Chapter 1

Introduction

1.1 Basics

Definition 1.1.1 Suppose S is a semigroup, we have the following brief definitions:

(1) S is a null semigroup if $\forall x, y \in S(xy = 0)$;

(2) S is a left zero semigroup if $\forall x, y \in S(xy = x)$, dually one can define a right zero semigroup;

(3) $I \subset S$ is a proper ideal if $\{0\} \subset I \subsetneq S$ and $IS \subset S \wedge SI \subset S$;

(4) given a set X, the full transformation semigroup is defined as $(\mathrm{End}_{\mathsf{Set}}(X), \circ)$, where $\circ$ refers the composition of functions;

(5) a morphism $S \xrightarrow[\mathsf{Smg}]{\phi} \mathrm{End}(X)$ is a *representation* of S, and φ is faithful if it is injective;

(6) S is a rectangular band if $\forall a, b \in S(aba = a)$;

(7) $\langle a \rangle := \langle \{a\} \rangle_{\mathrm{smg}}$ is called a *monogenic semigroup.*

Proposition 1.1.2 Let S be a semigroup, the statements listed below are equivalent.

(1) S is a group;

(2) for all $a, b \in S$, there exists $x, y \in S$ such that $ax = b \wedge ya = b$;

(3) $\forall a \in S(aS = Sa = S)$.

Proof. It is easy to verify that (1) $\Rightarrow$ (3) and (2) $\Leftrightarrow$ (3). So we proceed to prove (3) $\Rightarrow$ (1), and it is suffices to show that S has the unique identity, and that for any element, its inverse exists and is unique. Let $ax = ya = a$, then

$$x = ax_1 = ay_1a = yay_1a = yx = ax_2ax = ax_2a = y_2a = y.$$

Thus, every element a in S has an identity ϵ_a such that $\epsilon_a a = a\epsilon_a = a$. Now, the issue lies in proving $\epsilon_a = \epsilon_b$ for any a, b in S, and the method is analogous:

$$\epsilon_a = by_1 = by_2b = by_2b\epsilon_b = \epsilon_a\epsilon_b = \epsilon_a ax_2a = ax_2a = x_1a = \epsilon_b.$$

As for the existence and uniqueness of inverse, it also follows the same manner, so we omit it here. $\square$

Theorem 1.1.3 Suppