{dom}\varphi$ is called the domain of φ. The set of all partial mappings on X (from X to X) is denoted by $\mathcal{PT}(X)$.

Remark 1.1.15. The mapping $\varphi : \operatorname{dom}\varphi \to \operatorname{im}\varphi$ with $\operatorname{dom}\varphi = \operatorname{im}\varphi = \emptyset$ is called the empty mapping.

1.1.3. Order Relations

Definition 1.1.16 (Partial order). A reflexive, antisymmetric, and transitive relation α on a set X is called a *partial ordering* on X, or simply an ordering of X. One writes $x \leq y$ for $(x, y) \in \alpha$, and the pair $(X, \leq)$ is called a *partially ordered set* or a *poset.*

Definition 1.1.17 (Total order). If in addition, a partial ordering has the property that for every $x, y \in X$, either $x \leq y$ or $y \leq x$. In this case, $\leq$ is called a *total order*. Then $(X, \leq)$ is also called a *linearly ordered set* or a *chain*.

Definition 1.1.18 (Maximal and minimal elements). Let X be a poset. An element $w \in X$ is called a *maximal* (respectively, *minimal*) element of $(X, \leq)$ if $w \leq u$ (respectively, $u \leq w$) implies $u = w$ for every $u \in X$.

Definition 1.1.19 (Minimal condition and well-ordering). A poset $(X, \leq)$ satisfies the *minimal condition* if every non-empty subset of X has a minimal element. In that case, we also say that $(X, \leq)$ is *well ordered*.

Definition 1.1.20 (Lower bound and meet). Let Y be a non-empty subset of a poset X. An element $c \in X$ is called a *lower bound* for Y if $c \leq y$ for all $y \in Y$. An element $u \in X$ is called the *greatest lower bound* or *meet* of Y if u is a lower bound for Y and $z \leq u$ for every lower bound z of Y. The greatest lower bound of Y is denoted by $\bigwedge y \,:\, y \in Y$. If $Y = \{a, b\}$, we also write $a \wedge b$.

Definition 1.1.21 (Lower semilattice). If $(X, \leq)$ is such that $a \wedge b$ exists for every pair $a, b \in X$, then $(X, \leq)$ is called a *lower semilattice*. If, in addition, $\bigwedge\{y \,:\, y \in Y\}$ exists for every non-empty subset $Y \subseteq X$, then $(X, \leq)$ is called a *complete lower semilattice*.

Definition 1.1.22 (Upper bound and join). Similarly, for a non-empty subset $Y \subseteq X$, an element $c \in X$ is called an *upper bound* for Y if $y \leq c$ for all $y \in Y$. An element $v \in X$ is called the *least upper bound* or *join* of Y if v is an upper bound for Y and $v \leq z$ for every upper bound z of Y. The least upper bound of Y is denoted by $\bigvee\{y \,:\, y \in Y\}$. If $Y = \{a, b\}$, we also write $a \vee b$.

Definition 1.1.23 (Upper semilattice). If $(X, \leq)$ is such that $a \vee b$ exists for every pair $a, b \in X$, then $(X, \leq)$ is called an *upper semilattice*. If, in addition, $\bigvee y \,:\, y \in Y$ exists for every non-empty subset $Y \subseteq X$, then $(X, \leq)$ is called a *complete upper semilattice*.

Definition 1.1.24 (Lattice). If a poset is both a (complete) lower semilattice and a (complete) upper semilattice then it is called a (complete) lattice. In this case we use the notation $(X, \leq, \wedge, \vee)$.

Remark 1.1.25. The set $\mathfrak{B}(X)$ of all binary relations on a set X is a poset under inclusion; that is, $\rho \leq \tau$ if and only if $\rho \subseteq \tau$, for $\rho, \tau \in \mathfrak{B}(X)$. Moreover, it is a lattice with

$$\rho \wedge \tau = \rho \cap \tau \quad \text{and} \quad \rho \vee \tau = \rho \cup \tau,$$

which is called the lattice of relations on X and is denoted by $(\mathfrak{B}(X), \leq, \wedge, \vee)$.

Lemma 1.1.1 (Zorn's lemma). *If $(X, \leq)$ is a non-empty poset such that every chain of elements has an upper bound in X, then X has at least one maximal element.*

Theorem 1.1.2 (Zermelo's theorem on well-ordering). *Every non-empty set can be well ordered.*

1.1.4. Equivalence relations and partitions

Definition 1.1.26. An *equivalence* or *equivalence relation* on X is a reflexive, symmetric and transitive relation on X.
Special equivalence relations on X are $\mathrm{id}_X = \{(x, x) \mid x \in X\}$, the *diagonal relation* on X, also denoted by Δ_X, and the *total relation* $X \times X$, also denoted by ∇_X.

Definition 1.1.27. Let $K \subseteq X$ be a subset. Define the *Rees equivalence* ρ_K by setting

$$x \, \rho_K \, x' \iff x, x' \in K \text{ or } x = x'.$$

We denote the set of all equivalences on a set X by $\mathscr{E}(X)$. As a subset of $\mathfrak{B}(X)$ it is partially ordered by inclusion.
We call the intersection of all equivalences containing the relation $\rho \in B(X)$ the *equivalence on X generated by ρ* or the *equivalence closure* of ρ, and denote it by ρ^e.
If $\{\rho_i \in \mathscr{E}(X) \mid i \in I\}$ is a non-empty set of equivalences on X, then $\bigcap_{i\in I} \rho_i$ is again an equivalence on X.
If $\rho \in B(X)$, then the intersection of all equivalences containing ρ is the unique minimal equivalence on X containing ρ.
In fact $\mathscr{E}(X)$ is a lattice. If $\rho, \sigma \in \mathscr{E}(X)$, then their greatest lower bound $\rho \wedge \sigma$ is $\rho \cap \sigma$ and their least upper bound $\rho \vee \sigma$ is $(\rho \cup \sigma)^e$.

Definition 1.1.28. For $\rho \in \mathscr{E}(X)$ and $A \subseteq X$, set

$$\rho(A) := \{\, b \in X \mid \text{there exists } a \in A \text{ with } (a, b) \in \rho \,\}.$$

For $A = \{a\}$ we write instead of $\rho(a)$ also $[a]_\rho$ or just $[a]$, and call this set the ρ-class of a or the class of a (with respect to ρ).

Let $\rho, \sigma \in \mathscr{E}(X)$. Then $\rho \subseteq \sigma$ if and only if every σ-class is a union of ρ-classes.

Definition 1.1.29. A family of subsets X_i, $i \in I$, of a set X is called a *partition* of X if the subsets X_i are pairwise disjoint, non-empty, and their union is X.

If ρ is an equivalence relation on X, then the set of equivalence classes

$$\pi(\rho) = \{[x]_\rho \mid x \in X\}$$

is the partition of X corresponding to ρ.
On the other hand, if $\pi = \{X_i \mid i \in I\}$ is a partition of X into subsets X_i, then the relation

$$\rho(\pi) = \{(x, y) \in X \times X \mid \text{there exists } i \in I \text{ such that } x, y \in X_i\}$$

is an equivalence relation on X. Note that

$$\rho(\pi(\rho)) = \rho, \qquad \pi(\rho(\pi)) = \pi.$$

The set of classes of an equivalence relation ρ on a set X is denoted by X/ρ, that is, $X/\rho = \{[x]_\rho \mid x \in x\}$ and is called the *quotient (or factor) set* of X by ρ, and there exists a natural map $\rho^\natural : X \to X/\rho$ (read rho natural) such that $x\rho^\natural = [x]_\rho$.

For any $\rho \in \mathfrak{B}(X)$, let

$$\rho^R = \bigcap\{\sigma \in B(X) \mid \rho \subseteq \sigma,\ \sigma \text{ is reflexive}\},$$
$$\rho^S = \bigcap\{\sigma \in B(X) \mid \rho \subseteq \sigma,\ \sigma \text{ is symmetric}\}.$$

There is at least one element $\sigma \in \mathfrak{B}(X)$ satisfying the condition in each of the collections above, namely $\sigma = X \times X$. Furthermore, since every such σ contains ρ, the intersections ρ^R and ρ^S are both 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.

1.1.5. Inverse relation, restriction and composition

Let $\rho \subseteq X \times Y$. The *inverse* (*converse*) relation to ρ is

$$\rho^{-1} = \{(y, x) \in Y \times X \mid (x, y) \in \rho\}.$$

Similar as for mappings, we now define the *restriction* $\rho|_{X'}$ of a relation $\rho \in B(X)$ for a subset $X' \subseteq X$ by

$$\rho|_{X'} = \rho \cap (X' \times X').$$

The *composition* of relations $\rho, \sigma \in \mathfrak{B}(X)$ is defined as

$$\rho \circ_r \sigma = \{(x, z) \in X \times X \mid \text{there exists } y \in X \text{ with } x\sigma y \text{ and } y\rho z\},$$

if we start with the right relation σ, and analogously for $\rho \subseteq X \times Y$, $\sigma \subseteq Y \times Z$ as

$$\rho \circ_r \sigma = \{(x, z) \in X \times Z \mid \text{there exists } y \in Y \text{ with } x\sigma y \text{ and } y\rho z\}.$$

If we start with the left relation ρ, we define

$$\rho \circ_l \sigma = \{(x, z) \in X \times X \mid \text{there exists } y \in X \text{ with } x\rho y \text{ and } y\sigma z\},$$

for $\rho, \sigma \in B(X)$, and analogously for $\rho \subseteq X \times Y$, $\sigma \subseteq Y \times Z$ as

$$\rho \circ_l \sigma = \{(x, z) \in X \times Z \mid \text{there exists } y \in Y \text{ with } x\rho y \text{ and } y\sigma z\}.$$

Usually, for convenience, we will denote either $\circ_r$ or $\circ_l$ by $\circ$. We will be careful in any situation to indicate the use of either convention.
If $\varphi \in \mathrm{Map}(X, Y)$ and $\psi \in \mathrm{Map}(Y, Z)$, then in the case when mapping symbols are written to the left of the elements on which they act, by $\psi\varphi$ we mean $\psi \circ_r \varphi$, i.e.

$$(\psi\varphi)(x) = \psi(\varphi(x)) \qquad \forall\, x \in X.$$

In the case when mapping symbols are written to the right of the elements on which they act, by $x\varphi\psi$ we mean $\varphi \circ_l \psi$, i.e.

$$(x\varphi)\psi = (x\varphi)\psi \qquad \forall\, x \in X.$$

1.1.6. Transitive and equivalence closure

It is clear that the operation $\circ$ on $\mathfrak{B}(X)$ is associative and thus $(\mathfrak{B}(X), \circ)$ will be one of the examples of monoids (definition in a further section) with the identity element id_X. Sometimes we write $\rho\sigma$ for $\rho \circ \sigma$. We define powers of a relation $\rho \in \mathfrak{B}(X)$ as follows:

$$\rho^0 = id_X, \qquad \rho^i = \rho \circ \rho \circ \cdots \circ \rho,\ i \text{ times}, \quad i \in \mathbb{N}.$$

Definition 1.1.30. The *transitive closure* of a relation $\rho \in \mathfrak{B}(X)$ is the relation

$$\rho^{\infty} = \bigcup_{n=1}^{\infty} \rho^n \in \mathfrak{B}(X).$$

Lemma 1.1.3. *If $\rho \in B(X)$, then ρ^{∞} is the smallest transitive relation in $(B(X), \leq)$ containing ρ.*

Proof. If $(x, y), (y, z) \in \rho^{\infty}$, then there exist $m, n \in \mathbb{N}$ such that $(x, y) \in \rho^m$, $(y, z) \in \rho^n$, and

$$(x, z) \in \rho^m \circ \rho^n = \rho^{m+n} \subseteq \rho^{\infty}.$$

Thus ρ^{∞} is a transitive relation and $\rho \subseteq \rho^{\infty}$. If now σ is a transitive relation on X and $\rho \subseteq \sigma$, then

$$\rho^2 = \rho \circ \rho \subseteq \sigma \circ \sigma \subseteq \sigma.$$

By induction it follows easily that $\rho^n \subseteq \sigma$ for all $n \in \mathbb{N}$, i.e. $\rho^{\infty} \subseteq \sigma$. □

Theorem 1.1.4. *If $\rho \in \mathfrak{B}(X)$, then for the equivalence closure ρ^e we get*

$$\rho^e = (\rho \cup \rho^{-1} \cup id_X)^{\infty}.$$

Proof. It is clear that $\tau = (\rho \cup \rho^{-1} \cup id_X)^{\infty}$ contains ρ and is transitive and reflexive. The relation $\nu = \rho \cup \rho^{-1} \cup id_X$ is symmetric and therefore $\nu^n = (\nu^{-1})^n = (\nu^n)^{-1}$. Thus, if $(x, y) \in \tau$, then $(x, y) \in \nu^n$ for some $n \in \mathbb{N}$ and therefore $(y, x) \in \nu^n$. Thus $(y, x) \in \tau$, i.e. τ is symmetric. This means that $\tau \in \mathscr{E}(X)$.
If $\sigma \in \mathscr{E}(X)$ and $\rho \subseteq \sigma$, then $id_X \subseteq \sigma$, $\rho^{-1} \subseteq \sigma^{-1} = \sigma$, and therefore $\nu = \rho \cup \rho^{-1} \cup id_X \subseteq \sigma$. Since $\nu \circ \nu \subseteq \sigma \circ \sigma \subseteq \sigma$, we get $\nu^n \subseteq \sigma$ for all $n \in \mathbb{N}$, and hence $\tau \subseteq \sigma$. □

Corollary 1.1.5. *If $\rho \in \mathfrak{B}(X)$, then $(x, y) \in \rho^e$ if and only if $x = y$ or for some $n \in \mathbb{N}$ there exists a sequence of elements $x_0, x_1, x_2, \dots, x_n$ in X such that $x_0 = x$, $x_n = y$, and for every $i \in \{1, \dots, n\}$ either $(x_{i-1}, x_i) \in \rho$ or $(x_i, x_{i-1}) \in \rho$.*
In particular, if ρ and σ are equivalence relations on a set X, then in $\mathscr{E}(X)$ their join $\rho \vee \sigma$ is the relation defined by

$$x(\rho \vee \sigma)y \iff \textit{there exist } x_0, x_1, \dots, x_n \in X \textit{ such that } x = x_0,\ y = x_n$$

and

$$(x_{i-1}, x_i) \in \tau_i, \qquad \tau_i \in \{\rho, \sigma\},\ i \in \{1, \dots, n\}.$$

Proposition 1.1.6. *For any $\rho \in \mathfrak{B}(X)$,*

1. $\rho^R = \rho \cup id_X$;
2. $\rho^S = \rho \cup \rho^{-1}$;
3. $(\rho^R)^S = (\rho^S)^R = \rho \cup \rho^{-1} \cup id_X$;
4. $\rho^e = \left(\left(\rho^R\right)^S\right)^{\infty}$.

1.1.7. Kernel equivalence and Homomorphism Theorem for sets

Definition 1.1.31. Let $\varphi : X \to Y$ be a mapping. The relation

$$\ker \varphi = \{(x, x') \in X \times X \mid \varphi(x) = \varphi(x')\}$$

is an equivalence on X which is called the *kernel equivalence* or the *kernel* of φ.
It follows from the definition of the composition of relations that

$$\ker \varphi = \varphi^{-1} \circ \varphi = \varphi^{-1} \circ_r \varphi.$$

Theorem 1.1.7 (Homomorphism Theorem for sets). *Let $\varphi : X \to Y$ be a mapping and let ρ be an equivalence on X such that $x\rho x'$ implies $\varphi(x) = \varphi(x')$, i.e. $\rho \leq \ker \varphi$. Then $\varphi' : X/\rho \to Y$, with $\varphi'([x]_\rho) := \varphi(x)$, $x \in X$, is the unique mapping such that the following diagram is commutative:*

$$\begin{tikzcd} X \arrow[r, "\varphi"] \arrow[d, "\pi_\rho"'] & Y \\ X/\rho \arrow[ur, "\varphi'"'] & \end{tikzcd}$$

i.e. such that $\varphi'\pi_\rho = \varphi$, where π_ρ denotes the canonical surjection.
If $\rho = \ker \varphi$, then φ' is injective, and if φ is surjective, then φ' is surjective.

Proof. Define $\varphi' : X/\rho \to Y$ by $\varphi'([x]_\rho) = \varphi(x)$ for any $x \in X$. Suppose $[x]_\rho = [x']_\rho$ for $x, x' \in X$. Then $(x, x') \in \rho$ and thus $\varphi(x) = \varphi(x')$. Hence φ' is well-defined.
Suppose $\varphi'([x]_\rho) = \varphi'([x']_\rho)$. Then $\varphi(x) = \varphi(x')$ and thus $(x, x') \in \ker \varphi$.
If $\rho = \ker \varphi$, then $[x]_\rho = [x']_\rho$ and thus φ' is injective. □

1.1.8. Congruences

Definition 1.1.32. A relation ρ on X is called

- *left compatible* if for all $x, y, z \in X$,

$$(x, y) \in \rho \implies (zx, zy) \in \rho;$$

- *right compatible* if for all $x, y, z \in X$,

$$(x, y) \in \rho \implies (xz, yz) \in \rho;$$

- *compatible* if for all $x, y, s, t \in X$,

$$(x, y) \in \rho \text{ and } (s, t) \in \rho \implies (xs, yt) \in \rho.$$

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

Proposition 1.1.8. *A relation ρ on X is a congruence if and only if it is both a left and a right congruence.*

Proof. Suppose ρ is both a left and a right congruence. Let $x, y, z, t \in X$ be such that $(x, y) \in \rho$ and $(z, t) \in \rho$. Since ρ is a right congruence, $(xz, yz) \in \rho$, and since ρ is a left congruence, $(yz, yt) \in \rho$. By transitivity of ρ, it follows that $(xz, yt) \in \rho$. Hence ρ is a congruence.
Conversely, suppose ρ is a congruence. Let $x, y \in X$ be such that $(x, y) \in \rho$, and let $z \in X$. Since ρ is reflexive, $(z, z) \in \rho$. By compatibility, $(zx, zy) \in \rho$. Thus ρ is left compatible. Similarly, $(xz, yz) \in \rho$, so ρ is right compatible. Hence ρ is both a left and a right congruence. □

For any $\rho \in \mathfrak{B}(X)$, let

$$\rho^c = \bigcap\{\sigma \in \mathfrak{B}(X) \mid \rho \subseteq \sigma,\ \sigma \text{ is left and right compatible}\}.$$

Then ρ^c is the smallest left and right compatible relation containing ρ. Also, let

$$\rho\# = \bigcap\{\sigma \in \mathfrak{B}(X) \mid \rho \subseteq \sigma,\ \sigma \text{ is a congruence}\}.$$

Then ρ^c, called the congruence generated by ρ, is the smallest congruence containing ρ.

Proposition 1.1.9. *For any $\rho, \sigma \in \mathfrak{B}(X)$,*

1. $(\rho \cup \sigma)^c = \rho^c \cup \sigma^c$;
2. $(\rho^{-1})^c = (\rho^c)^{-1}$.

Proposition 1.1.10. *For any $\rho \in \mathfrak{B}(X)$, we have*

$$\rho^\# = (\rho^c)^e.$$

Proof. By definition, $(\rho^c)^e$ is an equivalence relation containing ρ^c, and hence containing ρ. Notice that

$$\begin{aligned}(\rho^c)^e &= (\rho^c \cup (\rho^c)^{-1} \cup id_X)^\infty \\ &= ((\rho \cup \rho^{-1} \cup id_X)^c)^\infty \\ &= \cup_{n=0}^{\infty}((\rho \cup \rho^{-1} \cup id_X)^c)^n\end{aligned}$$

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

$$\begin{aligned}&(x, y) \in (\rho^c)^e \\ \Longrightarrow\ &(x, y) \in \cup_{n=0}^{\infty}((\rho \cup \rho^{-1} \cup id_X)^c)^n \\ \Longrightarrow\ &\exists\ n \in \mathbb{N} \text{ such that } (x, y) \in ((\rho \cup \rho^{-1} \cup id_X)^c)^n \\ \Longrightarrow\ &\exists\ x_0, x_1, \dots, x_n \text{ such that } x = x_0 andy = x_n \text{ and } (\forall\ i)\ \ (x_i, x_{i+1}) \in (\rho \cup \rho^{-1} \cup id_X)^c \\ \Longrightarrow\ &zx = zx_0, zx_n = zy \text{ and } (\forall\ i)\ \ (zx_i, zx_{i+1}) \in (\rho \cup \rho^{-1} \cup id_X)^c \\ &(\text{since } (\rho \cup \rho^{-1} \cup id_X)^c \text{ is left and right congruence}) \\ \Longrightarrow\ &(zx, zy) \in ((\rho \cup \rho^{-1} \cup id_X)^c)^n \\ \Longrightarrow\ &(zx, zy) \in \cup_{n=0}^{\infty}((\rho \cup \rho^{-1} \cup id_X)^c)^n \\ \Longrightarrow\ &(zx, zy) \in (\rho^c)^e.\end{aligned}$$

Therefore, $(\rho^c)^e$ is left compatible. Similarly, $(\rho^c)^e$ is right compatible. Hence $(\rho^c)^e$ is a congruence containing ρ.
Finally, let τ be any congruence containing ρ. Then τ is left and right compatible, so $\rho^c \subseteq \tau$. Since τ is an equivalence relation, it must contain $(\rho^c)^e$. Hence $(\rho^c)^e \subseteq \tau$. Therefore, $(\rho^c)^e$ is the smallest congruence containing ρ, and therefore $\rho^\# = (\rho^c)^e$. Consequently, $\rho^\# = (\rho^c)^e$ □

We denote by $\mathscr{C}(X)$ the set of all congruences on X. Then $\mathscr{C}(X)$, as a subset of $\mathscr{E}(X)$ and $\mathfrak{B}(X)$, is partially ordered by inclusion.
In fact, $\mathscr{C}(X)$ forms a lattice. For $\rho, \sigma \in \mathscr{C}(X)$, we have

$$\rho \wedge \sigma = \rho \cap \sigma \qquad \text{and} \qquad \rho \vee \sigma = (\rho \cup \sigma)^{\#}.$$

Also,

$$\begin{aligned}(\rho \cup \sigma)^{\#} &= ((\rho \cup \sigma)^{c})^{e} \\ &= (\rho^{c} \cup \sigma^{c})^{e} \\ &= (\rho \cup \sigma)^{e}\end{aligned}$$

so there is no ambiguity in writing $\rho \vee \sigma$ whether one means the join $(\rho \vee \sigma)^{e}$ in the lattice $\mathscr{E}(X)$ or the join $(\rho \vee \sigma)^{\#}$ in the lattice $\mathscr{C}(X)$.

Proposition 1.1.11. *Let $\rho, \sigma \in \mathscr{E}(X)$. Then*

$$\rho \vee \sigma = (\rho \circ \sigma)^{\infty}.$$

Proof. Let $\rho, \sigma \in \mathscr{E}(X)$. Since $\rho \vee \sigma$ contains both ρ and σ, it follows that

$$\rho \circ \sigma \subseteq (\rho \cup \sigma) \circ (\rho \cup \sigma) = (\rho \vee \sigma)^{2}.$$

More generally, $(\rho \circ \sigma)^{n} \subseteq (\rho \cup \sigma)^{2n}$. Thus,

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

On the other hand, $\rho \circ \sigma \supseteq \rho \circ id_X = \rho$ (since σ is reflexive), and $\rho \circ \sigma \supseteq id_X \circ \sigma = \sigma$ (since ρ is reflexive). Thus, $\rho \cup \sigma \subseteq \rho \circ \sigma$. Hence, $(\rho \cup \sigma)^{\infty} \subseteq (\rho \circ \sigma)^{\infty}$.
Consequently, $(\rho \cup \sigma)^{\infty} = (\rho \circ \sigma)^{\infty}$.
Then,

$$\begin{aligned}\rho \vee \sigma = (\rho \cup \sigma)^{e} &= \left(\left((\rho \cup \sigma)^{R}\right)^{S}\right)^{\infty} \\ &= \left((\rho \cup \sigma) \cup (\rho \cup \sigma)^{-1} \cup \mathrm{id}_X\right)^{\infty} \\ &= \left(\rho \cup \sigma \cup \rho^{-1} \cup \sigma^{-1} \cup \mathrm{id}_X\right)^{\infty} \\ &= (\rho \cup \sigma \cup \mathrm{id}_X)^{\infty} \\ &= (\rho \cup \sigma)^{\infty} = (\rho \circ \sigma)^{\infty}.\end{aligned}$$

This completes the proof. □

Proposition 1.1.12. *Let $\rho, \sigma \in \mathscr{E}(X)$. If $\rho \circ \sigma = \sigma \circ \rho$, then*

$$\rho \vee \sigma = \rho \circ \sigma.$$

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

$$(\rho \circ \sigma)^{2} = \rho \circ \sigma \circ \rho \circ \sigma = \rho \circ \rho \circ \sigma \circ \sigma = \rho \circ \sigma,$$

since ρ and σ are transitive.
Hence, $(\rho \circ \sigma)^{n} = \rho \circ \sigma$ for all $n \in \mathbb{N}$, and therefore

$$\rho \circ \sigma = (\rho \circ \sigma)^{\infty} = \bigcup_{n \geq 0} (\rho \circ \sigma)^{n} = \rho \circ \sigma.$$

So $\rho \vee \sigma = \rho \circ \sigma$. □

Lemma 1.1.13. *If $\rho = \cap_i \rho_i$ (an intersection of congruences, or even just equivalence relations on a set X), then for any $x \in X$*

$$[x]_\rho = \cap_i [x]_{\rho_i}.$$

Proof. ; For any $y \in X$

$$x \in [x]_\rho \iff (x, y) \in \rho \iff (x, y) \in \rho_i \quad \forall\ i \iff y \in [x]_{\rho_i} \quad \forall\ i \iff y \in \cap_i [x]_{\rho_i}$$

□

1.2. Introductory Algebraic structures

1.2.1. Groupoids, Identities, and Zeros

Definition 1.2.1. A *groupoid* is a non-empty set A together with a binary operation

$$A \times A \to A, \qquad (a, a') \mapsto aa'.$$

The operation is usually called the *multiplication* of the groupoid.

Remark 1.2.2. Let A be a groupoid. For non-empty subsets $B, C \subseteq A$, define

$$BC = \{bc \mid b \in B,\ c \in C\}.$$

We write $B^2 = BB$, and similarly for higher products.

Definition 1.2.3. Let S be a groupoid. An element $e \in S$ is called

- a *left identity* if $es = s$ for all $s \in S$;
- a *right identity* if $se = s$ for all $s \in S$;
- an *identity* if $es = s = se$ for all $s \in S$.

An identity is also called a *neutral element.*

Proposition 1.2.1. *If a groupoid S has both a left and a right identity, then they coincide. Hence a groupoid has at most one identity.*

Proof. Let e' be a left identity and e'' a right identity. Then

$$e'' = e'e'' = e'.$$

□

We denote the identity (when it exists) by 1 or more precisely by 1_S.

Definition 1.2.4. Let S be a groupoid with identity.

- $s \in S$ is *left invertible* if there exists $t \in S$ such that $ts = 1$.
- s is *right invertible* if there exists $t \in S$ such that $st = 1$.
- s is *invertible* if there exists $t \in S$ satisfying $ts = st = 1$.

In third case, such an element t is called an inverse of s, and is denoted by s^{-1} whenever it is unique.

Definition 1.2.5. Let S be a groupoid. An element $z \in S$ is called

- a *left zero* if $zs = z$ for every $s \in S$;
- a *right zero* if $sz = z$ for every $s \in S$;
- a *zero* if $zs = z = sz$ for every $s \in S$.

A zero is usually denoted by 0.

Exercise 1.2.2. *Show that if a groupoid has both a left zero and a right zero, then they coincide. Hence a groupoid has at most one zero.*

1.2.2. Semigroups, monoids and groups

Definition 1.2.6. A *semigroup* is a groupoid whose multiplication is associative. A semigroup with an identity element is called a *monoid.*

Proposition 1.2.3. *If an element of a monoid has both a left and a right inverse, then they coincide.*

Proof. Suppose $ts = 1$ and $st' = 1$. Then

$$t' = (ts)t' = t(st') = t.$$

□

Corollary 1.2.4. *Every element of a monoid has at most one inverse.*

Definition 1.2.7. A *group* G is a monoid in which every element is invertible.

For any $a, b \in G$,

$$(ab)^{-1} = b^{-1}a^{-1}, \qquad (a^{-1})^{-1} = a.$$

Exercise 1.2.5. *Suppose S is a semigroup with an element e satisfying $es = s$ for every $s \in S$, and suppose every $s \in S$ has an element $t \in S$ such that $ts = e$. Show that S is a group.*

Remark 1.2.8 (Free semigroup and free monoid). Let X be a non-empty set, called an *alphabet.* Define

$$X^+ = \{x_1x_2\cdots x_n \mid n \in \mathbb{N},\ x_i \in X,\ 1 \le i \le n\},$$

the set of all finite non-empty words over X.
Two words

$$x_1x_2\cdots x_n, \qquad y_1y_2\cdots y_m$$

are equal if and only if

$$n = m \quad \text{and} \quad x_i = y_i \quad \text{for all } 1 \le i \le n.$$

Define the multiplication (concatenation) of words by

$$(x_1x_2\cdots x_n)(y_1y_2\cdots y_m) = x_1x_2\cdots x_ny_1y_2\cdots y_m.$$

With this operation, X^+ forms a semigroup, called the *free semigroup* on X, or the *free semigroup with basis X.*
Now let

$$X^* = X^+ \cup \{\varepsilon\},$$

where ε denotes the empty word. Then X^* is a monoid under concatenation, with identity element ε. It is called the *free monoid* on X, or the *free monoid with basis X.*

1.2.3. Examples

Example 1.2.9 (Groupoids).

1. $(\mathbb{Z}, -)$.
2. $(\mathbb{Q} \setminus \{0\}, /)$.
3. $(\mathbb{N}, \uparrow)$, where $n \uparrow m = n^m$.
4. The vector product $(\mathbb{R}^3, \times)$.

Example 1.2.10 (Semigroups and monoids).

1. If $(R, +, \cdot)$ is a ring, then $(R, +)$ is a group and $(R, \cdot)$ is a semigroup.
2. $(\mathbb{N}, \cdot)$ is a monoid.
3. $(\mathbb{N}, +)$ is a semigroup.
4. $(\mathscr{T}(X), \circ)$, the full transformation monoid.
5. $(\mathscr{P}\mathscr{T}(X), \circ)$, the monoid of partial transformations.
6. $(\mathfrak{B}(X), \circ)$, the semigroup of binary relations.
7. The free semigroup X^+.
8. The free monoid X^*.
9. $(\mathbb{Z}, \gcd)$.
10. **The bicyclic monoid:**
    Let $B = \mathbb{N}_0 \times \mathbb{N}_0$, where $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$. Define a binary operation on B by

    $$(m, n)(p, q) = (m - n + \max\{n, p\},\ q - p + \max\{n, p\}).$$

    Equivalently,

    $$(m, n)(p, q) = \begin{cases} (m - n + p,\ q), & \text{if } p \geq n, \\ (m,\ n - p + q), & \text{if } p \leq n. \end{cases}$$

    Then $(B, \cdot)$ is a monoid, called the *bicyclic monoid*, with identity element $(0, 0)$.

Example 1.2.11 (Groups).

1. $(\mathbb{Z}, +)$.
2. $(\mathbb{Q}, +)$.
3. $(\mathbb{Q} \setminus \{0\}, \cdot)$.
4. The residue class group $(\mathbb{Z}_r, +)$.
5. The symmetric group $S(X)$, or S_n when $|X| = n$.

2. The Semigroup

2.1. Semigroups and Monoids

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 operation $\circ$, 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.
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, $\mathbb{N} = \{1, 2, 3, \dots\}$ does not include 0.)

Example 2.1.1. 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.

2.1.1. Basic Concepts

Definition 2.1.2. 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.

Definition 2.1.3. 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.

If a semigroup does not contain identity (zero element), we can always add a new element to act as an identity (zero element). To see this, 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.
Throughout this chapter, 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 $\varphi\psi$ or simply $\varphi\psi$, and is a map from X to Z with $x(\varphi\psi) = (x\varphi)\psi$ for all $x \in X$.

Definition 2.1.4 (Cartesian Product). Let $X = \{X_i : i \in I\}$ be a collection of sets. Informally, the Cartesian product $\prod_{i\in I} X_i$ of the sets in 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 $\prod_{i\in I} X_i$ is 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 $I = \{1, \dots, n\}$ is finite, we write $X_1 \times \cdots \times X_n$ for $\prod_{i\in I} X_i$. When the sets X_i are all equal to a set X, that is, when we consider products of $|I|$ copies of the set X, we write X^I for $\prod_{i\in I} X_i$.

Definition 2.1.5. Let $S = \{S_i : i \in I\}$ be a collection of semigroups. The direct product of the semigroups in S is their Cartesian product $\prod_{i\in I} S_i$ with componentwise multiplication: $(i)(s)(i)(t) = (i)(s)(i)t$, or, using tuple notation, if $(\dots, s_i, \dots), (\dots, t_i, \dots) \in \prod_{i\in I} S_i$, then

$$(\dots, s_i, \dots)(\dots, t_i, \dots) = (\dots, s_i t_i, \dots).$$

It is easy to prove that this componentwise multiplication is associative, and so the direct product is itself a semigroup.
For $x \in S$ and $n \in \mathbb{N}$, define

$$x^n = \underbrace{x \cdots x}_{n \text{ times}}.$$

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 *idempotent* if $x^2 = x$. The set of idempotents of S is denoted $E(S)$.
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, Z of S, we have $X(YZ) = (XY)Z$. By analogy with the above, for $X \subseteq S$ and $n \in \mathbb{N}$, define

$$X^n = \underbrace{X \cdots X}_{n \text{ times}}.$$

Definition 2.1.6 (Nilpotent Semigroup). The semigroup S is nilpotent if it contains a zero and there exists some $n \in \mathbb{N}$ such that $S^n = \{0\}$.

Definition 2.1.7. 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 $x^n = \{0\}$.

Definition 2.1.8 (Cancellative Semigroup). 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 2.1.9. A non-trivial semigroup with zero cannot be cancellative.

Definition 2.1.10 (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.

2.1.2. Regular Semigroups

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, $(xy)^2 = xyxy = x(yx)y = xy$ and $(yx)^2 = yxyx = y(xy)x = yx$ and hencen xy and yx are idempotent elements of S.

Definition 2.1.11 (Regular Semigroup). If every element of S is regular, then S is a regular semigroup.

Now we define the inverse of an element of a semigroup S in general.

Definition 2.1.12. Let $x \in S$. An element $x' \in S$ is called as inverse of x if $x = xx'x$ and $x' = x'xx'$.

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

Proof. 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

$$xx'x = x(yxy)x = (xyx)yxyx = xyx = x$$

and

$$x'xx' = (yxy)x(yxy) = y(xyx)yxy = yxy = x',$$

so x' is an inverse of x. □

In the proof of Proposition 2.1.1, 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. The set of inverses of x is denoted $V(x)$. Notice also that a zero of a semigroup has an inverse, namely itself. In general, if $e \in S$ is idempotent, then $e^2 = e$ and so e is an inverse of itself. In particular, every idempotent is regular.

Example 2.1.13. (a) Let $U = \{0, \dots, k\}$ for some $k > 0$. Define $m\Delta n = \min\{m, n\}$. It is easy to see that Δ is associative, and so (U, Δ) is a semigroup. Notice that $0\Delta m = m\Delta 0 = 0$ and $k\Delta m = m\Delta k = m$ for all $m \in U$. Hence U has zero 0 and identity k. Furthermore, $m\Delta m = m$ for all $m \in U$, so every element of U is idempotent. Finally, $m\Delta n = n\Delta m$ for all $m, n \in U$, so U is commutative.

(b) Define a similar associative operation Δ on $\mathbb{N}_0 \cup \{0\} = \{0, 1, 2, \dots\}$ by

$$m\Delta n = \min\{m, n\}.$$

Then $(\mathbb{N}, \Delta)$ 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:

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

With the usual matrix multiplication, $M_2(\mathbb{Z})$ is a monoid with identity

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and zero

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

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 $R^{-1} \in M_2(\mathbb{Q})$. Hence V is left-cancellative. Similarly, it is right-cancellative and therefore cancellative.

Definition 2.1.14. Let L be a left zero semigroup and R a right zero semigroup. Let $B = L \times R$. This semigroup is called as $|L| \times |R|$ rectangular band, or simply a *rectangular band.*

For $(\ell_1, r_1), (\ell_2, r_2) \in B$, we have

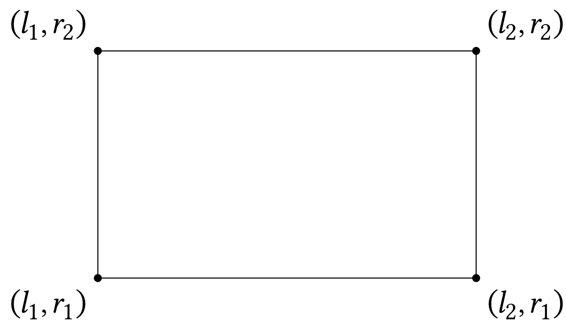
$$(\ell_1, r_1)(\ell_2, r_2) = (\ell_1, r_2),$$

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 vertically in line with (ℓ_1, r_1) and horizontally in line with (ℓ_2, r_2), as shown in Figure 2.1.2.



2.1.3. Subsemigroups

Definition 2.1.15 (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 subsemigroup 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 2.1.2. *The set of invertible elements of a monoid forms a subgroup.*

Proof. 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

$$y^{-1}x^{-1}xy = y^{-1}y = 1 \qquad \text{and} \qquad xyy^{-1}x^{-1} = xx^{-1} = 1.$$

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. □

Proposition 2.1.2 makes following definition justifiable:

Definition 2.1.16 (Group of units). The set of invertible elements of a monoid is called its group of units.

Lemma 2.1.3. *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 S.*

Proof. 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 $gh \in gG = G$, and so 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 $x \in G$, and then

$$eh = egx = gx = h.$$

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 1.2.1. 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 1.2.3. Since $g \in G$ was arbitrary, G is a subgroup. □

2.1.4. Generators

Let $\mathscr{T} = \{T_i : i \in I\}$ be a collection of subsemigroups of S. Then if their intersection $\bigcap T = \bigcap_{i \in I} T_i$ is non-empty, it is also a subsemigroup.

Definition 2.1.17 (Generating a subsemigroup). Let $X \subseteq S$, and let $\mathscr{T}$ be the collection of subsemigroups of S that contain X. The collection $\mathscr{T}$ has at least one member, namely the semigroup S itself, and every subsemigroup in $\mathscr{T}$ contains X, so $\bigcap T$ is non-empty and is thus a subsemigroup. Indeed, it is the smallest subsemigroup of S that contains X. This subsemigroup, denoted by $\langle X \rangle$, is called the subsemigroup generated by X.

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.

Proposition 2.1.4. *Let $X \subseteq S$. Then*

$$\langle X \rangle = \{x_1 x_2 \cdots x_n : n \in \mathbb{N},\ x_i \in X\}.$$

Proof. Let
$$U = \{x_1 x_2 \cdots x_n \,:\, n \in \mathbb{N},\ x_i \in X\}.$$
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 T, and so $\langle X \rangle \subseteq U$. Since $X \subseteq \langle X \rangle$ and $\langle X \rangle$ is closed under multiplication, we have $U \subseteq \langle X \rangle$. Therefore $\langle X \rangle = U$. $\square$

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, that is, 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, denoted by $\mathrm{Mon}(X)$.

Definition 2.1.18. This submonoid $\mathrm{Mon}(X)$ is called the submonoid generated by X.

Proposition 2.1.5. *Let $X \subseteq M$. Then*
$$\mathrm{Mon}(X) = \{1_M x_1 x_2 \cdots x_n \,:\, n \in \mathbb{N} \cup \{0\},\ x_i \in X\}.$$

Remark 2.1.19. Essentially, when we generate a submonoid of a monoid, we always include the identity of the monoid. If $X \subseteq M$ is such that $\mathrm{Mon}(X) = M$, then X is a monoid generating set for M and M is generated by X as a monoid. 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.

2.1.5. Ideals and Monogenic Semigroup

Definition 2.1.20 (Ideal)**.** 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.

Definition 2.1.21 (Principal ideal)**.** For any $x \in S$, define
$$L(x) = S^1 x = \{x\} \cup Sx, \qquad R(x) = xS^1 = \{x\} \cup xS, \qquad J(x) = S^1 x S^1 = \{x\} \cup xS \cup Sx \cup SxS.$$
Then $L(x)$, $R(x)$, and $J(x)$ are, respectively, the principal left ideal generated by x, the principal right ideal generated by x, and the principal ideal generated by x. As they are, respectively, a left ideal, a right ideal, and a (two-sided) ideal.

Example 2.1.22.

1. 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, $I_n = L(n) = R(n) = J(n)$.

2. 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 is a right ideal of S if and only if $T = S$.

3. 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.

Definition 2.1.23 (Rees congruence and Rees quotient). Let S be a semigroup and I a proper ideal of S. The *Rees congruence* on S modulo I is

$$\rho_I = (I \times I) \cup \mathbf{1}_S,$$

so that $x\,\rho_I\,y$ if and only if $x = y$ or $x, y \in I$. The quotient semigroup S/ρ_I, also written as S/I and called the *Rees quotient* of S by I, may be identified with

$$S/I = \{I\} \cup \{\{x\} : x \in S \setminus I\},$$

which can be regarded as I together with the elements of $S \setminus I$.

In S/I the product of two elements in $S \setminus I$ is same as their product in S if this lies in $S \setminus I$; otherwise the product is I.
Since the element I is the zero element of the semigroup, another way of thinking S/ρ_I is as $(S \setminus I) \cup \{0\}$, where all products not falling in $S \setminus I$ are zero.
The map $\varphi : S \to S/I$ given by $x\varphi = x$ if $x \notin I$ and $x\varphi = 0$ if $x \in I$ is a surjective homomorphism, called the *natural homomorphism.*

Definition 2.1.24. Let $\varphi : S \longrightarrow T$ be a homomorphism. Then, φ is said to be a *rees morphism* if $\ker\varphi$ is a rees congruence on S.

Definition 2.1.25 (Ideal extension). Let M be a semigroup and T a semigroup with zero 0. A semigroup E is called an *ideal extension of M by T* if M is an ideal of E and the Rees quotient semigroup E/M is isomorphic to T.

Definition 2.1.26 (Monogenic semigroup). Suppose S is generated by a single element x; that is, $S = \langle x \rangle$. Then by Proposition 2.1.4,

$$S = \{x^n : n \in \mathbb{N}\},$$

and we call S the monogenic semigroup generated by x.

There are two possibilities: either all the powers of x are distinct, or there exist $k, m \in \mathbb{N}$ such that $x^k = x^{k+m}$. In the latter case, x is said to be periodic. If k and m are minimal, then S is finite, with $k + m - 1$ elements,

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

We call k the *index* of x and m the *period* of x.

Remark 2.1.27. Let $K = \{x^k, x^{k+1}, \dots, x^{k+m-1}\}$. It is easy to see that K is an ideal of S. Furthermore, K is a subgroup of S, since the integers $k, k+1, \dots, k+m-1$ 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.

Definition 2.1.28. A periodic semigroup is one in which every element is periodic.

2.1.6. Homomorphisms

Definition 2.1.29. Let S and T be semigroups. A map $\varphi : S \to T$ is a *homomorphism* if

$$(xy)\varphi = (x\varphi)(y\varphi) \quad \forall \quad x, y \in S.$$

If S and T are monoids, then φ is a *monoid homomorphism* if

$$(xy)\varphi = (x\varphi)(y\varphi) \quad \forall \quad x, y \in S \qquad \text{and } 1_S\varphi = 1_T.$$

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.

Definition 2.1.30. 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 $\varphi\varphi^{-1} = id_T$ and $\varphi^{-1}\varphi = id_S$. If there is an isomorphism $\varphi : S \to T$, then we say that S and T are isomorphic, and denote this by $S \cong T$.
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.

Definition 2.1.31. 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 identity relation (that is, $\ker\varphi = id_S$).
The following result shows that every semigroup is isomorphic to a subsemigroup of a transformation semigroup. This is the semigroup analogue of Cayley's theorem for groups, which states that every group is isomorphic to a subgroup of a symmetric group.

Theorem 2.1.6. *For any $x \in S$, let $\rho_x \in \mathscr{T}_{S^1}$ be the map defined by $s\rho_x = sx$ for all $s \in S^1$. Then the map $\varphi : S \to \mathscr{T}_{S^1}$ given by $x \mapsto \rho_x$ is a monomorphism of S.*

Proof. Let $x, y, s \in S$. Then

$$s\rho_x\rho_y = (s\rho_x)\rho_y = (sx)\rho_y = (sx)y = s(xy) = s\rho_{xy}.$$

Hence $\rho_x\rho_y = \rho_{xy}$, and so $(xy)\varphi = (x\varphi)(y\varphi)$. Therefore φ is a homomorphism.
Furthermore, if $x\varphi = y\varphi$, then $\rho_x = \rho_y$. Hence

$$1\rho_x = 1\rho_y,$$

that is, $x = y$. Therefore φ is injective. □

A map $\varphi : S \to T$ is an *anti-homomorphism* if

$$(xy)\varphi = (y\varphi)(x\varphi)$$

for all $x, y \in S$.

Remark 2.1.32. An *endomorphism* is a homomorphism from a semigroup S to itself. The set of all endomorphisms on S is denoted $\operatorname{End}(S)$ and forms a subsemigroup of $\mathscr{T}_S$.

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 $\operatorname{im}\varphi$ of G. Clearly any group-embeddable semigroup is cancellative, but we shall see that there exist cancellative semigroups that are not group-embeddable.

2.1.7. Subdirect products

Definition 2.1.33 (Projection maps). 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 $\prod_{i \in I} S_i$ onto S_j, taking an element of the direct product to its j-th component:

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

Notice that every π_j is an epimorphism.

Definition 2.1.34 (Subdirect product). A *subdirect product* of $\mathcal{S}$ is [a semigroup isomorphic to] a subsemigroup P of the direct product $\prod_{i \in I} S_i$ such that $P\pi_i = S_i$ for all $i \in I$.

Definition 2.1.35 (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

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

Proposition 2.1.7. *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. If S is a subdirect product of $\mathcal{S}$, then the collection of projection maps restricted to S (that is, $\{\pi_i|_S : S \to S_i : i \in I\}$) separates the elements of S.
On the other hand, suppose the collection Φ separates the elements of S. Define $\psi : S \to \prod_{i \in I} S_i$ 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 $s\varphi_i = t\varphi_i$ for all $i \in I$, which means that Φ separates the elements of S. Hence ψ is injective, so S is isomorphic to the subsemigroup $\operatorname{im}\psi$ of $\prod_{i \in I} S_i$. Finally, the projection maps π_i are all surjective since each φ_i is surjective. So $\operatorname{im}\psi$ is a subdirect product of S. $\square$

Proposition 2.1.8. *Let S be a semigroup and let $\Sigma = \{\sigma_i : i \in I\}$ be a collection of congruences on S. Let $\sigma = \bigcap_{\sigma_i \in \Sigma} \sigma_i$. Then S/σ is a subdirect product of $\{S/\sigma_i : i \in I\}$.*

Proof. 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 by Lemma 1.1.13. 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 $[x]_{\sigma_i} = [y]_{\sigma_i}$ for all $i \in I$, which implies $(x, y) \in \sigma$. Therefore S/σ is a subdirect product of $\{S/\sigma_i : i \in I\}$ by Proposition 2.1.7. $\square$

Proposition 2.1.9. *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. 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

$$\begin{aligned}(x\psi)(y\psi) &= x1_M y1_M \\ &= xy1_M \\ &= (xy)\psi,\end{aligned}$$

since $y1_M$ lies in the ideal M of E. Thus ψ is a homomorphism. Both φ and ψ are clearly surjective. Furthermore, if $x\varphi = y\varphi$, then either $x, y \in E - M$ and $[x]_M = [y]_M$, so $x = y$, or $x, y \in M$ and $x1_M = y1_M$, 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. $\square$

2.1.8. Actions

Definition 2.1.36 (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

$$(a \cdot x) \cdot y = a \cdot (xy)$$

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.

Example 2.1.37.

1. Any subsemigroup S of $\mathcal{T}(A)$ acts on A by $a \cdot \varphi = a\varphi$ (where $\varphi \in \mathcal{T}(A)$).
2. 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, 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 $(a \cdot x) \cdot y = a \cdot (xy)$ implies that φ is a homomorphism. Conversely, given a homomorphism $\varphi : S \to \mathcal{T}(A)$, we can define an action by $a \cdot s = a(s\varphi)$, which satisfies $(a \cdot x) \cdot y = a \cdot (xy)$. There is thus a one-to-one correspondence between actions of a semigroup S on A and homomorphisms $\varphi : S \to \mathcal{T}(A)$.

Definition 2.1.38 (Free action). An action of S on A is *free* if distinct elements of S act differently on every element of A, or, equivalently,

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

Definition 2.1.39 (Transitive action). An action of S on A is *transitive* if for all $a, b \in A$, there exists some element $s \in S$ such that $a \cdot s = b$.

Definition 2.1.40 (Regular action). An action of S on A 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 $s\varphi \in \mathrm{End}(A)$ for each $s \in S$; in this case,

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

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

Note 2.1.41. The above discussions concern a right semigroup action. There is a dual notion of a left semigroup action

Definition 2.1.42. A *left semigroup action* of S on A 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 endomorphisms also apply to left actions.

Remark 2.1.43. 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 correspond to homomorphisms.

2.2. Free semigroups and presentations

Informally, the free semigroup on a set A is the unique most general semigroup generated by A, in the sense that every other semigroup generated by A is a homomorphic image (and hence a factor semigroup) of the free semigroup on A.

Definition 2.2.1. An alphabet A is an abstract set whose elements are called *letters*.

2.2.1. Free Semigroups

A word over A is a finite sequence

$$(a_1, a_2, \dots, a_n),$$

where $a_i \in A$. The length of this word is defined to be n.
The empty sequence is called the *empty word* and is denoted by ε; its length is 0. We denote the set of all non-empty words over A by A^+, and the set of all words, including the empty word, by A^*. That is

$$A^* = A^+ \cup \{\varepsilon\}.$$

The multiplication of words is defined by concatenation:

$$(a_1, \dots, a_n)(b_1, \dots, b_m) = (a_1, \dots, a_n, b_1, \dots, b_m).$$

Clearly, this multiplication is associative, and so A^+ forms a semigroup and A^* forms a monoid. The empty word ε is the identity of A^*.

Definition 2.2.2. The semigroup A^+ is called the *free semigroup* on A, and the monoid A^* as *free monoid* on A.

We shall usually write

$$a_1 a_2 \cdots a_n$$

instead of $(a_1, a_2, \dots, a_n)$, which is possible because of associativity. We denote the length of a word u by $|u|$. In particular,

$$|u| = 0 \iff u = \varepsilon.$$

Lemma 2.2.1. *Let $u, v \in A^*$. Then*

$$|uv| = |u| + |v|.$$

2.2.2. Results and Properties

Definition 2.2.3 (Equidivisible semigroup). A semigroup S is called *equidivisible* if, for all $x, y, z, t \in S$,

$$xy = zt$$

implies that either

$$(\exists p \in S)\,(x = zp \text{ and } t = py),$$

or

$$(\exists q \in S)\,(z = xq \text{ and } y = qt).$$

Every group is equidivisible. Indeed, if $xy = zt$, then one may take $p = z^{-1}x$ or $q = x^{-1}z$.

Proposition 2.2.2. *The free semigroup A^* is equidivisible.*

Proof. 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

$$x = a_1 \cdots a_k, \qquad y = a_{k+1} \cdots a_n, \qquad z = a_1 \cdots a_\ell, \qquad t = a_{\ell+1} \cdots a_n,$$

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 $k \leq \ell$, 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 $t = py$. □

Proposition 2.2.3. *Let $A = \{x, y\}$. Let $B = \{b_i : i \in \mathbb{N}\}$. Then A^* contains a submonoid isomorphic to B^*.*

Proof. 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 by 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_i; that is, $u = b_i u'$ and $v = b_i v'$. Then

$$(b_i\varphi)(u'\varphi) = (b_i\varphi)(v'\varphi)$$

and so $u'\varphi = v'\varphi$ by cancellativity in A^*. Thus 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,

$$u = b_i u', \qquad v = b_j v'.$$

Then

$$xy^ix(u'\varphi) = (b_i\varphi)(u'\varphi) = (b_j\varphi)(v'\varphi) = xy^jx(v'\varphi).$$

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 $\operatorname{im}\varphi$. □

A similar result holds for free semigroups.

Definition 2.2.4 (Indecomposable element). An element a of a semigroup S is said to be *indecomposable* if there do not exist $u, v \in S$ such that

$$a = uv.$$

Proposition 2.2.4. *Let M be a submonoid of A^*, and let*

$$N = M \setminus \{\varepsilon\}.$$

Then $N \setminus N^2$ is the unique minimal generating set for M.

Proof. 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 Lemma 2.2.1, 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 the other hand, if $u \notin N - N^2$, then $u \in N^2$ and so

$$u = u'u''$$

for $u', u'' \in N$. By Lemma 2.2.1,

$$|u'|, |u''| < |u| = l.$$

So, by assumption,
$$u', u'' \in \langle N - N^2 \rangle$$
and hence
$$u \in \langle N - N^2 \rangle.$$
Therefore, by induction,
$$N \subseteq \langle N - N^2 \rangle.$$
Hence
$$M = \langle N - N^2 \rangle.$$
Therefore $N - N^2$ is a generating set for M, and since every generating set must contain $N - N^2$, it is the unique minimal generating set. □

The elements of $N \setminus N^2$ are precisely the *indecomposable* elements of M.

Definition 2.2.5. The base of a submonoid or a subsemigroup M of A^* is defined to be $N - N^2$, where $N = M - \{\varepsilon\}$.

The base is the unique minimal generating set for M.

Corollary 2.2.5. *The alphabet A is the base of both A^+ and A^*.*

Proposition 2.2.6. *Let $u, v \in A^*$. Then*
$$uv = vu$$
if and only if there exist $w \in A^*$ and $i, j \in \mathbb{N}$ such that
$$u = w^i \qquad \text{and} \qquad v = w^j.$$

Proof. 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 2.2.2, there exists $p \in A^*$ such that
$$u = vp \qquad \text{and} \qquad u = pv.$$
If $p = \varepsilon$, then $u = v$. Otherwise,
$$vp = pv,$$
where
$$|vp| < |uv|.$$
So by induction,
$$v = w^j \qquad \text{and} \qquad p = w^i$$
for some $w \in A^*$ and $i, j \in \mathbb{N}$. Thus
$$u = vp = w^{i+j}.$$
Hence, by induction, the result holds for all $u, v \in A^+$. □

Proposition 2.2.7. *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. Clearly every element of A^+ has a unique representative as a product of elements of A. 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 by $b_1\cdots b_m$, where $b_i \in A$, 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. □

Example 2.2.6. 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 $S - S^2$. Hence S is not free.

The above example shows that a free semigroup contains subsemigroups which are not free. In contrast, every subgroup of a free group is free by the Nielsen-Schreier theorem.

Definition 2.2.7 (Length function). 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 additional property that

$$|s| = 0 \implies s = 1_M.$$

Notice that the usual notion of length for free semigroups as defined previously is also a proper length function.

Proposition 2.2.8. *A monoid M is equidivisible and has a proper length function if and only if it is isomorphic to A^*.*

Proof. 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

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

Let $A = N - N^2$ and $w \in N^2$. Then $w = w'w''$ with

$$0 < |w'| < |w| \qquad \text{and} \qquad 0 < |w''| < |w|.$$

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 either

$$a_1 = b_1 p \qquad \text{and} \qquad pa_2 \cdots a_n = b_2 \cdots b_m,$$

or

$$b_1 = a_1 p \qquad \text{and} \qquad pb_2 \cdots b_m = a_2 \cdots a_n.$$

Since $a_1 \in A = N - N^2$, it cannot be written as a product of two non-identity elements. Thus in the first case $p = 1_M$, and so

$$a_1 = b_1, \qquad a_2 \cdots a_n = b_2 \cdots b_m.$$

The second case is similar. Applying the induction hypothesis shows

$$m = n$$

and

$$a_i = b_i$$

for all $i \geq 2$.
Thus every element of N has a unique representative as a product of elements of A, and so $N \cong A^+$ by Proposition 2.2.7. Hence

$$M = N \cup \{1_M\} \cong A^*.$$

□

Definition 2.2.8. 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 $z \in M - \{1_M\}$.

Proposition 2.2.9. *A monoid M is free if it has the following four properties:*

1. *the only left- and right-invertible element of M is 1_M;*
2. *M is cancellative;*
3. *M is equidivisible;*
4. *no element of M has infinitely many distinct non-trivial left factors.*

Proof. Clearly, A^* has the four properties. So suppose M has the four properties (1)–(4). 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, $yx = 1_M$. Thus 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

$$y_1 \cdots y_k, \qquad k < m + 2,$$

are all non-trivial left factors of x. Furthermore, they are all distinct, for if

$$y_1 \cdots y_k = y_1 \cdots y_{k+1},$$

then cancellativity shows that

$$y_{k+1} \cdots y_{k+1} = 1_M,$$

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

$$N \supsetneq N^2 \supsetneq N^3 \supsetneq \cdots,$$

and hence every element $x \in N$ lies in $N^m - N^{m+1}$ for some unique m, and so x has an expression

$$x = n_1 \cdots n_m$$

as a product of elements $n_i \in N$.
Arguing by equidivisibility as in the proof of Proposition 2.2.8, we see that each element has a unique expression of this form. So M is free by Proposition 2.2.7. □

2.2.3. Universal Property

Let F be a semigroup and let A be an alphabet. 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:

$$\begin{tikzcd} A \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & F \arrow[d, "\varphi^+"] \\ & S \end{tikzcd}$$

Proposition 2.2.10 (Uniqueness of free semigroups). *Let A be an alphabet and let F be a semigroup. Then F is free on A if and only if $F \cong A^+$.*

Proof. Suppose $F \cong A^+$. 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. Let S be a semigroup and $\varphi : A \to S$ be a map. Define

$$\varphi^+ : A^+ \to S$$

by

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

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 $a_1 a_2 \cdots a_n \in A^+$,

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

Thus $\psi = \varphi^+$. Hence φ^+ is the unique homomorphism from A^+ to S with $\iota\varphi^+ = \varphi$, and so A^+ is free on A.
Now let F be a semigroup that is free on A. Let

$$\iota_1 : A \to A^+ \qquad \text{and} \qquad \iota_2 : A \to F$$

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

$$\iota_1 = \iota_2\iota_1^+ \qquad \text{and} \qquad \iota_2 = \iota_1\iota_2^+.$$

That is, the following diagrams commute:

$$\begin{tikzcd} A \arrow[r, "\iota_1"] \arrow[dr, "\iota_2"'] & A^+ \arrow[d, "\iota_2^+"] \\ & F \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "\iota_2"] \arrow[dr, "\iota_1"'] & F \arrow[d, "\iota_1^+"] \\ & A^+ \end{tikzcd}$$

Therefore, by the uniqueness requirement in the definition of freedom,

$$\iota_2^+ \iota_1^+ = id_{A^+} \qquad \text{and} \qquad \iota_1^+ \iota_2^+ = id_F.$$

Hence ι_1^+ and ι_2^+ are mutually inverse isomorphisms, and so

$$F \cong A^+.$$

□

Remark 2.2.9. What makes free semigroups 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 (e.g., we could choose A to have the same cardinality as S and φ to be a bijection). Then φ^+ extends to a homomorphism $\varphi^+ : A^+ \to S$. Since $< \operatorname{im}\varphi >= S$, we have $\operatorname{im}\varphi^+ = S$.

By the Homomorphism Theorem 1.1.7, $\begin{tikzcd} A^+ \arrow[r, "\varphi^+"] \arrow[d, "\pi_{\ker\varphi^+}"] & S \\ A^+/\ker\varphi^+ \arrow[ur, "\varphi^{+\prime}"'] \end{tikzcd}$ and hence

$$A^+/\ker\varphi^+ \cong \operatorname{im}\varphi^+ = S.$$

Thus, as expected, S is isomorphic to a quotient of a free semigroup.

Instead of choosing a semigroup S and knowing that it is a quotient of a free semigroup, we can start with a free semigroup and impose a congruence σ on it to obtain the quotient semigroup A^+/σ. This is the idea of semigroup presentations, which we shall discuss next, but first we have a lemma which will be uselful later in the discussion of presentations.

Lemma 2.2.11. *For any $\rho \in \mathfrak{B}(S)$, we have*

$$\rho^c = \{(pxq, pyq) \in S \times S : p, q \in S^1,\ (x, y) \in \rho\}.$$

Proof. Let

$$\sigma = \{(pxq, pyq) \in S \times S : p, q \in S^1,\ (x, y) \in \rho\}.$$

To prove $\sigma = \rho^c$, 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. Therefore $\sigma = \rho^c$. □

2.2.4. Presentations

Now we introduce the idea of a semigroup presentation which, as mentioned previously, is to define a semigroup as a quotient of a free semigroup, that is, as A^+/σ for some congruence σ on the free semigroup A^+.
By Proposition 2.2.10, 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 which generates σ.

Definition 2.2.10 (Semigroup presentation). 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 $A^+/\rho^\#$, where $\rho^\#$ is the congruence generated by ρ.

If both A and ρ are finite, then the presentation is said to be *finite*, and the semigroup presented by it is said to be *finitely presented.*
The elements of ρ are called *defining relations.* We think of the semigroup presented by $\langle A \mid \rho \rangle$ as the largest semigroup generated by A and satisfying the defining relations in ρ.
If $S = \langle A \mid \rho \rangle$, we view words in A^+ as representing elements of S. In particular, A represents a generating set for S.
In general, an element of S may have different representatives in A^+. If $u, v \in A^+$ represent the same element of S, that is, if $(u, v) \in \rho^\#$, we write

$$u =_S v.$$

Definition 2.2.11. An elementary $\rho-$*transition* is a pair $(u, v) \in (\rho^S)^c$. Thus, by Lemma 2.2.11, (u, v) is an elementary ρ-transition if and only if v can be obtained from u by substituting a subword y for a subword x of u, where $(x, y) \in \rho$ or $(y, x) \in \rho$.

Proposition 2.2.12. *Let S be presented by $\langle A \mid \rho \rangle$. Then $u =_S v$ if and only if there is a sequence*

$$u = u_0, u_1, \dots, u_m = v$$

in A^+ such that each pair (u_i, u_{i+1}) is an elementary ρ-transition.

Proof. First of all, notice that

$$
\begin{aligned}
& u =_S v \\
\iff & (u, v) \in \rho^{\#} \\
\iff & (u, v) \in (\rho^c)^e \\
\iff & (u, v) \in (((\rho^c)^R)^S)^\infty \\
\iff & (u, v) \in (\rho^c \cup (\rho^c)^{-1} \cup id_{A^+})^\infty \\
\iff & (u, v) \in \bigcup_{n=1}^{\infty} (\rho^c \cup (\rho^c)^{-1} \cup id_{A^+})^n \\
\iff & (\exists\, n \in \mathbb{N})\, ((u, v) \in (\rho^c \cup (\rho^c)^{-1} \cup id_{A^+})^n) \\
\iff & (\exists\, n \in \mathbb{N}) \text{ and } (u = u_0, \dots, u_n = v)\, ((u_i, u_{i+1}) \in (\rho^c \cup (\rho^c)^{-1} \cup id_{A^+})).
\end{aligned}
$$

Hence $u =_S v$ if and only if there is a sequence $u_0, \dots, u_n$ 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 such a sequence consisting entirely of *elementary ρ-transitions.* □

When there is a sequence of elementary ρ-transitions from u to v, we say that (u, v) is a *consequence* of ρ, or that $u =_S v$ can be deduced from the defining relations.

Definition 2.2.12 (Monoid presentation). The analogous discussion applies to monoids. A monoid M is free on A if and only if $M \cong A^*$. As for semigroups, every monoid is a quotient of a free monoid.
A monoid presentation $\langle A \mid \rho \rangle$ consists of an alphabet A and a binary relation ρ on A^*, and presents a monoid isomorphic to $A^*/\rho^{\#}$.

In a monoid presentation $\langle A \mid \rho \rangle$, the defining relations may involve the empty word ε. Thus relations in ρ may be of the form (u, ε) or (ε, u).
If $M = \langle A \mid \rho \rangle$, then, for $u, v \in A^*$, $u =_M v$ if and only if there is a sequence of elementary ρ-transitions from u to v.

Proposition 2.2.13. *Suppose S is finitely presented and that $\langle A \mid \rho \rangle$ is a presentation for S. Then there exist $B \subseteq A$ and $\sigma \subseteq \rho$ such that $\langle B \mid \sigma \rangle$ is a finite presentation for S.*

Remark 2.2.13. The presentation $\langle A \mid \emptyset \rangle$, where there are no defining relations, defines the free semigroup A^+.
Indeed, there are no non-trivial consequences of defining relations, and so all words over A represent different elements of the semigroup by Proposition 2.2.10. Alternatively, we may note that $\emptyset^{\#} = id_{A^+}$ and hence $A^+/id_{A^+} \cong A^+$.

Example 2.2.14. (a) The presentation $\langle a \mid \{(a^2, a)\} \rangle$ defines a trivial semigroup, since $a^n = a$ is the consequence of the defining relation.

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

(c) Let M be a monoid presented by $\langle a, b \mid (ab, ba) \rangle$. Then every element of M is of the form $a^i b^j$. So $M \cong (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\})$.

Definition 2.2.15 (Bicyclic monoid). 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 $c^\alpha b^\beta$, where $\alpha, \beta \in \mathbb{N} \cup \{0\}$, because if we have a word $w \in \{b, c\}^*$ that contains a subword bc, we can replace bc by ε. This process must end with a word that does not contain bc; that is, a word $c^\alpha b^\beta$. In fact, each element is represented by a unique word of this form.

Example 2.2.16. Let $X = \{xyz, yz, yt, xy, zy, zt\} \subseteq \{x, y, z, t\}^+$ and let S be the subsemigroup of $\{x, y, z, t\}^+$ generated by X.
Let $A = \{a, b, c, d, e, f\}$ and $\varphi : A^+ \to S$ such that

$$a\varphi = xyz, b\varphi = yz, c\varphi = yt,$$
$$d\varphi = xy, e\varphi = zy, \text{ and } f\varphi = zt.$$

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

$$(ab^\alpha c)\varphi = (a\varphi)(b\varphi)^\alpha(c\varphi) = (xyz)(yz)^\alpha(yt) = x(yz)^{\alpha+1}yt = xy(zy)^\alpha t = (de^\alpha f)\varphi.$$

Hence, if $\langle A \mid \rho\rangle$ is a presentation for S, then $\rho^\#$ must contain the relation $(ab^\alpha c, de^\alpha f)$, for every $\alpha \in \mathbb{N} \cup \{0\}$.
Then 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 αc is the unique word representing $(\alpha c)\varphi = y(zy)^\alpha t$.
Hence, in an elementary sequence of ρ-transitions from $ab^\alpha c$ to $de^\alpha f$, the first must involve a defining relation from ρ, whose one side is $ab^\alpha c$. Thus ρ must contain infinitely many defining relations. Hence S is finitely generated, but not finitely presented.

The above example shows that a semigroup might be finitely generated but not finitely presented.

Example 2.2.17. Let $A = \{a, b, c, d, e, f, g, h\}$ and let $\rho = \{(ab, ba), (cf, de), (dg, ch)\}$.
Let S be the semigroup presented by $\langle A \mid \rho\rangle$.
Now suppose that $cu =_S cv$. Then there is an elementary ρ-transition sequence $cu = w_0, w_1, \ldots, w_n = cv$.
Without loss of generality, we may assume that n be minimal among all such sequences.
Assume that c is altered at some step in this sequence. Then this step must involve applying one of the defining relations (cf, de) or (dg, ch). Assume the former (latter is similar), then for some i, $w_i = cfw'$ and $w_{i+1} = dew'$.
Now, no defining relation begins with the symbol e, then e must occur in the terms of the sequence until the relation (cf, de) is applied again (as 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 the (cf, de) twice. That is, there is a shorter sequence of elementary ρ-transitions from cu to cv, a contradiction to the minimality of n. Hence the initial symbol c is never altered. Thus we can delete the initial symbol c from each step in the sequence, and so $u \equiv_S v$.
Reasoning in this way for every symbol in A shows that S is left cancellative. Similarly, 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

$$\begin{aligned}
(ag)\varphi &= (a\varphi)(g\varphi) \\
&= (a\varphi)(e\varphi)(e\varphi)^{-1}(g\varphi) \\
&= (b\varphi)(f\varphi)(e\varphi)^{-1}(g\varphi) \quad (asae =_S bf) \\
&= (b\varphi)(c\varphi)^{-1}(c\varphi)(f\varphi)(e\varphi)^{-1}(g\varphi) \\
&= (b\varphi)(c\varphi)^{-1}(d\varphi)(e\varphi)(e\varphi)^{-1}(g\varphi) \quad (ascf =_S de) \\
&= (b\varphi)(c\varphi)^{-1}(d\varphi)(g\varphi) \\
&= (b\varphi)(c\varphi)^{-1}(c\varphi)(h\varphi) \quad (asdg =_S ch) \\
&= (b\varphi)(h\varphi) \\
&= (bh)\varphi
\end{aligned}$$

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

This example shows that cancellativity is not sufficient condition for group embeddability.

3. Green's Relations and Basic Structure

3.1. Green's equivalences

Green's relations, first studied by J. A. Green, are one of the fundamental concepts in semigroup theory. They help us understand the structure of a semigroup.

3.1.1. Introduction

As already introduced, we denote the semigroup S^1 by $S \cup \{1\}$ if S has no identity, and S otherwise. For any $a \in S$, aS^1 is the right ideal generated by a, and S^1a is the left ideal generated by a. The smallest left ideal of S containing a is $S^1a = Sa \cup \{a\}$, and similarly for the right ideal.
We define an equivalence $\mathscr{L}$ on S by the rule that $a\mathscr{L}b$ if and only if $S^1a = S^1b$, that is, if a and b generate the same left ideal. Similarly, we define $\mathscr{R}$ by the rule that $a\mathscr{R}b$ if and only if $aS^1 = bS^1$.

Proposition 3.1.1. *Let S be a semigroup and $a, b \in S$. Then $a\mathscr{L}b$ if and only if there exist $x, y \in S^1$ such that $xa = b$ and $yb = a$. Also, $a\mathscr{R}b$ if and only if there exist $u, v \in S^1$ such that $au = b$ and $bv = a$.*

Another immediate property of $\mathscr{L}$ and $\mathscr{R}$ is:

Proposition 3.1.2. *$\mathscr{L}$ is a right congruence and $\mathscr{R}$ is a left congruence.*

We denote the intersection of $\mathscr{L}$ and $\mathscr{R}$ by $\mathscr{H}$. That is, $\mathscr{H} = \mathscr{L} \cap \mathscr{R}$, which is again an equivalence. The smallest equivalence relation which contains both $\mathscr{L}$ and $\mathscr{R}$ is denoted by $\mathscr{D}$. That is,

$$\mathscr{D} = \mathscr{L} \vee \mathscr{R}.$$

To make the relation easier to use, we have the following lemma.

Lemma 3.1.3. *The relations $\mathscr{L}$ and $\mathscr{R}$ commutes; that is,*

$$\mathscr{L} \circ \mathscr{R} = \mathscr{R} \circ \mathscr{L}.$$

Proof. Let S be a semigroup, let $a, b \in S$, and suppose that $(a, b) \in \mathscr{L} \circ \mathscr{R}$. Then there exists $c \in S$ such that $a\mathscr{L}c$ and $c\mathscr{R}b$. That is, there exist $x, y, u, v \in S^1$ such that

$$\begin{aligned} xa &= c, \qquad & cu &= b, \\ yc &= a, \qquad & bv &= c. \end{aligned}$$

If we now write d for the element ycu of S, we see that

$$au = ycu = d, \qquad dv = ycuv = ybv = yc = a;$$

hence $a\mathscr{R}d$. Also,

$$yb = ycu = d, \qquad xd = xycu = xau = cu = b,$$

and so $d\mathscr{L}b$. We deduce that $(a, b) \in \mathscr{R} \circ \mathscr{L}$.
We have shown that $\mathscr{L} \circ \mathscr{R} \subseteq \mathscr{R} \circ \mathscr{L}$; the reverse inclusion follows in a similar way. □

Then, it follows from Proposition 1.1.12 that

$$\mathscr{D} = \mathscr{L} \circ \mathscr{R} = \mathscr{R} \circ \mathscr{L} = \mathscr{L} \vee \mathscr{R}.$$

Finally, the relation $\mathscr{J}$ is defined by $a\mathscr{J}b$ if and only if

$$S^1aS^1 = S^1bS^1,$$

that is, if a and b generate the same principal two-sided ideal.
As for $\mathscr{L}$ and $\mathscr{R}$, we have the following immediate property of $\mathscr{J}$:

Proposition 3.1.4. *Let S be a semigroup and $a, b \in S$. Then $a\mathscr{J}b$ if and only if there exist $x, y, u, v \in S^1$ such that $axy = b$ and $ubv = a$.*

Notice that $\mathscr{L} \subseteq \mathscr{J}$ and $\mathscr{R} \subseteq \mathscr{J}$. Since $\mathscr{D}$ is the smallest equivalence containing both $\mathscr{L}$ and $\mathscr{R}$, $\mathscr{D} \subseteq \mathscr{J}$.
On a group G, we have

$$\mathscr{H} = \mathscr{L} = \mathscr{R} = \mathscr{D} = \mathscr{J} = G \times G.$$

And on a commutative semigroup,

$$\mathscr{H} = \mathscr{L} = \mathscr{R} = \mathscr{D} = \mathscr{J}.$$

Proposition 3.1.5. *In a periodic semigroup, $\mathscr{J}$ and $\mathscr{D}$ coincide.*

Proof. We only need to show one side of inclusion.
Suppose that $a, b \in S$ are such that $a\mathscr{J}b$. Then there exist $x, y, u, v \in S^1$ such that $xay = b$ and $ubv = a$.
To prove the desired result we need to find an element c in S such that $a\mathscr{L}c$, $c\mathscr{R}b$. It follows easily from the equations above that
$a = (ux)a(yv) = (ux)^2a(yv)^2 = (ux)^3a(yv)^3 = \cdots$.
$b = (xu)b(vy) = (xu)^2b(vy)^2 = (xu)^3b(vy)^3 = \cdots$.
Since S is periodic we can find an m for which $(ux)^m$ is idempotent. Then, if we let $c = xa$, we find that
$a = (ux)^m a(yv)^m = (ux)^m(ux)^m a(yv)^m = (ux)^m a = (ux)^{m-1}uxa = (ux)^{m-1}uc$,
and so $a\mathscr{L}c$. Also, $cy = xay = b$, and if we choose n so that $(vy)^n$ is idempotent, we have

$$\begin{aligned} c = xa &= x(ux)^{n+1}a(yv)^{n+1} = (xu)^{n+1}xay(vy)^n v \\ &= (xu)^{n+1}b(vy)^{2n}v = (xu)^{n+1}b(vy)^{n+1}(vy)^{n-1}v \\ &= b(vy)^{n-1}v. \end{aligned}$$

Hence $c\mathscr{R}b$ as required. □

The $\mathscr{L}$-class, $\mathscr{R}$-class, $\mathscr{D}$-class, and $\mathscr{J}$-class containing the element a will be denoted by L_a, R_a, D_a, and J_a, respectively.
Since $\mathscr{L}$, $\mathscr{R}$, and $\mathscr{J}$ are defined in terms of the ideals, the inclusion order among these ideals induces a partial order among the corresponding equivalence classes as;

$$L_a \leq L_b \iff S^1 a \subseteq S^1 b,$$

$$R_a \leq R_b \iff aS^1 \subseteq bS^1,$$

$$J_a \leq J_b \iff S^1 a S^1 \subseteq S^1 b S^1.$$

Thus, we may regard $S/\mathscr{L}$, $S/\mathscr{R}$, and $S/\mathscr{J}$ as posets.
Immediately from the above definitions, for $a \in S$ and $x, y \in S^1$,

$$L_{xa} \leq L_a, \qquad R_{ax} \leq R_a.$$

We shall say that a semigroup S satisfies the conditions $\min_L$, $\min_R$, $\min_J$, accordingly as the minimum condition is satisfied by the POSets $S/\mathscr{L}$, $S/\mathscr{R}$, and $S/\mathscr{J}$.

Proposition 3.1.6. *If S is a semigroup satisfying $\min_L$ and $\min_R$, then $\mathscr{D} = \mathscr{J}$.*

Proof. Suppose that S satisfies $\min_{\mathscr{L}}$ and $\min_{\mathscr{R}}$. Then so also does S^1, for S^1 has exactly the same principal left and right ideals as S, except (in the case where $S^1 \neq S$) for S^1 itself. So we may assume that S has an identity element.
Suppose now that $a\mathscr{J}b$, so that there exist $p, q, r, s \in S$ such that $paq = b$, $rbs = a$.
It follows that the set $X = \{x \in S : (\exists y \in S)\, xay = b\}$ is non-empty, and hence so also is the subset $\Lambda = \{L_x : x \in X\}$ of $S/\mathscr{L}$. The condition $\min_{\mathscr{L}}$ allows us to select a minimal element L_u in Λ, and we can then choose an element v in S such that $uav = b$.
Now $uruavsv = b$, and so $L_{uru} \in \Lambda$. Then, we have $L_{uru} \leq L_u$, and it then follows by the minimality of L_u in Λ that $L_u = L_{uru} \leq L_{ru} \leq L_u$.
Hence $ru\mathscr{L}u$. By Proposition 3.1.2 it follows that $ruav\mathscr{L}uav$, that is, $rb\mathscr{L}b$.
A similar argument using the condition $\min_{\mathscr{R}}$ establishes that $bs\mathscr{R}b$, and then by Proposition 3.1.2 we deduce that $rbs\mathscr{R}rb$. We thus have $a\mathscr{R}rb$, $rb\mathscr{L}b$, which implies $a\mathscr{R} \circ \mathscr{L}b$, and so $a\mathscr{D}b$ as required. □

3.1.2. The structure of D-classes

Each $\mathscr{D}$-class in a semigroup S is a union of $\mathscr{L}$-classes and also a union of $\mathscr{R}$-classes. The intersection of an $\mathscr{L}$-class and an $\mathscr{R}$-class is either empty or is an $\mathscr{H}$-class. Hence, by the definition of $\mathscr{D}$,

$$a\mathscr{D}b \iff R_a \cap L_b \neq \emptyset \iff L_a \cap R_b \neq \emptyset.$$

We visualize a $\mathscr{D}$-class in a table, from which each row represents an $\mathscr{R}$-class, each column represents an $\mathscr{L}$-class, and each cell represents an $\mathscr{H}$-class, usually called as eggbox.

Remark 3.1.1. Let D be a $\mathscr{D}$-class in a semigroup S, and let $a, b \in D$ are such that $a\mathscr{R}b$ (so a and b are in the same row of eggbox), then by definition, of $\mathscr{R}$ there exist $s, s' \in S^1$ such that

$$as = b, \qquad bs' = a.$$

The right translation $\rho_s : S \to S$ such that $x\rho_s = xs$, thus maps a to b. It, in fact, maps L_a to L_b; for if $x \in L_a$ then $xs\mathscr{L}as$ by proposition 3.1.2, and so $xs \in L_a s = L_b$. Similarly, $\rho_{s'}$ maps L_b to L_a.
Now if we consider the composition $\rho_s\rho_{s'} : L_a \to L_a$, we have for $x = ua \in L_a$

$$x\rho_s\rho_{s'} = uass' = ubs' = ua = x.$$

Thus, $\rho_s\rho_{s'}$ is identity map of L_a.
Similarly, $\rho_{s'}\rho_s$ is the identity map of L_b. Consequently, we deduce that $\rho|_{L_a}$ and $\rho|_{L_b}$ are mutually inverse bijections from L_a onto L_b and L_b onto L_a, respectively.
In fact, if $x \in L_a$, then $y = x\rho_s \in L_b$ has the property that $y = xs$ and $x = ys'$. Thus, $x\mathscr{R}y$ ans so the map ρ_s is $\mathscr{R}-$class preserving. It maps each $\mathscr{H}$-class in L_a in a one-one manner onto the corresponding ($\mathscr{R}$ equivalent) $\mathscr{H}$-class in L_b. Similar remark apply to $\rho_{s'}$.
To summarise, we have the following result:

Lemma 3.1.7 (Green's lemma). *Let a, b be $\mathscr{R}$-equivalent elements in a semigroup S, and let $s, s' \in S^1$ be such that*

$$as = b, \qquad bs' = a.$$

Then the right translations $\rho_s|_{L_a}$ and $\rho_{s'}|_{L_b}$ are mutually inverse $\mathscr{R}$-class preserving bijections from L_a onto L_b and from L_b onto L_a, respectively.

Similarly, for a, b belonging to the same $\mathscr{L}$-class, the left translations $\lambda_s|_{R_a}$ and $\lambda_{s'}|_{R_b}$ are mutually inverse bijections preserving $\mathscr{L}$-classes from R_a onto R_b and from R_b onto R_a, respectively. We have the corresponding result as follows (also known as Green's Lemma):

Lemma 3.1.8. *Let a, b be $\mathscr{L}$-equivalent elements in S, and let $t, t' \in S^1$ be such that*

$$ta = b, \qquad t'b = a.$$

Then the left translations $\lambda_t|_{R_a}$ and $\lambda_{t'}|_{R_b}$ are mutually inverse L-class preserving bijections from R_a onto R_b and from R_b onto R_a, respectively.

The combined effect of these two lemmas is as follows;

Lemma 3.1.9. *If a, b are $\mathscr{D}$-equivalent elements in a semigroup S, then $|H_a| = |H_b|$.*

Proof. Let c be such that $a\mathscr{R}c$ and $c\mathscr{L}b$, with $as = c$, $cs' = a$, $tc = b$, $t'b = c$.
Then by the preceding lemmas $\rho_s|_{H_a}$ is a bijection onto H_c and $\lambda_t|_{H_c}$ is a bijection onto H_b. Thus $\rho_s\lambda_t : x \mapsto txs$ is a bijection from H_a onto H_b (with inverse $\lambda_{t'}\rho_{s'} : y \mapsto t'ys'$), and it follows that $|H_a| = |H_b|$. □

We have seen that if $as\mathscr{R}a$, then $x \mapsto xs$ is a bijection from H_a onto H_{as}. So, in particular, if $as\mathscr{H}a$ then $x \mapsto xs$ is a bijection of H_a onto itself. This, together with the dual argument, gives

Lemma 3.1.10. *Let x, y be elements of a semigroup S. If $xy \in H_x$ then $\rho_y|_{H_x}$ is a bijection of H_x onto itself. If $xy \in H_y$ then $\lambda_x|_{H_y}$ is a bijection of H_y onto itself.*

Then we have the following result, usually called Green's Theorem:

Theorem 3.1.11 (Green's Theorem). *If H is an $\mathscr{H}$-class in a semigroup S then either $H^2 \cap H = \emptyset$ or $H^2 = H$ and H is a subgroup of S.*

Proof. Suppose $H^2 \cap H \neq \emptyset$, so that there exist a, b in H such that $ab \in H$. By the lemma, ρ_b and λ_a are bijections of H onto itself. Hence $hb \in H$ and $ah \in H$ for every h in H. Again by the lemma, it follows that λ_h and ρ_h are bijections of H onto itself. Hence $Hh = hH = H$ for every h in H. Certainly $H^2 = H$, and it follows from that H is a subgroup of S. □

Corollary 3.1.12. *If e is an idempotent in a semigroup S, then H_e is a subgroup of S. No $\mathscr{H}$-class in S can contain more than one idempotent.*

3.1.3. Regular $\mathscr{D}$-classes

Definition 3.1.2. Let S be a semigroup and let $a \in S$. Then a is said to be *regular* if $\exists\ x \in S$ such that $axa = a$. The semigroup S is called *regular* if all of its elements are regular.

If a is a regular element with $axa = a$, and $b\mathscr{L}a$, then by definition, $\exists u, v \in S^1$ such that $ua = b$, $vb = a$, and so

$$b = ua = uaxa = bxa = b(xv)b.$$

Hence b is also regular.
Similarly, if a is regular with $axa = a$, and $b\mathscr{R}a$, then $\exists u, v \in S^1$ such that $au = b$, $av = a$, and so

$$b = au = axau = axb = b(vx)b.$$

Hence b is again regular.

Proposition 3.1.13. *If a is a regular element of a semigroup S, then every element of D_a is regular.*

Thus, if D is a $\mathscr{D}$-class, then either all of the elements of D are regular or no element of D is regular.
If all of elements of D are regular then we call it regular; otherwide irregular.
Again, if e is an idempotent, then since $e = eee$, e is regular. It follows that if a $\mathscr{D}$-class contains an idempotent then it is regular. The converse is also true: every regular $\mathscr{D}$-class must contain atleast one idempotent. In fact, we have the following generalised result:

Proposition 3.1.14. *In a regular $\mathscr{D}$-class, each $\mathscr{L}$-class and each $\mathscr{R}$-class contains an idempotent.*

Proof. If a is a member of a regular $\mathscr{D}$-class, and $xax = a$, then xa is idempotent and $xa\mathscr{R}a$, while ax is idempotent and $ax\mathscr{L}a$. □

Proposition 3.1.15. *Every idempotent e in a semigroup S is a right identity for L_e and a left identity for R_e.*

Proof. If $a\mathscr{L}e$, then $a = xe$ for some $x \in S^1$, and so

$$ae = (xe)e = xe^2 = xe = a.$$

Similarly, if $b\mathscr{R}e$, then $b = ex$ for some $x \in S^1$, and so

$$eb = e(ex) = e^2x = ex = b.$$

□

Definition 3.1.3 (Inverse element). Let S be a semigroup and $a \in S$. We say that a' is an *inverse* of a if $aa'a = a$ and $a'aa' = a'$.

Remark 3.1.4. Every element with an inverse is regular. In fact, every regular element has an inverse. To see this, let a be a regular element with $axa = a$, then define $a' = xax$. So we have a' is an inverse of a. Indeed, $aa'a = a(xax)a = (axa)xa = axa = a$, and $a'aa' = (xax)a(xax) = x(axa)xax = x(axa)x = xax = a'$.

Remark 3.1.5. An element may have more than one inverse. For example, in a rectangular band every element is an inverse of every other element.

We shall denote the set of inverses of an element a by $V(a)$.
Now, notice that if a is an element of a regular $\mathscr{D}$-class D, then every inverse a' of a must lie in D, as $a\mathscr{R}aa'$ and $a\mathscr{L}a'a$.

	L_a	$L_{a'}$
R_a	a	aa'
$R_{a'}$	$a'a$	a'

We have proved part of the following theorem:

Theorem 3.1.16. *Let a' be an element of a regular $\mathscr{D}$-class D in a semigroup S.*

(1) If $a' \in V(a)$, then $a' \in D$ and the two $\mathscr{H}$-classes $R_a \cap L_{a'}$, $L_a \cap R_{a'}$ contain the idempotents aa' and $a'a$, respectively.

(2) If $b \in D$ is such that $R_a \cap L_b$ and $L_a \cap R_b$ contain idempotents e and f, respectively, then H_b contains an inverse a^* of a such that $aa^* = e$, $a^*a = f$.

(3) No $\mathscr{H}$-class contains more than one inverse of a.

Proof. It remains to establish the second and third parts.

	L_a	L_b
R_a	a	e
R_b	f	a^*, b

To prove (2), notice that from $a\mathscr{R}e$ it follows by Proposition 3.1.15 that $ea = a$. Similarly, from $a\mathscr{L}f$ it follows that $af = a$. Again from $a\mathscr{R}e$ it follows that there exists x in S^1 such that $ax = e$. Let $a^* = fxe$. Then

$$aa^*a = (af)x(ea) = axa = ea = a,$$
$$a^*aa^* = fx(eaf)xe = fx(ax)e = fxe^2 = fxe = a^*,$$

and so $a^* \in V(a)$. Also

$$aa^* = (af)xe = (ax)e = e^2 = e.$$

Further, since $a\mathscr{L}f$, there exists y in S^1 such that $ya = f$. Hence

$$a^*a = fxea = fxa = yaxa = yea = ya = f.$$

It now follows easily that

$$a^* \in L_e \cap L_f = L_b \cap R_b = H_b.$$

To prove part (3), suppose that both a' and a^* are inverses of a inside the single $\mathscr{H}$-class H_b. It follows that both aa' and aa^* are idempotents in the $\mathscr{H}$-class $R_a \cap L_b$. Hence $aa' = aa^*$ by Corollary 3.1.12. Similarly,

$$a'a = a^*a,$$

and it now follows that

$$a^* = a^*aa^* = a^*aa' = a'aa' = a'.$$

□

We have the following easy consequence of the above theorem:

Proposition 3.1.17. *Let e, f be idempotents in a semigroup S. Then $(e, f) \in \mathscr{D}$ if and only if there exists $a \in S$ and an inverse a' of a such that $aa' = e$, $a'a = f$.*

Proof. Suppose first that $(e, f) \in \mathscr{D}$. Then e and f are members of the same regular $\mathscr{D}$-class.

$$\begin{array}{c|cc} & L_f & L_e \\ \hline R_e & a & e \\ R_f & f & a' \end{array}$$

Let $a \in R_e \cap L_f$. Then by Theorem 3.1.16(2) there is an inverse a' of a in $R_f \cap L_e$ such that

$$aa' = e, \qquad a'a = f.$$

Conversely, if there exist mutually inverse elements a, a' such that

$$aa' = e, \qquad a'a = f,$$

then from Theorem 3.1.16(1) it follows that $e\mathscr{R}a$, $a\mathscr{L}f$. Hence $e\mathscr{D}f$ as required. □

Proposition 3.1.18. *If H and K are two group $\mathscr{H}$-classes in the same regular $\mathscr{D}$-class, then H and K are isomorphic.*

Proof. The method of proof is essentially that used in the proof of Lemma 3.1.9, with a careful (yet obvious) choice of translation maps. Suppose that $H = H_e$ and $K = H_f$, where e, f are idempotents and are, respectively, the identities of the groups H_e and H_f.

$$\begin{array}{c|cc} & L_e & L_f \\ \hline R_e & e & a \\ R_f & a' & f \end{array}$$

Let $a \in R_e \cap L_f$ (which is non-empty since $e\mathscr{D}f$ by assumption); then by Theorem 3.1.16 there is a unique inverse a' of a in $L_e \cap R_f$, and we have

$$aa' = e, \qquad a'a = f, \qquad ea = af = a, \qquad a'e = fa' = a'.$$

By Green's Lemmas (3.1.7 and 3.1.8) it follows that $\rho_a|_{H_e}$ is a bijection from H_e onto H_a and $\lambda_{a'}|_{H_a}$ is a bijection from H_a onto H_f. Thus the map $\phi = \rho_a\lambda_{a'}$ given by

$$x\phi = a'xa \qquad (x \in H_e)$$

is a bijection from H_e onto H_f, with inverse given by

$$y\phi^{-1} = aya' \qquad (y \in H_f).$$

The bijection ϕ is even an isomorphism, for if $x_1, x_2 \in H_e$ then

$$(x_1\phi)(x_2\phi) = a'x_1aa'x_2a = a'x_1ex_2a = a'(x_1x_2)a = (x_1x_2)\phi,$$

since e is the identity element of the group H_e. □

We have a final result to conclude the section:

Proposition 3.1.19. *Let $a, b \in D$, where D is a $\mathscr{D}$-class. Then $ab \in R_a \cap L_b$ if and only if $L_a \cap R_b$ contains an idempotent.*

Proof. Suppose first that $ab \in R_a \cap L_b$. Then there exists c such that $abc = a$, and by Green's Lemma 3.1.7 the right translation

$$\rho_c : x \mapsto xc$$

maps H_b onto $L_a \cap R_b$. Thus in particular $bc \in L_a \cap R_b$. The translation

$$\rho_b : y \mapsto yb$$

maps $L_a \cap R_b$ onto H_b, and is the inverse of ρ_c, and it then follows that bc is idempotent, since

$$(bc)^2 = b\rho_c\rho_b\rho_c = b\rho_c = bc.$$

Conversely, suppose that $L_a \cap R_b$ contains an idempotent e. Then $eb = b$ by Proposition 3.1.15, and hence the translation $x \mapsto xb$ maps H_a onto $R_a \cap L_b$. In particular, $ab \in R_a \cap L_b$. □

3.2. Simple and 0-Simple Semigroups

Definition 3.2.1. Let S be a semigroup with zero. If, for all $x, y \in S$, $xy = 0$, then S is called as null semigroup. That is, $S^2 = \{0\}$.

Definition 3.2.2. A semigroup is simple if it contains no proper ideals. A semigroup with 0 is 0-simple if it is not null and its only proper ideal is $\{0\}$.

Definition 3.2.3. An ideal of a simple 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 3.2.1. *A semigroup contains at most one minimal ideal.*

Proof. 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 $I = J$. □

A semigroup might not contain a minimal ideal. But if a semigroup contains one then it is unique, by above proposition. Such a unique minimal ideal is called kernel and is denoted as $K(S)$. Clearly, if S is a semigroup with zero, then $K(S) = \{0\}$.

Remark 3.2.4. Clearly, S is simple if and only if $\mathscr{J} = S \times S$. The corresponding criterion for 0-simplicity is that $S^2 \neq \{0\}$ and that $\{0\}$ and $S \setminus \{0\}$ are only $\mathscr{J}$-classes.

A simple semigroup can be made into a 0-semigroup by adjoining a zero element. However the zero element of a 0-simple semigroup cannot be removed, in general, to get a simple semigroup. But if 0 is a prime element of S in the sense that

$$(ab = 0) \Rightarrow (a = 0 \text{ or } b = 0),$$

then 0 can be removed. The condition is also familiar in ring theory for a ring to be an integral domain. So, above condition can be expressed by saying that if S has no proper zero divisors.

Proposition 3.2.2. *A semigroup S is 0-simple if and only if $SxS = S$ for all $x \in S \setminus \{0\}$.*

Proof. 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 $S^3 = S^2 S = SS = S$.
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 see 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. □

Corollary 3.2.3. *A semigroup S is simple if $SxS = S$ for all $x \in S$.*

Proposition 3.2.4. *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. 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 $S^1 x S^1$ is an ideal of S contained in I. Since $x \in S^1 x S^1$, we have $S^1 x S^1 \neq \{0\}$; hence $S^1 x S^1 = I$ since I is 0-minimal. Hence $I = I^3 = IS^1 x S^1 I \subseteq IxI \subseteq I$. Hence $IxI = I$ for all $x \in I - \{0\}$ and so I is 0-simple by Proposition 3.2.2. □

For any $x \in S$, recall that the principal ideal $J(x) = S^1 x S^1$. Also, the $\mathcal{J}$-class of x, J_x, is the set of all the elements of S that generate $J(x)$. Let $I(x) = J(x) - J_x$. Notice that $I(x) = \{y \in S : J_y \subseteq J_x\}$.

Lemma 3.2.5. *$I(x)$ is empty or an ideal of S.*

Proof. Suppose $I(x) \neq \emptyset$. 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. □

Definition 3.2.5. The factor semigroups $J(x)/I(x)$, where x is such that $I(x) \neq \emptyset$, and the kernel $K(S)$ are called *principal factors* of S.

Proposition 3.2.6. *Let S be a semigroup. If the kernel $K(S)$ exists, x is simple. All principal factors $J(x)/I(x)$ are either null or 0-simple.*

Proof. By Proposition 3.2.4(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 3.2.4(a). □

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

$$(K(S) = S_1 \subsetneq S_2 \subsetneq \cdots \subsetneq S_n = S)$$

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

Theorem 3.2.7 (Jordan–Holder Theorem). *Let S be a semigroup admitting a principal ideal series*

$$(K(S) = S_1 \subseteq S_2 \subseteq \cdots \subseteq S_n = S).$$

Then the factors S_{i+1}/S_i are, in some order, isomorphic to the principal factors of S.

4. Regular And Completely Regular Semigroups

Content to be added later

4.1. Completely Regular Semigroups

4.2. Clifford Semigroups

5. Inverse Semigroups

Contetn to be added later

5.1. Basic Theory

Part II.

Homological Methods and Acts

6. Acts Over Monoids

6.1. Basic Definition and Concepts

We have seen that the set $\mathscr{T}(A)$ of all transformations of a set A forms a monoid under the composition of mappings. If we write mappings on the left we get the product of $f, g : A \to A$ by the rule

$$(fg)(a) = f(g(a)) \quad \text{for all } a \in A.$$

Writing mappings on the right we get the product as

$$a(fg) = (af)g \quad \text{for all } a \in A.$$

In the first case the monoid $\mathscr{T}(A)$ will be denoted by $\mathscr{T}^l(A)$ and in the second case by $\mathscr{T}^r(A)$. Apparently there exists an anti-isomorphism between these monoids

$$\mathscr{T}^l(A) \to \mathscr{T}^r(A); \;\; f \to f; \;\; fg \to gf.$$

Definition 6.1.1. Let S be a semigroup and A be a set. A semigroup homomorphism

$$\psi : S \to \mathscr{T}^r(A)$$

is called a *representation* of S by transformations of A.

If S is a monoid and ψ is monoid homomorphism then ψ is called a *unitary representation* of S by transformations of A.
If ψ is anti-homomorphism then ψ is called a *anti-representation* of S by transformations of A.

6.1.1. Acts over Semigroups and Monoids

The idea of representing a mathematical object by another object that is better understood, at least in some respects, is very familiar in mathematics. A classical example is the representation of groups by invertible matrices. Another important development was the representation of associative rings by endomorphisms of abelian groups. In fact, a representation of a ring by endomorphisms of an abelian group naturally gives rise to a module over that ring, and conversely.
In a similar way, representing semigroups (monoids) by transformations of sets leads to the notion of acts over semigroups (monoids).
We recall the definition of an action.

Definition 6.1.2. Let S be a monoid and $A \neq \emptyset$ is a set, we have a mapping $\mu : A \times S \to A$ defined as $(a, s) \mapsto as := \mu(a, s)$, such that

(a) $a1 = a$ and

(b) $a(st) = (as)t$ for $a \in A,\ s, t \in S$.

We call A a *right S-act* or a *right act over S* and write A_S.

Informally, we say the μ define a right multiplication of elements from A by elements of S.
A left S-act is defined analogously and denoted by ${}_SA$.
S-Acts are also known by names such as S-sets, S-spaces, S-polygons, S-systems, transition systems, and S-automata.
Additionally, if S is a group then the name vector system has also been used.

Remark 6.1.3. If S is a semigroup without identity, then condition (a) is nullified. The definition amounts to the definition of a semigroup act A_S, as defined in an earlier chapter.

Remark 6.1.4. If S is a commutative monoid then left S-act and right S-act coincide. For if ${}_SA$ is a left S-act, then we may define right multiplication by elements of S by $a * s = sa$ for $a \in A,\ s \in S$.
Then $a * 1 = 1a = a$ for all $a \in A$ and $a * (s_1 s_2) = a * (s_2 s_1) = (s_2 s_1)a = s_2(s_1 a) = s_2(a * s_1) = (a * s_1) * s_2$.
In this case, we consider A as a S-S-biact since for all $s_1, s_2 \in S$ and $a \in A$, we have
$(s_1 a) * s_2 = s_2(s_1 a) = (s_2 s_1)a = (s_1 s_2)a = s_1(s_2 a) = s_1(a * s_2)$.
If S is a monoid then the opposite monoid S^{op} is defined by reversing the factors, $s \circ t = ts,\ s, t \in S$.
We shall mostly consider monoids and unitary acts over them. We have a result which says that every unitary representation by transformations in $\mathcal{T}^r(A)$ gives a right S-act and every unitary antirepresentation gives a left S-act. And if we consider the monoid $\mathcal{T}^l(A)$, then the terms left and right get interchanged in above description. We shall state it formally below.

Proposition 6.1.1. *Every unitary representation (antirepresentation) of a monoid S by transformations in $\mathcal{T}^r(A)$ gives a right S-act and every unitary antirepresentation gives a left S-act. Conversely, for every right(left) $S-$ act $A_S({}_SA)$ there is an associated representation (antirepresentation) of S by transformations in $\mathcal{T}^r(A)$.*
Every unitary representation (antirepresentation) of a monoid S by transformations in $\mathcal{T}^l(A)$ gives a left S-act and every unitary antirepresentation gives a right S-act. Conversely, for every left(right) $S-$ act ${}_SA(A_S)$ there is an associated representation (antirepresentation) of S by transformations in $\mathcal{T}^l(A)$.

Proof. Let $\psi : S \to \mathcal{T}^r(A)$ be a unitary representation of the monoid S by transformations of A, define $\mu : A \times S \to A$ by

$$\mu(a, s) = a\psi(s).$$

Then, using the fact that ψ is a homomorphism, we get

(a) $a1 = a\psi(1) = a\,\mathrm{id}_A = a$.

(b) $a(st) = a\psi(st) = (a\psi(s))\psi(t) = (as)\psi(t) = (as)t$.

Conversely, if A_S is a right S-act, i.e. we have $\mu : A \times S \to A$ with properties (a) and (b) above, we define $\psi : S \to \mathcal{T}^1(A)$ by

$$s \mapsto \mu(-, s) : a \mapsto as.$$

That is, if we define $\sigma_s : A \to A$ by $a\sigma_s = as$, then, it is easy to see that $\sigma_s \in \mathcal{T}^r(A)$, and we have, $\psi(s) = \sigma_s$.
Clearly, $\psi(1) = \sigma_1 = \mathrm{id}_A$, and $a\sigma_{st} = a(st) = (as)t = (as)\sigma_t = (a\sigma_s)\sigma_t$. Thus, $\sigma_{st} = \sigma_s \circ \sigma_t = \sigma_s\sigma_t$.
Consequently, ψ is a homomorphism and hence a unitary representation of the monoid S by transformations in $\mathcal{T}^r(A)$.
Correspondingly alterations of this proof can be used to prove other cases as well. □

Definition 6.1.5. We say that an element $s \in S$ *acts injectively* on A_S if $as = a's$, $a, a' \in A_S$, implies $a = a'$. If every $s \in S$ acts injectively on A_S, then we say that S *acts injectively* on A_S.

Definition 6.1.6. We say that an element $s \in S$ *acts surjectively* on A_S if $A_S s = \{as \mid a \in A_S\} = A_S$. If every $s \in S$ acts surjectively on A_S, then we say that S *acts surjectively* on A_S.

Definition 6.1.7. We call A_S a *faithful* right S-act if, for $s, t \in S$, $as = at$ for all $a \in A$ implies $s = t$. We call A_S a *strongly faithful* S-act if, for $s, t \in S$, $as = at$ for some $a \in A$ implies $s = t$.

Remark 6.1.8. Every strongly faithful act is also faithful. The acts S_S and ${}_SS$ are always faithful since $1 \in S$ and they are strongly faithful if S is left or right cancellative, respectively.

Example 6.1.9. Let S be a monoid and K be a right ideal of S. Since $KS \subseteq K$, we have K is a right S-act and we write K_S. In particular, S_S (resp. ${}_SS$) is a right (resp. left) S-act and even a biact (${}_SS_S$). If R is a submonoid of S, then ${}_RS_R$ is an R-R-biact.

Example 6.1.10. Let $(K, +, \cdot)$ be a field and let V be a vector space over K. Then V is a left $(K, \cdot)$-act, but not a $(K, +)$-act.

Example 6.1.11. Take a left S-act ${}_SA$. Then $\mathscr{P}(A)$ turns into a left S-act by setting

$$\begin{aligned} \mu \ : & S \times \mathscr{P}(A) \to \mathscr{P}(A) \\ & (s, X) \mapsto sX = \{sx \mid x \in X\}, \end{aligned}$$

where $X \subseteq A$.

Remark 6.1.12. Let S be a semigroup without identity and A be a right S-act. Then, adjoining identity 1 to S to get S^1, we can turn A into a unitary right S^1-act by setting $a1 = a$ for all $a \in A$.

Definition 6.1.13. Let A_S be a right S-act. An element $\theta \in A_S$ is called a *zero* of A_S (a *fixed element*, a)*sink* if $\theta s = \theta$ for $s \in S$. i.e., $\{\theta\}$ is a one-element subact.

An act can have more than one zero.
If the monoid S has a left zero z, then $az \in A_S$ for $a \in A_S$ is a zero of A_S.

Remark 6.1.14. Every act A_S can be extended into an S-act with zero by taking the disjoint union $A_S \cup \{\theta\}$, where $\{\theta\}$ is the one-element act.

Definition 6.1.15. Let A_S be an S-act and $A' \subseteq A_S$ a non-empty subset. Then A' is called a *subact* of A_S if $a's \in A'$ for all $s \in S$ and $a' \in A'$.

Definition 6.1.16. We call A_S a *simple act* if it contains no subacts other than itself. A_S is called a 0-*simple act* if it contains no subacts other than A_S and one 1-element subact.

Clearly, one-element subact $\{\theta\}$ is simple.

6.1.2. Act Homomorphism and Act Congruence

Definition 6.1.17. Let A_S, B_S be two right S-acts. A mapping $f : A_S \to B_S$ is called a *homomorphism of right S-acts*, or just an *S-homomorphism*, if $f(as) = f(a)s$ for all $a \in A_S,\ s \in S$.

The set of all homomorphisms from A_S to B_S will be denoted by $\mathrm{Hom}(A_S, B_S)$ or by $\mathrm{Hom}_S(A, B)$.

Definition 6.1.18. Let ${}_SA, {}_SB$ be left S-acts and $f : {}_SA \to {}_SB$ be such that $(sa)f = s(af)$ for $a \in {}_SA,\ s \in S$. Then f is called a homomorphism of left S-acts (S-homomorphism).

The set of all S-homomorphisms from ${}_SA$ to ${}_SB$ is denoted by $\mathrm{Hom}({}_SA, {}_SB)$ or by $\mathrm{Hom}_S(A, B)$. The identity mapping $\mathrm{Id}_A : A_S \to A_S$ is a homomorphism of right S-acts. The same is true for left S-acts.

Definition 6.1.19. Let $f : A_S \to B_S$ be an S-homomorphism. If f is bijective, then it is called an *S-isomorphism*. In such a case, we say that A_S and B_S are *isomorphic*, and, symbolically, write $A_S \cong B_S$.

Remark 6.1.20. If $f : A_S \to B_S$ is an S-homomorphism then $\mathrm{im}\, f = f(A_S)$ is a subact of B_S.

Lemma 6.1.2. *Let $f \in \mathrm{Hom}(A_S, B_S)$ and $g \in \mathrm{Hom}(B_S, C_S)$, then the composition of f and g, $gf \in \mathrm{Hom}(A_S, C_S)$.*

Proof. Let $h = gf$, $a \in A_S$, $s \in S$. Then

$$h(as) = (gf)(as) = g(f(as)) = g(f(a)s) = (g(f(a)))s = ((gf)(a))s = h(a)s.$$

Thus, $h = gf \in \mathrm{Hom}(A_S, C_S)$. □

Lemma 6.1.3. *Let $f \in \mathrm{Hom}(A_S, B_S)$ be bijective. Then $f^{-1} \in \mathrm{Hom}(B_S, A_S)$, that is, the inverse of a bijective homomorphism of right S-acts is a homomorphism of right S-acts.*

Proof. Let $b \in B_S$, $s \in S$. Then

$$f(f^{-1}(bs)) = bs = f(f^{-1}(b))s.$$

Since f is injective (hence monomorphic and so left cancellative(as we are writing mappings on the right)), we get

$$f^{-1}(bs) = f^{-1}(b)s.$$

Consequently, $f^{-1} \in \mathrm{Hom}(B_S, A_S)$. □

Definition 6.1.21. Let A_S be an act.

- An endomorphism of A_S is an S-homomorphism from A_S to itself, i.e., an S-homomorphism of the type $f : A_S \to A_S$.
- An automorphism of A_S is a bijective endomorphism.

Remark 6.1.22.

- The set of all endomorphisms of A_S, $\mathrm{Hom}(A_S, A_S)$, forms a monoid under composition of mappings, and denoted by $\mathrm{End}(A_S)$ or sometimes simply by $\mathrm{End}\, A$, is called the endomorphism monoid of A_S.
- The set of all automorphisms of A_S, denoted by $\mathrm{Aut}(A_S)$ or sometimes simply by $\mathrm{Aut}\, A$, forms a group under composition of mappings and is called the automorphism monoid of A_S.

Definition 6.1.23 (Congruence). An equivalence relation ρ on A_S is called an *S-act congruence* or a *congruence* in A_S, if $a\rho a'$ implies $(as)\rho(a's)$ for $a, a' \in A_S,\ s \in S$.

If $X \subseteq A_S \times A_S$, then the smallest congruence in A_S containing X is denoted by $\rho(X)$.
A congruence ρ is *finitely generated* if there is a finite subset $X \subseteq A_S \times A_S$ such that $\rho = \rho(X)$.
A congruence is called *monogenic* if it is finitely generated by a single element $(x, y) \in A_S \times A_S$ and is denoted by $\rho(x, y)$.
Let ρ be a congruence and $A_S/\rho = \{[a]_\rho \mid a \in A\}$ be the factor set. Define a multiplication on the elements of A_S/ρ by the elements of S as

$$[a]_\rho s = [as]_\rho \text{ for every } s \in S.$$

From the property of an act congruence, this multiplication is well-defined.

Definition 6.1.24. A_S/ρ with multiplication defined above becomes a right S-act, and is called the *factor act* of A_S by ρ.

A right factor act of S by a monogenic right congruence is called a *monogenic right act.*

Remark 6.1.25. Analogous definitions and notations are used for congruences on left S-acts. If $X \subseteq {}_SA \times {}_SA$, then, by $\rho(X)$, we denote the smallest congruence on ${}_SA$ containing X.

Example 6.1.26. If S is a monoid then any right (semigroup) congruence ρ on S_S is an act congruence on S_S.

Remark 6.1.27. Let ρ be a congruence on an act A_S. The canonical surjection

$$\begin{aligned} \pi_\rho\ : A_S &\to A_S/\rho \\ a &\mapsto [a]_\rho \end{aligned}$$

is a homomorphism called *a canonical epimorphism.*

Definition 6.1.28. Any subact $B_S \subseteq A_S$ defines the *Rees congruence* ρ_B on A_S, by setting $a\rho_B a'$ if $a, a' \in B$ or $a = a'$. We denote the resulting factor act by A_S/B_S and call it the *Rees factor* act of A_S by the subact B_S.

In particular if $K_S \subseteq S_S$ is a right ideal, then S_S/K_S is called Rees factor act of S_S by the right ideal K_S.

Definition 6.1.29. Let $f : A_S \to B_S$ be an S-homomorphism. Then the kernel of f is defined as $\ker f = \{(a, a') \in A_S \times A_S \mid f(a) = f(a')\}$. The $\ker f$ is an equivalence and, in fact, an act congruence which is called the *kernel congruence* of f.

Definition 6.1.30. Let A_S be an act and $a \in A_S$. Then, we define a homomorphism $\lambda_a : S_S \to A_S$ such that $\lambda_a(s) = as$ for every $s \in S$. The kernel congruence $\ker \lambda_a$ on S_S is called the *annihilator congruence* of $a \in A_S$.

Similarly, if ${}_SA$ is an act and $a \in A$, then by ρ_a we denote the homomorphism from ${}_SS$ into ${}_SA$ defined by $\rho_a(s) = sa$.
The kernel congruence $\ker \rho_a$ on ${}_SS$ is also called the *annihilator congruence* of $a \in {}_SA$.

Remark 6.1.31. $B_S \in A_S/B_S$ is a zero of A_S/B_S, and all other classes are one-element sets. Moreover, any subact $B_S \subseteq A_S$ gives rise to a kernel congruence $\ker \pi$, where $\pi : A_S \to A_S/B_S$ is the canonical epimorphism.

Theorem 6.1.4 (Homomorphism theorem for acts). *Let $f : A_S \to B_S$ be an S-homomorphism and ρ be a congruence on A_S such that $a\rho a' \Rightarrow f(a) = f(a')$, i.e., $\rho \leq \ker f$.*
Then $f' : A_S/\rho \to B_S$ with $f'([x]_\rho) := f(x)$, $x \in A_S$, is the unique S-homomorphism such that the diagram commutes

$$\begin{tikzcd} A_S \arrow[r, "f"] \arrow[d, "\pi_\rho"'] & B_S \\ A_S/\rho \arrow[ur, "f'"'] & \end{tikzcd}$$

If $\rho = \ker f$, then f' is injective, and if f is surjective, then f' is surjective.

Corollary 6.1.5. *If $f : A_S \to B_S$ is an epimorphism then $B_S \cong A_S/\ker f$.*

Definition 6.1.32 (Biacts). Let S, T be monoids, ${}_TA$ a left T-act, and A_S a right S-act. If

$$(ta)s = t(as) \text{ for } t \in T,\ s \in S,\ a \in A,$$

then A is called a T-S act and denoted by ${}_TA_S$.

Example 6.1.33. If ${}_RA$ is a left R-act and B_S is a right S-act, then the Cartesian product $A \times B$ with multiplication (action) defined as $r(a, b) = (ra, b)$ and $(a, b)s = (a, bs)$ for $r \in R$, $a \in A$, $b \in B$, $s \in S$ is an R-S-biact.

Example 6.1.34. Let R be a submonoid of a monoid S. Then the Rees factor $A = S/R$ is a R-R-biact consisting of the elements of $S \setminus R$ together with the element 0 corresponding to R, with left and right multiplication (actions) defined by

$$r * a = \begin{cases} ra, & \text{if } ra \notin R, \\ 0, & \text{otherwise,} \end{cases}$$

$$r * 0 = 0, \text{ and}$$

$$a * r = \begin{cases} ar, & \text{if } ar \notin R, \\ 0, & \text{otherwise,} \end{cases}$$

$$0 * r = 0,$$

for $r \in R$ and $a \in A = S/R$.

Definition 6.1.35 (Bimorphism). Let R, U, S, T be monoids and let ${}_TA_S, {}_UB_R$ be biacts. A triple (ξ, α, δ) is called a bihomomorphism (bimorphism) if $\xi : T \to U$, $\delta : S \to R$ are homomorphisms (isomorphisms) of monoids and $\alpha : A \to B$ is a (bijective) mapping such that $(tas)\alpha = (t\xi)(a\alpha)(s\delta)$ for all $t \in T$, $a \in A$, $s \in S$.

7. Introductory Category Theory

7.1. Categories and Functors

7.1.1. Categories

Definition 7.1.1. A *category* $\mathbf{C}$ is given by

1. a class $\operatorname{Ob}\mathbf{C}$, whose members are called *objects* of $\mathbf{C}$;

2. associating a set $\operatorname{Mor}_{\mathbf{C}}(A, B)$, the *morphisms* from A to B, to every ordered pair (A, B) of objects in $\mathbf{C}$ such that

$$\operatorname{Mor}_{\mathbf{C}}(A, B) \cap \operatorname{Mor}_{\mathbf{C}}(A', B') = \emptyset \text{ if } A \neq A' \text{ or } B \neq B';$$

3. defining composition of morphisms, i.e., for every triple (A, B, C) of objects in $\mathbf{C}$, a mapping

$$\operatorname{Mor}_{\mathbf{C}}(A, B) \times \operatorname{Mor}_{\mathbf{C}}(B, C) \to \operatorname{Mor}_{\mathbf{C}}(A, C)$$
$$(f, g) \mapsto g \circ f,$$

   such that

   a) this composition is associative, i.e., for objects A, B, C, D in $\mathbf{C}$ and $f \in \operatorname{Mor}_{\mathbf{C}}(A, B)$, $g \in \operatorname{Mor}_{\mathbf{C}}(B, C)$, $h \in \operatorname{Mor}_{\mathbf{C}}(C, D)$, we have

$$(h \circ g) \circ f = h \circ (g \circ f);$$

   b) there exist identities, i.e., for every $A \in \operatorname{Ob}\mathbf{C}$ there exists $\mathrm{id}_A \in \operatorname{Mor}_{\mathbf{C}}(A, A)$, the *identity morphism* of A, such that for every $f \in \operatorname{Mor}_{\mathbf{C}}(A, B)$, $B \in \operatorname{Ob}\mathbf{C}$, we have

$$f\,\mathrm{id}_A = \mathrm{id}_B\, f = f.$$

Remark 7.1.2. We often write the notation gf instead of $g \circ f$. The composition is also called *multiplication* of morphisms and gf is called the *product* of morphisms f and g.

The class of all morphisms of $\mathbf{C}$ will be denoted by $\operatorname{Mor}\mathbf{C}$.

Remark 7.1.3. We call A the *domain* and B the *codomain* of every element f of $\operatorname{Mor}(A, B)$ and write,

$$f : A \to B \text{ or } A \xrightarrow{f} B \text{ for } f \in \operatorname{Mor}(A, B).$$

For $A, B, C, D \in \operatorname{Ob}\mathbf{C}$, the morphisms $A \xrightarrow{f} B$, $B \xrightarrow{g} D$, $A \xrightarrow{h} C$, $C \xrightarrow{k} D$ can be visualised in the following diagram:

$$\begin{tikzcd} \mathbf{A} \arrow[r, "f"] \arrow[d, "h"'] & \mathbf{B} \arrow[d, "g"] \\ \mathbf{C} \arrow[r, "k"'] & \mathbf{D} \end{tikzcd}$$

This diagram is called a *commutative square* if $gf = kh$.
We shall, as usual, write $A \in \mathbf{C}$ instead of $A \in \mathrm{Ob}\,\mathbf{C}$ and sometimes also $\mathrm{Mor}(A, B)$ instead of $\mathrm{Mor}_{\mathbf{C}}(A, B)$.

Definition 7.1.4. A category $\mathbf{C}$ is called a *concrete category* if all objects are (structured) sets, morphisms from A to B are (structure preserving) mappings from A to B, composition of morphisms is the composition of mappings, and the identities are the identity mappings.
A category $\mathbf{C}$ is called a *small category* if $\mathrm{Ob}\,\mathbf{C}$ is a set.

Definition 7.1.5. A category $\mathbf{D}$ is called a *subcategory* of the category $\mathbf{C}$ if

1. $\mathrm{Ob}\,\mathbf{D} \subseteq \mathrm{Ob}\,\mathbf{C}$;

2. $\mathrm{Mor}_{\mathbf{D}}(A, B) \subseteq \mathrm{Mor}_{\mathbf{C}}(A, B)$ for all $A, B \in \mathrm{Ob}\,\mathbf{D}$;

3. the composition of morphisms in $\mathbf{D}$ is the restriction of the composition in $\mathbf{C}$.

If, in addition, $\mathrm{Mor}_{\mathbf{D}}(A, B) = \mathrm{Mor}_{\mathbf{C}}(A, B)$ for all $A, B \in \mathrm{Ob}\,\mathbf{D}$, then $\mathbf{D}$ is called a *full subcategory* of $\mathbf{C}$.

We will now look at a few examples of categories of acts.

Example 7.1.6.

1. We denote by $\mathrm{Act} - S(S - \mathrm{Act})$ the category of *right S-acts* (*left S-acts*) as class of objects and S-homomorphisms as a set of morphisms, where S is a semigroup or a monoid.

2. If, in addition, S contains 0, then we take the class of objects as right S-acts (left S-acts) with unique zero θ such that $A0 = \{\theta\}$ $(0A = \{\theta\})$ and the set of all S-homomorphisms preserving 0 as the set of morphisms and denote the category thus obtained by $\mathrm{Act}_0 - S$ $(S - \mathrm{Act}_0)$.

3. Similarly, for biacts we take $T - S$*-biacts* as class of objects and corresponding bimorphisms as morphisms and denote the category by $T - \mathrm{Act} - S$, where T and S are semigroups or monoids.

4. Including the empty S-act $\emptyset_S({}_S\emptyset)$ as an object in (1) gives rise to a new category denoted as $\bar{\mathrm{A}}\mathrm{ct} - S(S - \bar{\mathrm{A}}\mathrm{ct})$.

Definition 7.1.7. The *dual* or *opposite category*, $\mathbf{C}^{\mathrm{op}}$, to a category $\mathbf{C}$ is such that

$$Ob\mathbf{C}^{\mathbf{op}} = Ob\mathbf{C};$$

$$\mathrm{Mor}_{\mathbf{C}^{\mathrm{op}}}(A, B) = \mathrm{Mor}_{\mathbf{C}}(B, A) for A, B \in \mathbf{C};$$

$$\mathrm{Mor}_{\mathbf{C}^{\mathrm{op}}}(C, B) \times \mathrm{Mor}_{\mathbf{C}^{\mathrm{op}}}(B, A) \to \mathrm{Mor}_{\mathbf{C}^{\mathrm{op}}}(C, A)$$

$$(g, f) \mapsto g \circ f.$$

Definition 7.1.8 (Product Category). The *product category* $\mathbf{C} \times \mathbf{D}$ of the categories $\mathbf{C}$ and $\mathbf{D}$ is defined as follows.
Objects: ordered pairs (A, B) with $A \in \mathbf{C}$, $B \in \mathbf{D}$.
Morphisms: $\mathrm{Mor}_{\mathbf{C}\times\mathbf{D}}((A, B), (A', B')) = \{(f, g) : f \in \mathrm{Mor}_{\mathbf{C}}(A, A'),\ g \in \mathrm{Mor}_{\mathbf{D}}(B, B')\}$.
Composition: componentwise. That is

$$(f', g') \circ (f, g) = (f' \circ f, g' \circ g).$$

Analogously, multiple product categories are defined.

Definition 7.1.9. Let $f : A \to B$ be a morphism in a category $\mathbf{C}$. Then f is called

1. a *monomorphism* if f is left cancellative, i.e., $fk = fh \Rightarrow k = h$ for all $k, h \in \mathrm{Mor}(C, A)$. Then A is called a *subobject* of B.
2. an *epimorphism* if f is right cancellative, i.e., $kf = hf \Rightarrow k = h$ for all $k, h \in \mathrm{Mor}(B, D)$. Then B is called a *factor object* of A.
3. a *bimorphism* if it is both a monomorphism as well as an epimorphism.
4. a *coretraction* if f is left invertible, i.e., there exists $g \in \mathrm{Mor}(B, A)$ with $gf = \mathrm{id}_A$, written $A \xrightarrow{f} B$; A is called a *coretraction* of B.
5. A *retraction* if f is right invertible, i.e., there exists $g \in \mathrm{Mor}(B, A)$ with $fg = \mathrm{id}_B$, written $A \xrightarrow{f} B$; B is called a *retraction* of A.
6. An *isomorphism* if it is a retraction and a coretraction. In this case we say that A and B are isomorphic and, symbolically, write $A \cong B$.

Definition 7.1.10. The category $\mathbf{C}$ is called a *balanced category* if bimorphisms are isomorphisms.

Remark 7.1.11. In act categories we call a monomorphism $f : A_S \to B_S$ an *embedding* of A_S into B_S. If there exists such a monomorphism, we say that A_S can be embedded into B_S, or B_S contains (an isomorphic copy) of A_S, or B_S is an extension of A_S. If $A_S \subseteq B_S$ is a subact, then the restriction $(id_{B_S}|_{A_S})$ is called the *inclusion* or the *natural embedding* of A_S into B_S.

Proposition 7.1.1. *A right S-act B_S is a* retract *of a right S-act A_S if and only if there exists a subact $A'_S \subseteq A_S$ and an epimorphism $h : A_S \to A'_S$ such that $B_S \cong A'_S$ and $h(a') = a'$ for every $a' \in A'_S$.*

Corollary 7.1.2. *Let $e \in S$ be an idempotent. Then the principal right ideal eS is a retract of S_S.*

Remark 7.1.12. Every coretraction is a monomorphism and every retraction is an epimorphism.

Remark 7.1.13. Let $A \xrightarrow{f} B \xrightarrow{g} C$ in $\mathbf{C}$. Then

$$f, g \text{ epimorphisms} \implies gf \text{ epimorphism} \implies g \text{ epimorphism};$$

$$f, g \text{ monomorphism} \implies gf \text{ monomorphism} \implies f \text{ monomorphism}.$$

Definition 7.1.14. Let $f : A \to B$ be a morphism in a category $\mathbf{C}$. Then f is called

- a *left zero morphism* if $fg = fh$ for all $C \in \mathbf{C}$ and $g, h \in \mathrm{Mor}(C, A)$;
- a *right zero morphism* if $gf = hf$ for all $D \in \mathbf{C}$ and $g, h \in \mathrm{Mor}(B, D)$.
- a *zero morphism* is it is a left zero and a right zero morphism.

Definition 7.1.15. Let $\mathbf{C}$ be a category and $A \in \mathbf{C}$. Then A is called

- an *initial object* if $|\mathrm{Mor}(A, D)| = 1$ for all $D \in \mathbf{C}$;
- a *terminal object* if $|\mathrm{Mor}(C, A)| = 1$ for all $C \in \mathbf{C}$;
- a *zero object* if it is initial and terminal.

7.1.2. Functors

Definition 7.1.16. Let $\mathbf{C}$ and $\mathbf{D}$ be two categories, then a *covariant functor* $F : \mathbf{C} \to \mathbf{D}$ is an function that assigns to each object $A \in \mathbf{C}$, an object $F(A)$ in $\mathbf{D}$ and to each morphism $f : A \to A'$ in $\mathbf{C}$, a morphism $F(f) : F(A) \to F(A')$ in $\mathbf{D}$ satisfying following:

i) F preserves composition, i.e., $F(g \circ f) = F(g) \circ F(f)$, whenever gf is defined in $\mathbf{C}$.

ii) F preserves identity, i.e., $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ for each $A \in \mathbf{C}$.

Remark 7.1.17. If $F : \mathbf{C} \to \mathbf{D}$ satisfies preserves identity and reverses composition, i.e., $F(g \circ f) = F(f) \circ F(g)$, then F is called a *contravariant functor*. In this case

$$F\big(\mathrm{Mor}_{\mathbf{C}}(A_1, A_2)\big) \subseteq \mathrm{Mor}_{\mathbf{D}}\big(F(A_2), F(A_1)\big).$$

Remark 7.1.18. Functor is often used when it is not necessary to specify the variance of F.

Definition 7.1.19. Let $\mathbf{C}, \mathbf{D}, \mathbf{E}$ be categories and let $F : \mathbf{C} \to \mathbf{D}$, $G : \mathbf{D} \to \mathbf{E}$ be two functors. Then the composition GF of F and G is defined by

$$GF(A) = G(F(A)) \quad \text{and} \quad GF(f) = G(F(f)).$$

Remark 7.1.20. The functor GF is *covariant* if F and G both are covariant or both are contravariant. Otherwise, GF is a *contravariant* functor.

Proposition 7.1.3.

1. *Any monoid S can be considered as a one-object category $(\{1\}, S)$ with the object $\{1\}$ and $\mathrm{Mor}_S(\{1\}, \{1\}) = \{s \mid s \in S\}$, composition being multiplication in S.*
2. *Any right S-act A_S can be viewed as a* contravariant *functor from the category $(\{1\}, S)$ into* **Set**, *the category of all non-empty sets, and vice versa.*
3. *Any left S-act ${}_SA$ can be viewed as a* covariant *functor from the category $(\{1\}, S)$ into* **Set**, *and vice versa.*

Definition 7.1.21. A functor $F : \mathbf{C} \to \mathbf{D}$ is called an *isomorphism* provided there exists a functor $G : \mathbf{D} \to \mathbf{C}$ such that $F \circ G = \mathrm{id}_{\mathbf{D}}$ and $G \circ F = \mathrm{id}_{\mathbf{C}}$.
In this case, we say that $\mathbf{C}$ and $\mathbf{D}$ are isomorphic and write $\mathbf{C} \cong \mathbf{D}$. We call G the inverse of F, denoted by F^{-1}.

Proposition 7.1.4. *The inverse of a functor $F : \mathbf{C} \to \mathbf{D}$, if it exists, is unique.*

Definition 7.1.22. Let $\mathbf{C}$ be a concrete category. For $A \in \mathbf{C}$, by $\lfloor A \rfloor \in \mathbf{Set}$, the category of sets, denotes the underlying set of A.
$\lfloor f \rfloor : \lfloor A_1 \rfloor \to \lfloor A_2 \rfloor$ denote the mapping in $\mathbf{Set}$ underlying f.
Now, $\lfloor - \rfloor : \mathbf{C} \longrightarrow \mathbf{Set}$ defined as indicated is a covariant functor which is called the *forgetful functor* from $\mathbf{C}$ to $\mathbf{Set}$.

In particular, we have the forgetful functor

$$\lfloor - \rfloor : \mathbf{Act}\text{-}S \longrightarrow \mathbf{Set}.$$

Remark 7.1.23. The procedure which turns a category $\mathbf{C}$ into its dual or opposite category $\mathbf{C}^{op}$ is a contravariant functor and is called the *dualising* or *op-functor*; we write $-^{op} : \mathbf{C} \to \mathbf{C}^{op}$.

Definition 7.1.24. Let $\mathbf{C}, \mathbf{D}, \mathbf{E}$ be categories and let $\mathbf{C} \times \mathbf{D}$ be the product category of $\mathbf{C}$ and $\mathbf{D}$. A functor $F : \mathbf{C} \times \mathbf{D} \to \mathbf{E}$ is called a *bifunctor.* Analogously, *multifunctors* are defined.

Definition 7.1.25. A *covariant Hom functor*(Hon-functor in the second variable),

$$\mathrm{Hom}(A_S, -) : \mathrm{Act}\text{-}S \longrightarrow \mathbf{Set}$$

is given by

$$\begin{tikzcd}
B_S \arrow[r] \arrow[d, "g"'] & \mathrm{Hom}(A_S, B_S) \ni \arrow[d, "\mathrm{Hom}(A_S, g)"] & \alpha \arrow[d] \\
B'_S \arrow[r] & \mathrm{Hom}(A_S, B'_S) \ni & g\alpha
\end{tikzcd}
\qquad
g \longrightarrow
\qquad
\begin{tikzcd}
A_S \arrow[r, "\alpha"] \arrow[dr, "g\alpha"'] & B_S \arrow[d, "g"] \\
& B'_S
\end{tikzcd}$$

$(B_S, B'_S \in \mathrm{Act}\text{-}S)$.

Example 7.1.26. *Covariant functors*:

1. $\mathrm{Hom}({}_RA_S, -_S) : \mathrm{Act}\text{-}S \to \mathrm{Act}\text{-}R.$
2. $\mathrm{Hom}({}_RA_S, {}_R-) : R\text{-}\mathrm{Act} \to S\text{-}\mathrm{Act}.$
3. Letting $R = \mathrm{End}(A)$ and $R = C(S)$, respectively, in (1).

Definition 7.1.27. A *contravariant Hom functor* (Hom-functor in the first variable)

$$\mathrm{Hom}(-_S, B_S) : \mathrm{Act}\text{-}S \longrightarrow \mathbf{Set}$$

is given by

$$
\begin{tikzcd}
A_S \arrow[r] \arrow[d, "f"'] & \mathrm{Hom}(A_S, B_S) \ni & \beta f \\
{} \arrow[r] & {} & {} \\
A'_S \arrow[r] & \mathrm{Hom}(A'_S, B_S) \ni \arrow[uu, "\mathrm{Hom}(f, B_S)"] & \beta \arrow[uu]
\end{tikzcd}
\qquad
\begin{tikzcd}
A_S \arrow[d, "f"'] \arrow[dr, "\beta f"] & \\
A'_S \arrow[r, "\beta"'] & B_S
\end{tikzcd}
$$

$(A_S, A'_S) \in \mathrm{Act}\text{-}S$

Example 7.1.28. 1. $Hom(-_S, {}_R)B_S : \mathrm{Act}\text{-}S \to R\text{-}\mathrm{Act}$.

2. $Hom({}_R-, {}_R)B_S : R\text{-}\mathrm{Act} \to \mathrm{Act}\text{-}S$.

3. Letting $R = End(B)$ and $R = C(S)$, respectively, in (1).

Proposition 7.1.5. *Define* $\mathrm{Hom}(-_S, -_S) : (\mathrm{Act}\text{-}S)^{op} \times \mathrm{Act}\text{-}S \to \mathbf{Set}$ *by*

$$
\begin{tikzcd}
(A_S, B_S) \arrow[r] \arrow[d, "{(f,g)}"'] & \mathrm{Hom}(A_S, B_S) \ni \arrow[d, "{\mathrm{Hom}(f,g)}"] & \alpha \arrow[d] \\
(A'_S, B'_S) \arrow[r] & \mathrm{Hom}(A'_S, B'_S) \ni & g\alpha f
\end{tikzcd}
\qquad
\begin{tikzcd}
A_S \arrow[r, "\alpha"] \arrow[d, "f"'] & B_S \arrow[d, "g"] \\
A'_S \arrow[r, "g\alpha f"'] & B'_S
\end{tikzcd}
$$

where $(f, g) \in (\mathrm{Act}\text{-}S)^{op} \times \mathrm{Act}\text{-}S$, $\mathrm{Hom}(f, g) \in \mathbf{Set}$ *and right diagram is in* $\mathrm{Act}\text{-}S$*. Then,* $\mathrm{Hom}(-_S, -_S)$ *is a bifunctor which is covariant in both variables*

Remark 7.1.29. *Mor-functors* are defined parallelly to Hom-functors by replacing $\mathrm{Hom}(-_S, -_S)$ with $\mathrm{Mor}_{\mathbf{C}}(-, -)$ as;

- *Contravariant Mor-functor*: $\mathrm{Mor}_{\mathbf{C}}(-, B) : \mathbf{C} \to \mathbf{Set}$.
- *Covariant Mor-functor*: $\mathrm{Mor}_{\mathbf{C}}(A, -) : \mathbf{C} \to \mathbf{Set}$.
- $\mathrm{Mor}_{\mathbf{C}}(-, -) : (\mathbf{C})^{op} \times \mathbf{C} \to \mathbf{Set}$.

7.2. Brief Morita Equivalence

A semigroup S is called *factorisable* if every element of S is a product of two elements.
We say that $S \in S$ has a *weak right local unit u* (*weak left local unit v*) if $Su = S \quad (vS = S)$.
A semigroup has *weak local units* if each of its elements has both a weak right and a weak left local unit, and *local units* if the elements u, v above can always be chosen to be idempotents.
We say that S has common weak right (left) local units if for every $s, t \in S$ there exists $u \in S$ ($v \in S$) such that $s = su$ and $t = tu$ ($s = vs$ and $t = vt$).
It has common weak local units if u has both common left and common right local units.

Notation 7.2.1.

- Act_S: category of right S-acts.
- ${}_S\,\mathrm{Act}$: category of left S-acts.
- $S\,\mathrm{Act}_T$: category of (S,T)-biacts.

A right S-act is called *unitary* right S-act A_S if $AS = A$.

Notation 7.2.2. The category of all unitary right S-acts is denoted by $\mathbf{UAct}_S$.

A semigroup S is said to be *fair* if every subact of a unitary right S-act and every subact of a unitary left S-act is unitary.

Definition 7.2.3. Let $A_S \in \mathrm{Act}_S,\ {}_SM \in {}_S\,\mathrm{Act}$, and $Y \in \mathbf{Set}$. A mapping

$$\beta \,:\, A_S \times {}_SM \longrightarrow Y$$

is called S-*tensorial* or S-*balanced* if

$$\beta(as, m) = \beta(a, sm) \quad \forall \quad a \in A_S,\ m \in {}_SM,\ s \in S.$$

Definition 7.2.4. Let $A_S \in \mathrm{Act}_S,\ {}_SM \in {}_S\,\mathrm{Act}$. A set T, together with an S-tensorial mapping

$$\tau \,:\, A_S \times {}_SM \longrightarrow T$$

is called *tensor product* of A_S and ${}_SM$ if for every $Y \in \mathbf{Set}$, every S-tensorial mapping $\beta \,:\, A_S \times {}_SM \longrightarrow Y$ there exists a unique mapping $\bar{\beta}$ in $\mathbf{Set}$ such that the following diagram commutes

$$\begin{tikzcd} A_S \times {}_SM \arrow[r, "\beta"] \arrow[d, "\tau"'] & Y \\ T \arrow[ur, "\bar{\beta}"'] & \end{tikzcd}$$

Definition 7.2.5. Let $A_S \in \mathrm{Act}_S,\ {}_SM \in {}_S\,\mathrm{Act}$, and let ρ be the *tensor relation*, i.e. equivalence relation on $A_S \times {}_SM$ generated by the pairs

$$\big((as, m), (a, sm)\big) \quad \text{for } a \in A_S,\ m \in {}_SM,\ s \in S.$$

We define

$$A_S \otimes_S M \,:= (A_S \times {}_SM)/\rho,$$

and

$$a \otimes m \,:= [(a, m)]_\rho \in A_S \otimes {}_SM.$$

Definition 7.2.6. We say that a right S-act A_S is *firm* if the mapping

$$\mu_A \,:\, A \otimes S \longrightarrow A, \qquad a \otimes s \longmapsto as$$

is bijective.

A semigroup is *firm* if it is firm as a right (or equivalently, left) S-act.

Notation 7.2.7. The category of firm right S-acts is denoted by $\mathbf{FAct}_S$.

Remark 7.2.8. A_S is unitary iff and only if the mapping μ_A is surjective. Hence, for any semigroup S, $\mathbf{FAct}_S$ is a subcategory of $\mathbf{UAct}_S$. Also, a semigroup is factorisable iff S_S is unitary. Thus, every firm semigroup S has to be factorisable (but not necessarily conversely).

Definition 7.2.9. A right S-act A_S is called *non-singular* if, for $a, a' \in A$,

$$as = a's \ \ \forall s \in S \implies a = a'.$$

Notation 7.2.10. we denote the category of unitary non-singular right S-act by $\mathbf{NAct}_S$ ($\mathbf{US} - \mathbf{FAct}$ is also used by some authors).

There exist from left (right) S-acts which are not non-singular. Hence, in general, $\mathbf{FAct}_S$ and $\mathbf{NAct}_S$ are incomparable.
The S-act S_S is non-singular iff, for every $s, t \in S$, $sz = tz$ $\forall z \in S$ implies $s = t$. Semigroups with this property are called right reductive.

Definition 7.2.11. Let $\mathbf{C}$, $\mathbf{D}$ be categories and $F_1, F_2 : \mathbf{C} \to \mathbf{D}$ covariant functors. A family $\mu = (\mu_A)_{A \in \mathbf{C}}$ of morphisms in $\mathbf{D}$ indexed by objects in $\mathbf{C}$ is called a *natural transformation* of the functor F_1 into the functor F_2, written $\mu : F_1 \to F_2$, if

1. $\mu_A \in \mathrm{Mor}_{\mathbf{D}}(F_1(A), F_2(A))$ for all $A \in \mathbf{C}$ and
2. the condition of naturality is fulfilled, i.e.,

   $$F_2(f)\mu_A = \mu'_A F_1(f),$$

   that is, the diagram

   $$\begin{tikzcd} F_1(A) \arrow[r, "u_A"] \arrow[d, "F_1(f)"'] & F_2(A) \arrow[d, "F_2(f)"] \\ F_1(A') \arrow[r, "u_{A'}"'] & F_2(A') \end{tikzcd}$$

   is commutative for all $A, A' \in C$, $f \in \mathrm{Mor}(A, A')$.

If F_1, F_2 are contravariants then the condition of naturality changes to

$$u_A F_1(f) = F_2(f) u_{A'}.$$

Definition 7.2.12. Let $F_1, F_2 : \mathbf{C} \to \mathbf{D}$ be functors. A natural transformation $\mu : F_1 \to F_2$ is called a *natural equivalence* if u_A are isomorphisms in $\mathbf{D}$ for all $A \in \mathbf{C}$. If there exists a natural equivalence $\mu : F_1 \to F_2$, then F_1 and F_2 are called *naturally equivalent* functors. We write

$$F_1 \cong F_2.$$

Definition 7.2.13. An endofunctor is simply a functor from a category to itself. That is, if $\mathbf{C}$ is a category, an endofunctor is

$$F : \mathbf{C} \to \mathbf{C}.$$

An endofunctor $F : \mathbf{C} \to \mathbf{C}$ on some category along with a natural transformation $\zeta : 1 \to F$ satisfying $F(\zeta_A) = \zeta_{F(A)} : F(A) \to F(F(A))$ for every $A \in \mathbf{C}$ is called a *well pointed endofunctor*. A *well-copointed* endofunctor is defined as the dual notion, meaning that the components of natural transformation $\eta : F \to 1$ satisfy $F(\eta_A) = \eta_{F(A)} : F(F(A)) \to F(A)$. If $F(\zeta_A)$ (respectively, η_A) is an isomorphism for every $A \in \mathbf{C}$, then the well-(co)pointed functor is called idempotent.

Definition 7.2.14. If the A-component α_A of a natural tranformation α between endofunctor of a category $\mathbf{C}$ is an isomorphism, we say that A is *fixed* by the natural transformation α.

Notation 7.2.15. We denote by $Fix(\mathbf{C}, \alpha)$ the full subcategory of $\mathbf{C}$ spanned by all the objects that are fixed by α.

Notation 7.2.16. We denote by $\mathbf{CAct}_S$ the full subcategory of $\mathbf{Act}_S$ given by the acts A_S for which λ_A is invertible (that is, isomorphism).

Thus, we have $\mathbf{CAct} = Fix(Act_S, \lambda)$, where

$$\lambda_A : A \to \mathrm{Act}_S(S, A), a \mapsto (s \mapsto as).$$

In other words, the functor $-\otimes S : A_S \to \mathrm{Act}_S$ has $\mathrm{Act}_S(S, -) : \mathrm{Act}_S \to \mathrm{Act}_S$ as a right adjoint, we want to know what is the idempotent pointed endofunctor corresponding to $(-\otimes S, \mu)$. Let is denote it by $(\mathrm{Act}_S(S, -), \lambda)$ and hence we have the required λ.

Part III.

Varieties, Pseudovarieties, and Finite Semigroups

8. Finite Semigroups

In this chapter, the goal will be to study finite semigroups and develop the relevant background to study pseudovarieties. Also, for time being, I will skip the proofs of the results in this chapter.

8.1. Green's Relations, Semidirect and Wreath Products

8.1.1. Green's Relations

We have already seen that for finite semigroups $\mathscr{D}$ and $\mathscr{J}$ coincide. Now, we analyze the Green's relation further for finite semigroups.

Proposition 8.1.1. *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.*

Proposition 8.1.2. *Let S and S' be finite semigroups and $\varphi : S \longrightarrow S'$ be an epimorphism. Let G' be a maximal subgroup of S', then there exists a maximal subgroup G of S such that $G\varphi = G'$.*

Proposition 8.1.3. *Let S be a finite semigroup and let $x, y \in S$. If $x \mathscr{H} y$, then $y \in xG$ for some subgroup G of S.*

Definition 8.1.1. Let S be a semigroup. If for every $x \in S$, there exists $m \in \mathbb{N}$ such that $x^m = x^{m+1}$, then S is called *aperiodic*.

Proposition 8.1.4. *Let S be a finite semigroup. Then the following are equivalent:*

1. *$H = \mathrm{id}_S$;*
2. *all subgroups of S are trivial;*
3. *S is aperiodic.*

8.1.2. Semidirect and Wreath Products

Definition 8.1.2. 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 an antihomomorphism corresponding to this left action. to avoid using extra symbols, we write ${}^t s$ instead of $t\dot{s}$.
The semidirect product of S and T by φ is defined to be the Cartesian product $S \times T$ with multiplication defined as

$$(s_1, t_1)(s_2, t_2) = (s_1 {}^{t_1} s_2, t_1 t_2),$$

and is denoted by $S \rtimes_\varphi T$.

The multiplication is associative and so $S \rtimes_\varphi T$ is a semigroup. Also,

$$|S \rtimes_\varphi T| = |S||T|.$$

Remark 8.1.3. For any semigroup S and T, we can take trivial left action

$$t \cdot s = {}^t s = s;$$

then the corresponding anti-homomorphism $\varphi : T \to \mathrm{End}(S)$ is given by $y\varphi = id_S$ for all $y \in T$.

Define a left action of T on S by letting $y \cdot f = {}^y f$ such that $(x)^y f = (xy)f$.
Clearly, it is a left action as

$$(x)(z \cdot (y \cdot f)) = (x)(z \cdot {}^y f) = (x)^z({}^y f) = (xz)^y f = (xzy)f = (x)^{zy} f = (x)(zy \cdot f).$$

Definition 8.1.4. Let S and T be semigroups and define an action of T on S as above. Let φ denote the corresponding anti-homomorphism. Then the *wreath product* of S and T is the semidirect product $S^T \rtimes_\varphi T$, and is denoted as $S \wr T$.

Thus the product in $S \wr T$ is

$$(f_1, t_1)(f_2, t_2) = (f_1{}^{t_1} f_2, t_1 t_2).$$

Since the multiplication is derived from multiplication in direct and semidirect products, it is associative. Hence, $S \wr T$ forms a semigroup. Also,

$$|S \wr T| = |S|^{|T|}|T|.$$

Remark 8.1.5. The wreath product, as an operation on semigroups, is not associative. To see this, let S, T, U be finite semigroups. Then,

$$|(S \wr T) \wr U| = |S \wr T|^{|U|}|U| = (|S|^{|T|}|T|)^{|U|}|U| = |S|^{|T||U|}|T|^{|U|}|U|$$

and

$$|S \wr (T \wr U)| = |S|^{|T \wr U|}|T \wr U| = |S|^{|T|^{|U|}|U|}|T|^{|U|}|U|.$$

8.2. Division and Krohn-Rhodes Theorem

Definition 8.2.1. A semigroup S *divides* a semigroup T, denoted by $S \prec T$, if S is a homomorphic image of a subsemigroup of T.

It is easy to see that divisibility is reflexive.

Proposition 8.2.1. *The divisibility relation $\prec$ is transitive.*

Proposition 8.2.2. *Let S and T be semigroups. Then S, T, and $S \times T$ divide $S \wr T$.*

Proposition 8.2.3. *Let M be a monoid and let E be an ideal extension of M by T. Then $E \prec T \wr M$.*

Proposition 8.2.4. *If $S' \prec S$ and $T' \prec T$, then*

$$S' \wr T' \prec S \wr T.$$

Let S be a semigroup and S' be a set in bijection with S under $x \mapsto x'$. Define a multiplication on $S \cup S'$ as multiplication in S as before, and, for all $x, y \in S$,

$$xy' = x'y' = y', \qquad x'y = (xy)'.$$

It is easy, but tedious, to prove that this multiplication is associative; the set $S \cup S'$ is thus a semigroup.

Definition 8.2.2. The semigroup defined above is called the *constant extension* of S and denoted by $C(S)$.

Proposition 8.2.5. *If $S \prec T$, then $C(S) \prec C(T)$.*

Proposition 8.2.6. *Let M be a monoid and S be a semigroup. Then*

$$C(S \wr M) \prec C(S)^M \wr C(M).$$

Corollary 8.2.7. *Let M be a finite monoid and S be a semigroup. Then $C(S \wr M)$ divides a wreath product of copies of $C(S)$ and $C(M)$.*

Let U_3 be the monoid obtained by adjoining an identity to a two-element right zero semigroup $\{a, b\}$. So, $U_3 = \{1, a, b\}$, and the multiplication is defined as

	1	a	b
1	1	a	b
a	a	a	b
b	b	a	b

Remark 8.2.3. Notice that in U_3, the Green's relation $\mathscr{H}$ is the identity relation and so U_3 is aperiodic.

Theorem 8.2.8 (Krohn–Rhodes Theorem). *Let S be a finite semigroup. Then S divides a wreath product of subgroups of S and copies of U_3.*

(To be continued)

9. Varieties

9.1. Introduction

9.1.1. Preliminaries

Definition 9.1.1. 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
$$f_i : S^{f_i\alpha} \longrightarrow S$$
for some $f_i\alpha \in \mathbb{N} \cup \{0\}$. This $f_i\alpha$ is called the *arity* of f_i.

Example 9.1.2.
1. S is a semigroup, then the multiplication operation $\circ$ is a map $\circ : S^2 \longrightarrow S$ and so has arity 2.
2. If S is an inverse semigroup, the inverse operation $^{-1}$ is a map $^{-1} : S \longrightarrow S$ and so has arity 1.
3. If S is a monoid, then we consider the identity 1_S of S as a map $1_S : S^0 \longrightarrow S$ and so has arity 0.

Remark 9.1.3. The operations of arity 0 are called *constants*; operations of arity 1 are called *unary* operations; operations of arity 2 are called *binary* operations.

Definition 9.1.4. A *type* $\mathscr{T}$ of an algebra is a set of operation symbols $\{f_i : i \in I\}$ and a map $\alpha : \{f_i : i \in I\} \longrightarrow \mathbb{N} \cup \{0\}$ determining the arity of each operation.

We can write the type simply as a set consisting of pairs in the map α. A semigroup has type $\{(\circ, 2)\}$ and a lattice has type $\{(\wedge, 2), (\vee, 2)\}$. An algebra of type $\mathscr{T}$ is called a $\mathscr{T}$-algebra.

Remark 9.1.5. Some structure can be viewed as algebras in more than one way and thus have more than one type. For example, let G be a group. Then G, viewed as a group, is a $\{(\circ, 2), (^{-1}, 1), (e, 0)\}$-algebra; G, viewed as a monoid, is a $\{(\circ, 2), (e, 0)\}$-algebra; and G, viewed as a semigroup, is a $\{(\circ, 2)\}$-algebra.

Definition 9.1.6. Let S be a $\mathscr{T}$-algebra and $S' \subseteq S$. Then S' is called a *subalgebra* of S if S' is closed under all the operations in $\mathscr{T} = \{(f_i, f_i\alpha)\}$. That is, for each $i \in I$, we have
$$x_1, \ldots, x_{f_i\alpha} \in S' \Longrightarrow (x_1, \ldots, x_{f_i\alpha})f_i \in S'.$$

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 see that the subalgebra generated by X consists of all elements that can be obtained by starting from X and applying the operations f_i.

Definition 9.1.7. Let S and T be $\mathscr{T}$-algebras. Then $\varphi : S \longrightarrow T$ is a *homomorphism* if, for each $i \in I$, we have
$$((x_1, \ldots, x_{f_i\alpha})f_i)\varphi = (x_1\varphi, \ldots, x_{f_i\alpha}\varphi)f_i.$$

A *monomorphism* is an injective homomorphism, an *epimorphism* is a surjective homomorphism, and an *isomorphism* is a bijective homomorphism.

Remark 9.1.8. Let S and T be $\mathscr{T}$-algebras. If $\varphi : S \longrightarrow T$ is an epimorphism and T is a homomorphic image of S.

Definition 9.1.9. Let S be a $\mathscr{T}$-algebra and ρ be a binary relation on S. If $x_1, \dots, x_{f_i\alpha}, y_i, \dots, y_{f_i\alpha} \in S$ such that $x_i \rho y_i$ for all $1 \leq i \leq f_i\alpha$ implies

$$(x_1, \dots, x_{f_i\alpha})f_i \;\rho\; (y_1, \dots, y_{f_i\alpha})f_i,$$

then ρ is called a congruence.

Definition 9.1.10 (Direct Product). Let $S = \{S_j \mid j \in J\}$, be a collection of $\mathscr{T}$-algebras. The *direct product* of $\in S$-algebras in S is the cartesian product $\prod_{j\in J} S_j$ with the operations defined componentwise. Mathematically, view $s \in \prod_{j\in J} S_j$ as a map $s : J \longrightarrow \bigcup_{j\in J} S_j$ such that, for every $f_i \in \mathscr{T}$,

$$(j)(s_1, \dots, s_{f_i\alpha})f_i = ((j)s_1, \dots, (j)s_{f_i\alpha})f_i.$$

Definition 9.1.11 (Free $\mathscr{T}$-algebra). Let $A \neq \emptyset$ be a set and let $F_{\mathscr{T}}(A)$ be the set of all the words formed over $A \cup \{f_i : i \in I\} \cup \{(\} \cup \{)\} \cup \{,\}$, satisfying the following:

1. $A \subseteq F_{\mathscr{T}}(A)$;

2. if $u_1, \dots, u_{f_i\alpha} \in F_{\mathscr{T}}(A)$, then

$$(u_1, \dots, u_{f_i\alpha})f_i \in F_{\mathscr{T}}(A).$$

The set $F_{\mathscr{T}}(A)$ is a $\mathscr{T}$-algebra and is called the free $\mathscr{T}$-algebra or absolutely free $\mathscr{T}$-algebra.

Remark 9.1.12. $F_{\mathscr{T}}(A)$ is generated by A.

Example 9.1.13. Let $\mathscr{T} = \{(f, 2), (', 1)\}$ 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 $F_{\mathscr{T}}(A)$.

Let $i : A \longrightarrow F_{\mathscr{T}}(A)$ be the inclusion map. For any $\mathscr{T}$-algebra S and any map $\varphi : A \to S$, there is a unique extension $\hat{\varphi} : F_T(A) \to S$. That is, the following diagram is commutative:

$$\begin{tikzcd}
A \arrow[r, "i"] \arrow[dr, "\varphi"'] & F_{\mathscr{T}}(A) \arrow[d, "\hat{\varphi}"] \\
 & S
\end{tikzcd}$$

That is, $i\hat{\varphi} = \varphi$.

9.1.2. Varieties

Let $\mathscr{X}$ be a class of $\mathscr{T}$-algebras. Let $\operatorname{Hom}\mathscr{X}$ denote the class of all $\mathscr{T}$-algebras that are homomorphic images of the algebras in $\mathscr{X}$, and let $\operatorname{Sub}\mathscr{X}$ be the class of all $\mathscr{T}$-algebras that are subalgebras of algebras in $\mathscr{X}$, and Prod $\mathscr{X}$ denote the class of all $\mathscr{T}$-algebras that are direct products of the $\mathscr{T}$-algebras in $\mathscr{X}$. Mathematically,

$$\begin{aligned}
\operatorname{Hom}\mathscr{X} &= \{S \mid \exists T \in \mathscr{X} \textit{ s.t } S \text{ is a homomorphic image of } T\}.\\
\operatorname{Sub}\mathscr{X} &= \{S \mid \exists T \in \mathscr{X} \textit{ s.t } S \text{ is a subalgebra of } T\}.\\
\operatorname{Prod}\mathscr{X} &= \left\{S \mid \exists \{T_i : i \in I\}) \subseteq \mathscr{X} \textit{ s.t } S = \prod_{i \in I} T_i\right\}.
\end{aligned}$$

Thus, Hom, Sub, Prod are unary operations on classes of algebras.

Remark 9.1.14. $\mathscr{X}$ is contained in Hom $\mathscr{X}$, Sub $\mathscr{X}$, and Prod $\mathscr{X}$, respectively.

Definition 9.1.15. Let $\mathscr{X}$ be a class of $\mathscr{T}$-algebras. If $\mathscr{X}$ is closed under the operations Hom, Sub, and Prod, then $\mathscr{X}$ is called a *variety.*
That is, $\mathscr{X}$ is a variety if

$$\operatorname{Hom}\mathscr{X} \cup \operatorname{Sub}\mathscr{X} \cup \operatorname{Prod}\mathscr{X} \subseteq \mathscr{X}.$$

Remark 9.1.16. A class of algebraic structure (e.g. groups, semigroups, rings, etc) forms a variety if it is closed under taking homomorphic images, sub-algebraic structures (subgroups, subsemigroups, subrings, etc), and direct products.

Remark 9.1.17. A *variety of semigroups* is a class of semigroups that is closed under taking homomorphic images, subsemigroups, and arbitrary direct products.

Before proceeding, we check some examples of varieties.

Example 9.1.18. (a) Let $\mathsf{1} = \{e\}$, the class of the trivial semigroup $E = \{e\}$. Then $\mathsf{1}$ is a variety as only homomorphic image of E is E itself, only subalgebra of E is E itself, and any direct product of copies of E is isomorphic to E.

(b) Let $\mathsf{Com} = \{S \mid S \text{ is a commutative semigroup}\}$, where a semigroup $S \in \mathsf{Com}$ is viewed as a $\{(\circ, 2)\}$-algebra. Since any subalgebra or homomorphic image of a commutative semigroup is again a commutative semigroup, and direct product of commutative semigroups is again a commutative semigroup, Com is a variety.

(c) Let G consist of all groups viewed as $\{(0, 2), (1_G, 0), ({}^{-1}, 1)\}$-algebras. Since every subalgebra is a subgroup, as they are closed under inverses, and every homomorphic image, subalgebra, or direct product of groups is also a group, G is a variety.

(d) The class I of all inverse semigroups, viewed as $\{(0, 2), ({}^{-1}, 1)\}$-algebra, is a variety.

Remark 9.1.19. The class $\mathscr{G}$ of all the groups viewed as $\{(0, 2), (-1, 1)\}$-algebra does not form a variety as subalgebra are subsemigroup and so $\mathscr{G}$ is not closed under talking subalgebras. For example, $\mathbb{Z} \in \mathscr{G}$ but $\mathbb{N} \notin \mathscr{G}$, which is a subalgebra (subsemigroup) of $\mathbb{Z}$.

Definition 9.1.20. Let V be a variety of $\mathscr{T}$-algebras and $A \neq \emptyset$ be a set. Let $S \in \mathsf{V}$ and let $\varphi \in S^A$, then there exists a unique extension $\hat{\varphi} : F_{\mathscr{T}}(A) \to S$ of φ.
Now, $\operatorname{im}\hat{\varphi}$ is a subalgebra of S and hence is in V. Let

$$\rho = \bigcap\{\ker\hat{\varphi} : \varphi \in S^A,\ S \in \mathsf{V}\}.$$

Then ρ, being an intersection of congruences on $F_{\mathscr{T}}(A)$, is a congruence and $\rho \subseteq \ker\hat{\varphi}$ for any $\varphi \in S^A$.

Hence, for each $S \in \mathsf{V}$, there exists a unique homomorphism

$$\overline{\varphi} : F_{\mathscr{T}}(A)/\rho \to S$$

such that $\rho^{\natural}\overline{\varphi} = \varphi$. Thus $\overline{\varphi}$ is the unique homomorphism such that the following diagram commutes:

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[dr, "\varphi"'] & F_{\mathscr{T}}(A) \arrow[r, "\rho^{\natural}"] \arrow[d, "\hat{\varphi}"] & F_{\mathscr{T}}(A)/\rho \arrow[dl, "\overline{\varphi}"] \\ & S & \end{tikzcd}$$

By a result for $\mathscr{T}$-algebras analogous to Proposition (2.1.8), $F_{\mathscr{T}}(A)/\rho$ is a subdirect product of $\{F_{\mathscr{T}}(A)/\ker\hat{\varphi} : \varphi \in S^A,\ S \in \mathsf{V}\}$.
Now each algebra $F_{\mathscr{T}}(A)/\ker\hat{\varphi}$ is a subalgebra of an algebra in V and therefore is itself a member of V. Hence, $F_{\mathscr{T}}(A)/\rho \in \operatorname{Sub}\operatorname{Prod}\mathsf{V} = \mathsf{V}$.

Definition 9.1.21. The $\mathscr{T}$-algebra $F_{\mathsf{V}}(A)/\rho$ is called the V-free algebra, and is denoted by $F_{\mathsf{V}}(A)$.

Remark 9.1.22. It is easy to see that there is a map $\vartheta : A \to F_{\mathsf{V}}(A)$ given by $x\vartheta = xi\rho^{\natural} = [x]_\rho$ such that the universal mapping property holds: for any $S \in \mathsf{V}$ and any map $\varphi : A \to S$, there is a unique homomorphism $\overline{\varphi} : F_{\mathsf{V}}(A) \to S$ such that $\vartheta\overline{\varphi} = \varphi$. That is the diagram is

$$\begin{tikzcd} A \arrow[r, "\vartheta"] \arrow[dr, "\varphi"'] & F_{\mathsf{V}}(A) \arrow[d, "\overline{\varphi}"] \\ & S \end{tikzcd}$$

is commutative.

Definition 9.1.23. For $\mathscr{T}$-algebras, a law (identity or identical relation) over an alphabet A is a pair $u, v \in F_{\mathscr{T}}(A)$, usually written as $u = v$.

A $\mathscr{T}$-algebra S satisfies the law $u = v$, if, for every homomorphism $\varphi : A \to S$, we have $u\hat{\varphi} = v\hat{\varphi}$, where $\hat{\varphi}$ is given by the diagram

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[dr, "\varphi"'] & F_{\mathscr{T}}(A) \arrow[d, "\hat{\varphi}"] \\ & S \end{tikzcd}$$

For instance, commutative semigroups viewed as $\{(0,2)\}$-algebras satisfy $xy = yx$. Semigroups of idempotents satisfy $xx = x$.

Definition 9.1.24 (Equational class). Let $\mathscr{E}$ be a class of $\mathscr{T}$-algebras. Suppose that there is a set L of laws over an alphabet A such that $S \in \mathscr{E}$ if and only if S satisfies every law in L. Then $\mathscr{E}$ is the equational class defined by L.

Theorem 9.1.1 (Birkhoff's Theorem). *Let $\mathscr{T}$ be a type. Then a class of $\mathscr{T}$-algebras is a variety if and only if it is an equational class.*

Proof. **First part.** Suppose $\mathscr{X}$ is an equational class. Then there is a set of laws L over an alphabet A such that $S \in \mathscr{X}$ if and only if S satisfies every law in L. To prove that $\mathscr{X}$ is a variety, we must show that it is closed under Hom, Sub, and Prod.

Let $S \in \mathscr{X}$, and let T be a $\mathscr{T}$-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 $\theta a \in S$ be such that $a\theta\psi = a\varphi$ (such an θ exists because ψ is surjective). Notice that $\widehat{\theta\psi}$ and $\hat{\varphi}$ are homomorphisms from $F_{\mathscr{T}}(A)$ to S extending $\theta\psi = \varphi$ and so, by the uniqueness of such homomorphisms, $\widehat{\theta\psi} = \hat{\varphi}$. Since S satisfies L, we have $u\hat{\theta} = v\hat{\theta}$; hence $u\hat{\varphi} = u\hat{\theta}\psi = v\hat{\theta}\psi = v\hat{\varphi}$. So T satisfies $u = v$. Hence T satisfies every law in L and so $T \in \mathscr{X}$. Thus $\mathscr{X}$ is closed under Hom.

Let $S \in \mathscr{X}$ 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 $T \in \mathscr{X}$. Thus $\mathscr{X}$ is closed under Sub.

Let $\{S_j : j \in J\} \subseteq \mathscr{X}$ 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 map. So φ_j is a map from A to S_j, and S_j satisfies $u = v$, and thus $u\widehat{\varphi_j} = v\widehat{\varphi_j}$. The map $\psi : F_{\mathscr{T}}(A) \to T$ with $(j)(x\psi) = x\widehat{\varphi_j}$ is a homomorphism extending φ, so, by the uniqueness condition, $\psi = \hat{\varphi}$. Since $u\widehat{\varphi_j} = v\widehat{\varphi_j}$ for each j, we have $u\hat{\varphi} = u\psi = v\psi = v\hat{\varphi}$. So T satisfies $u = v$ and so $T \in \mathscr{X}$. Thus $\mathscr{X}$ 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 $F_{\mathsf{V}}(A) = F_{\mathscr{T}}(A)/\rho$, 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 $\rho \subseteq F_{\mathscr{T}}(A) \times F_{\mathscr{T}}(A)$ as a set of laws.

Let $S \in \mathsf{V}$. Let $(u, v) \in \rho$; notice that $u, v \in F_{\mathscr{T}}(A)$. 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 $F_{\mathsf{V}}(B) = F_{\mathscr{T}}(B)/\pi$ for some congruence π on $F_{\mathscr{T}}(B)$.

Let $\psi : F_{\mathscr{T}}(B) \to S$ 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 $\hat{\xi} : F_{\mathscr{T}}(A) \to F_{\mathscr{T}}(B)$, and η extends to a homomorphism $\hat{\eta} : F_{\mathscr{T}}(B) \to F_{\mathscr{T}}(A)$. Since $\hat{\xi}$ is injective, there are uniquely determined $u_0, v_0 \in F_{\mathscr{T}}(A)$ such that $u_0\hat{\xi} = u$ and $v_0\hat{\xi} = v$. Notice that $u\hat{\eta} = u_0$ and $v\hat{\eta} = v_0$.

Consider the map $\eta\rho^{\hat{}} : F_{\mathscr{T}}(B) \to F_{\mathsf{V}}(A)$. Since $F_{\mathsf{V}}(B)$ lies in the variety V, we must have $\pi \subseteq \eta\rho^{\hat{}}$. In particular, $u\eta\rho^{\hat{}} = v\eta\rho^{\hat{}}$ and so $(u_0, v_0) \in \rho$. Thus S satisfies the law $u_0 = v_0$. Therefore, since $\eta\psi : F_{\mathscr{T}}(B) \to S$ 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. □

The result shows that every variety can be defined by a set of laws, although in general this set may be infinite. This is true even for varieties of semigroups. In some cases, however, a finite set of laws is enough. Such varieties are called *finitely based.*
Let $\mathscr{T}$ be the type $(\circ, 2)$. The variety of all semigroups is defined by the law

$$x \circ (y \circ z) = (x \circ y) \circ z.$$

Since every semigroup satisfies this law, when working with varieties of semigroups we will always assume it implicitly and write xy for $x \circ y$.
Now let $\mathscr{T}$ be the type $\{(\circ, 2), ({}^{-1}, 1)\}$. Again, when working with semigroups, we assume the law $(xy)z = x(yz)$; we will also assume

$$xx^{-1}x = x \text{ and } (x^{-1})^{-1} = x.$$

Definition 9.1.25. Let $\mathscr{X}$ be a set of $\mathscr{T}$-algebras. Then the variety of $\mathscr{T}$-algebras generated by $\mathscr{X}$ is defined to be the intersection of all varieties of $\mathscr{T}$-algebras containing $\mathscr{X}$, and is simply called the variety generated by $\mathscr{X}$.

Remark 9.1.26. Let X be a set of $\mathscr{T}$-algebras. Then the variety generated by $\mathscr{X}$ consists of all $\mathscr{T}$-algebras that can be obtained from $\mathscr{X}$ by repeatedly forming subsemigroups, homomorphic images, and direct products. That is, the variety generated by $\mathscr{X}$ is

$$\{O_1 O_2 \dots O_n \mathscr{X} \,:\, n \in \mathbb{N},\ O_i \in \{\mathrm{Hom}, \mathrm{Sub}, \mathrm{Prod}\}\}.$$

For every non-empty class $\mathscr{X}$ of $\mathscr{T}$-algebras we have

$$\mathrm{Sub}\,\mathrm{Hom}\,\mathscr{X} \subseteq \mathrm{Hom}\,\mathrm{Sub}\,\mathscr{X}$$

$$\mathrm{Prod}\,\mathrm{Hom}\,\mathscr{X} \subseteq \mathrm{Hom}\,\mathrm{Prod}\,\mathscr{X}$$

$$\mathrm{Prod}\,\mathrm{Sub}\,\mathscr{X} \subseteq \mathrm{Sub}\,\mathrm{Prod}\,\mathscr{X}.$$

Proposition 9.1.2. *Let X be a class of $\mathscr{T}$-algebras. The variety generated by $\mathscr{X}$ is* $\mathrm{Hom}\,\mathrm{Sub}\,\mathrm{Prod}\,X$.

(To be continued)

10. Pseudovarieties

10.1. Psuedovarieties

10.1.1. Introduction

Let V be a variety that contains an algebra S of two elements. Then V contains the direct product of infinitely many copies of S, which is of course infinite. Hence, varieties are not useful in studying and classifying finite algebras.
Clearly, if we have a class of finite algebras, then it is closed under the operator Sub and Hom. The problem arises with the operator Prod, so we only need to modify Prod to study finite algebras. We therefore introduce a new operator on classes of $\mathscr{T}$-algebras.
Let $\mathrm{Prod}_{\mathrm{fin}}\,\mathscr{X}$ denote the class of all $\mathscr{T}$-algebras that are direct products of finite copies of the algebras in $\mathscr{X}$. That is,

$$\mathrm{Prod}_{\mathrm{fin}}\,\mathscr{X} = \{S \mid \exists\, T_1, T_2, \ldots, T_n \subseteq \mathscr{X},\ S = T_1 \times T_2 \times \cdots \times T_n\}.$$

Definition 10.1.1. A non-empty class of finite $\mathscr{T}$-algebras is called a pseudovariety if it is closed under the operations Hom, Sub, and $\mathrm{Prod}_{\mathrm{fin}}$.

That is, $\mathscr{X}$ is a pseudovariety if

$$\mathrm{Sub}\,\mathscr{X} \cup \mathrm{Hom}\,\mathscr{X} \cup \mathrm{Prod}_{\mathrm{fin}}\,\mathscr{X} \subseteq \mathscr{X}.$$

Example 10.1.2.

1. Let $1 = \{E\}$, where $E = \{e\}$ is the trivial semigroup.
2. Let Com consist of all finite commutative semigroups (viewed as $\{(0,2)\}$-algebras). Then Com is a pseudovariety.
3. Let G consist of all finite groups, viewed as $\{(0,2), ({}^{-1}, 0)\}$-algebras, then G is a pseudovariety.
4. The class I of all inverse semigroups, viewed as $\{(0,2), ({}^{-1}, 1)\}$-algebras, is a pseudovariety.
5. The class N of all nilpotent semigroups is a pseudovariety.
6. The class A of all finite aperiodic semigroups forms a pseudovariety.
7. The class S of all finite semigroups forms a pseudovariety.

Remark 10.1.3. The class G of all finite groups, viewed as $\{(0,2)\}$-algebras, is a pseudovariety. In this case, subalgebras are subgroups, as $x^m = 1$ implies $x^{-1} = x^{m-1}$. Hence, the class of finite groups viewed as $\{(0,2)\}$-algebras is a pseudovariety.

Definition 10.1.4. Let $\mathscr{X}$ be a class of finite $\mathscr{T}$-algebras. Then the intersection of all the pseudovarieties of $\mathscr{T}$-algebras containing $\mathscr{X}$ is called the pseudovariety generated by $\mathscr{X}$.

Similarly, as for varieties, the pseudovariety generated by $\mathscr{X}$ is

$$\{O_1O_2 \ldots O_n\mathscr{X} \;:\; O_i \in \{\mathrm{Hom}, \mathrm{Sub}, \mathrm{Prod_{fin}}\}\}.$$

Proposition 10.1.1. *Let $\mathscr{X}$ be a class of $\mathscr{T}$-algebras. The pseudovariety generated by $\mathscr{X}$ is* $\mathrm{Hom\,Sub\,Prod_{fin}}\,\mathscr{X}$.

10.1.2. Pseudovarieties of Semigroups

Now, we consider pseudovarieties of semigroups, that is of type $\{(0,2)\}$. Let V be a pseudovariety and $T \in \mathsf{V}$. If S is a semigroup dividing T, i.e., $S \prec T$, then there exists a subsemigroup T' of T and an epimorphism $\varphi : T' \to S$. Then, it is clear that pseudovarieties are closed under division.

Definition 10.1.5. Let V and W be two Pseudovarieties. The semidirect product V and W is defined to be the Pseudovariety generated by all the semidirect products $S \rtimes_\varphi T$, where $S \in \mathsf{V}$, $T \in \mathsf{W}$, and $\varphi : T \to \mathrm{End}(S)$ is an antihomomorphism.
We use $\mathsf{V} \rtimes \mathsf{W}$ to denote the semidirect product of V and W.

We want to show that $\rtimes$ is associative on the class of Pseudovarieties; which contrasts the fact that $\rtimes$ is not associative on the class of semigroups, for which we introduce new concepts.

Definition 10.1.6. A transformation semigroup is a pair (P, S) where P is a set and S embeds into $\mathscr{T}_P$ via a monomorphism $\alpha : S \to \mathscr{T}_P$.

Let (P, S) and (Q, T) be two transformation semigroups with embeddings $\alpha : S \to \mathscr{T}_P$ and $\beta : T \to \mathscr{T}_Q$. The wreath product of transformation semigroups (P, S) and (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 $(q)^t f = (q(t\beta))f$, where we write ${}^t f$ for $f(t\varphi)$.
[Mappings are written on right as usual, it is not f of $t\varphi$ but first φ is operated on t and then $t\varphi \in \mathrm{End}(S^Q)$ is operated on $f \in S^Q$.]
The embedding map $\delta : S^Q \rtimes_\varphi T \to \mathscr{T}_{P\times Q}$ is defined by

$$[p, q](f, t)\delta = [p(((q)f)\alpha), q(t\beta)].$$

[For clarity, we use square brackets for the elements of $P \times Q$.]

Remark 10.1.7. δ is a monomorphism. To see this, first, we have

$$\begin{aligned}
&(f_1, t_1)\delta = (f_2, t_2)\delta \\
\Longrightarrow\ &[p, q](f_1, t_1)\delta = [p, q](f_2, t_2)\delta \quad \forall\ [p, q] \in P \times Q \\
\Longrightarrow\ &[p(((q)f_1)\alpha), q(t_1\beta)] = [p(((q)f_2)\alpha), q(t_2\beta)] \\
\Longrightarrow\ &p(((q)f_1)\alpha) = p(((q)f_2)\alpha) \,\&\, q(t_1\beta) = q(t_2\beta) \quad \forall\ [p, q] \in P \times Q \\
\Longrightarrow\ &((q)f_1)\alpha = ((q)f_2)\alpha \,\&\, t_1\beta = t_2\beta \quad \forall\ q \in Q \\
\Longrightarrow\ &(q)f_1 = (q)f_2 \,\&\, t_1 = t_2 \quad \forall\ q \in Q \quad [\text{since, } \alpha, \beta \text{ are injective}] \\
\Longrightarrow\ &f_1 = f_2 \text{ and } t_1 = t_2 \\
\Longrightarrow\ &(f_1, t_1) = (f_2, t_2);
\end{aligned}$$

thus, δ is injective. Second,

$$\begin{aligned}
&[p,q]((f_1,t_1)(f_2,t_2))\delta \\
&\quad = [p,q][(f_1{}^{t_1}f_2, t_1t_2)]\delta \\
&\quad = [p(((q)f_1{}^{t_1}f_2)\alpha), q(t_1t_2)\beta] \\
&\quad = [p(((q)f_1(q)(t_1\beta)f_2)\alpha), q((t_1t_2)\beta)] \\
&\quad = [q(((q)f_1)\alpha)(((q(t_1\beta))f_2)\alpha), q(t_1\beta)(t_2\beta)] \quad \text{[since } \alpha, \beta \text{ are homomorphisms]} \\
&\quad = [p(((q)f_1)\alpha), q(t_1\beta)](f_2,t_2)\delta \\
&\quad = [p,q](f_1,t_1)\delta(f_2,t_2)\delta;
\end{aligned}$$

thus δ is a homomorphism.

A homomorphism between two transformation semigroups (P,S) and (Q,T) with embedding maps $\alpha : S \to \mathscr{T}_P$ and $\beta : T \to \mathscr{T}_Q$ 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

$$\begin{array}{ccc}
P & \xrightarrow{s\alpha} & P \\
\downarrow\varphi & & \downarrow\varphi \\
Q & \xrightarrow{s\psi\beta} & Q
\end{array} \tag{10.1}$$

An isomorphism between (P,S) and (Q,T) is a homomorphism (φ,ψ) where both φ and ψ are bijective.

Lemma 10.1.2. *For any three transformation semigroups (P,S), (Q,T), and (R,U), the wreath product*

$$((P,S) \wr (Q,T)) \wr (R,U) \text{ and } (P,S) \wr ((Q,T) \wr (R,U))$$

are isomorphic.

Proof. Suppose that the transformation semigroups (P,S), (Q,T), and (R,U) have embedding maps $\alpha : S \to \mathscr{T}_P$, $\beta : T \to \mathscr{T}_Q$, and $\gamma : U \to \mathscr{T}_R$. We have to show that the transformation semigroups

$$((P\times Q)\times R, (S^Q \rtimes T)^R \rtimes U) \text{ and } (P\times(Q\times R), S^{Q\times R} \rtimes (T^R \times U))$$

are isomorphic. Let these transformation semigroups have embedding maps ζ and η, respectively, and let the transformation semigroup $(P,S)\wr(Q,T)$ and $(Q,T)\wr(R,U)$ (that is, $(P\times Q, S^Q \rtimes T)$ and $(Q\times R, T^R \rtimes U)$) have embedding map δ and ρ, respectively.
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

$$\psi : (S^Q \rtimes T)^R \times U \to S^{Q\times R} \rtimes (T^R \times U)$$

as follows. For $f \in (S^Q \rtimes T)^R$ 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

$$[p,q]((r)f)\delta = [p(([\_,r]g)\alpha), q((rh)\beta)]$$

for any $[p,q] \in P\times Q$ 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

$$\begin{aligned}
[[p,q],r](f,u)\zeta &= [[p,q]((r)f)\delta, r(u\gamma)] \\
&= [[p(([q,r]g)\alpha), q(((r)h)\beta)], r(u\gamma)],
\end{aligned}$$

while

$$\begin{aligned}[p,[q,r]](g,(h,u))\eta &= [p(([q,r]g)\alpha),[q,r](h,u)\rho] \\ &= [p(([q,r]g)\alpha),[q(((r)h)\beta),r(u\gamma)]].\end{aligned}$$

Thus $x(\zeta\varphi) = (x\varphi)(\psi\eta)$ for all $x \in (P \times Q) \times R$ and $s \in (S^Q \rtimes T)^R \rtimes U$; that is, the diagram 10.1 commutes.

Now let $f, f' \in (S^Q \times T)^R$ and $u, u' \in U$. Then

$$\begin{aligned}[p,q]((r)f^u f')\delta &= [p,q]((r)f(r(u\gamma))f')\delta \\ &= [p,q]((r)f)\delta((r(u\gamma))f')\delta \\ &= [p(([\_,r]g)\alpha),q(((r)h)\beta)]((r(u\gamma))f')\delta \\ &= [p(([\_,r]g)\alpha)(([\_,r(u\gamma)]g')\alpha),q(((r)h)\beta)(((r(u\gamma))h')\beta)] \\ &= [p(([\_,r]g[\_,r(u\gamma)]g')\alpha),q(((r)h(r(u\gamma))h')\beta)] \\ &= [p(([\_,r]g[\_(((r)h)\beta),r(u\gamma)]g')\alpha),((q(r)h(r(u\gamma))h')\beta)] \\ &= [p(([\_,r]g[\_,r]^{(h,u)}g')\alpha),q(((r)h()^u h')\beta)] \\ &= [p(([\_,r]g^{(h,u)g'})\alpha),q(((r)h^u h')\beta)].\end{aligned}$$

Combining this with the definition of δ to see that ψ is a homomorphism.

The maps φ and ψ are clearly bijective from their definitions. Hence (φ,ψ) is an isomorphism. $\square$

Lemma 10.1.3. *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*

$$(S_1 \rtimes_{\varphi_1} T_1) \times (S_2 \rtimes_{\varphi_2} T_2) \cong (S_1 \times S_2) \rtimes_{\psi} (T_1 \times T_2),$$

where the left action of $T_1 \times T_2$ on $S_1 \times S_2$ is defined by

$$^{(t_1,t_2)}(s_1,s_2) = ({}^{t_1}s_1, {}^{t_2}s_2).$$

Proof. 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,

$$
\begin{aligned}
&[((s_1,t_1),(s_2,t_2))((s_1',t_1'),(s_2',t_2'))]\vartheta \\
&\qquad = [((s_1,t_1)(s_1',t_1'),(s_2,t_2)(s_2',t_2'))]\vartheta \\
&\qquad\qquad [\text{multiplication in the direct product } (S_1 \rtimes_{\varphi_1} T_1) \times (S_2 \rtimes_{\varphi_2} T_2)] \\
&\qquad = [(s_1{}^{t_1}s_1', t_1t_1'),(s_2{}^{t_2}s_2', t_2t_2')]\vartheta \\
&\qquad\qquad [\text{multiplication in the semidirect products } (S_1 \rtimes_{\varphi_1} T_1) \text{ and} (S_2 \rtimes_{\varphi_2} T_2)] \\
&\qquad = ((s_1{}^{t_1}s_1', s_2{}^{t_2}s_2'),(t_1t_1', t_2t_2')) \qquad [\text{by definition of } \vartheta] \\
&\qquad = ((s_1,s_2)({}^{t_1}s_1', {}^{t_2}s_2'),(t_1,t_2)(t_1',t_2')) \\
&\qquad\qquad [\text{factoring in the direct products } (S_1 \times S_2) \text{ and } (T_1 \times T_2)] \\
&\qquad = ((s_1,s_2)^{(t_1,t_2)}(s_1',s_2'),(t_1,t_2)(t_1',t_2')) \\
&\qquad\qquad [\text{definition of the action of } T_1 \times T_2 \text{ on } S_1 \times S_2] \\
&\qquad = [(s_1,s_2),(t_1,t_2)][(s_1',s_2'),(t_1',t_2')] \\
&\qquad\qquad [\text{factoring in the semidirect product } (S_1 \times S_2) \rtimes_\psi (T_1 \times T_2)] \\
&\qquad = [((s_1,t_1),(s_2,t_2))]\vartheta[((s_1',t_1'),(s_2',t_2'))]\vartheta;
\end{aligned}
$$

thus ϑ is a homomorphism and so an isomorphism. □

Lemma 10.1.4. *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. Let $\mathscr{X} = \{S \rtimes_\varphi T : S \in \mathsf{V}, T \in \mathsf{W}\}$. So $\mathsf{V} \times \mathsf{W}$ is, by definition, the pseudovariety generated by $\mathscr{X}$; hence $\mathsf{V} \rtimes \mathsf{W} = \mathrm{HomSub}\,\mathrm{Prod}_{\mathrm{fin}}\,\mathscr{X}$ by Proposition 10.1.1.
Let $U \in \mathrm{Prod}_{\mathrm{fin}}\,\mathscr{X}$. So

$$U = \prod_{i \in I} (S_i \rtimes_{\varphi_i} T_i)$$

where each $S_i \rtimes_{\varphi_i} T_i$ is in $\mathscr{X}$ and I is a finite index set. By Lemma 10.1.3,

$$U \cong \left(\prod_{i \in I} S_i\right) \rtimes_\psi \left(\prod_{i \in I} T_i\right).$$

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 $U \in \mathscr{X}$. Thus $\mathrm{Prod}_{\mathrm{fin}}\,\mathscr{X} \subseteq \mathscr{X}$. The opposite inclusion is obvious, so $\mathrm{Prod}_{\mathrm{fin}}\,\mathscr{X} = \mathscr{X}$.
Therefore $\mathsf{V} \rtimes \mathsf{W} = \mathrm{HomSub}\,\mathscr{X}$, and so $\mathsf{V} \times \mathsf{W}$ consists of all divisors of semidirect products $S \rtimes_\varphi T$, where $S \in \mathsf{V}$ and $T \in \mathsf{W}$. □

Lemma 10.1.5. *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. I will skip the proof for now but preceeding lemma can be used to prove it. □

As a consequence of Lemma 10.1.5, we have the following result:

Proposition 10.1.6. *The semidirect product of pseudovarieties is associative.*

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

$$S = \bigcup_{i=0}^{n} \left(G \rtimes \prod_{j=0}^{n} (A \rtimes G) \right).$$

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 $\mathsf{V} \wedge \mathsf{W} = \mathsf{V} \cap \mathsf{W}$; it is easy to prove that $\mathsf{V} \wedge \mathsf{W}$ is a pseudovariety.

Proposition 10.1.7. *The class of pseudovarieties of semigroups is a lattice with operations meet $\wedge$ and join $\vee$.*

10.2. Semigroups and Topology

10.2.1. Free Objects

Consider the pseudovariety N of nilpotent semigroups. Let, for any finite alphabet A, $I_n = \{w \in A^+ \mid |w| \geq n\}$. Then A^+/I_n is a nilpotent semigroup. Hence, $A^+/I_n \in \mathsf{N}$. Thus, N contains arbitrarily large A-generated semigroups. Since an A-generated free object for N may 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 $\mathscr{X}$ should be just general enough to be more general than any A-generated object in $\mathscr{X}$. 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 $\operatorname{im}\varphi_1$ generates S_1 and $\operatorname{im}\varphi_2$ 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:

$$\begin{tikzcd}
 & A \arrow[dl, "\varphi_1"'] \arrow[d, "\varphi"] \arrow[dr, "\varphi_2"] & \\
S_1 & T \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] & S_2
\end{tikzcd}$$

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.

10.2.2. Topologies on Semigroups

A poset $(I, \leq)$ is a *directed set* if every pair of elements of I has an upper bound.

Definition 10.2.1. A *topological semigroup* is a semigroup equipped with a topology such that the multiplication is a continuous map.

Any semigroup can be equipped with the discrete topology and hence becomes a topological semigroup.
For any alphabet A, an *A-generated topological semigroup* is a pair (A, φ), where S is a topological semigroup and $\varphi : S \to A$ is a map such that $\operatorname{im}\varphi$ generates a dense subsemigroup of S. We will often denote such an A-generated topological semigroup my 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 $\varphi_1\psi = \varphi_2$.

Definition 10.2.2. A *projective system* is a collection of A-generated topological semigroups $\{\varphi_i : A \to S_i \mid i \in I\}$, 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;

$$\text{for each } i \in I, \lambda_{i,j} \text{ is the identity map;}$$

$$\forall\ i, j, k \in I \text{ with } i \geq j \geq k,\ \lambda_{i,j}\lambda_{j,k} = \lambda_{i,k}.$$

Definition 10.2.3. Let $\{\varphi_i : A \to S_i \mid i \in I\}$ be a projective system. Then, the *projective limit* of this system is an A-generated topological semigroup $\Phi : A \to S$ equipped with homomorphism $\Phi_i : S \to S_i$ 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 $i \geq j$, $\Phi_i\lambda_{i,j} = \Phi_j$;

2. if there is an A-generated topological semigroup $\Psi : A \to T$ and homomorphisms $\Psi_i : A \to S_i$ from $\Psi : A \to T$ to $\varphi_i : A \to S_i$ such that for all $i, j \in I$ with $i \geq j$, we have $\Psi_i\lambda_{i,j} = \Psi_j$, then there is a homomorphism Θ from $\Psi : A \to T$ to $\Phi : A \to S$ such that $\Theta\Phi_i = \Psi$. That is, the following diagram commutes

$$\begin{tikzcd}
 & A \arrow[d, bend right, "\Psi"'] \arrow[dd, bend left, "\Phi"] \arrow[dddl, bend right, "\varphi_i"'] \arrow[dddr, bend left, "\varphi_j"] & \\
 & T \arrow[d, dashed, "\Theta"] \arrow[ddl, "\Psi_i"'] \arrow[ddr, "\Psi_j"] & \\
 & S \arrow[dl, "\Phi_i"] \arrow[dr, "\Phi_j"'] & \\
S_i \arrow[rr, "\lambda_{i,j}"'] & & S_j
\end{tikzcd}$$

Remark 10.2.4. The projective limit is unique (up to isomorphism). To see this, let

$$\Phi : A \to S \qquad \text{and} \qquad \Phi' : A \to S'$$

be two projective limits of the projective system $\{\phi_i : A \to S_i \mid i \in I\}$. By the property 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

$$\Phi\Theta\Theta' = \Phi \quad \text{and} \quad \Phi'\Theta'\Theta = \Phi';$$

hence $\Theta\Theta' \mid_{A\Phi} = \mathrm{id}_{A\Phi}$ and $\Theta'\Theta \mid_{A\Phi'} = \mathrm{id}_{A\Phi'}$.
Hence $\Theta\Theta'$ restricts to the identity on the subsemigroup generated by $A\Phi$ is the identity map; since this subsemigroup is dense in S and Θ, 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 $\Phi' : A \to S'$, as required.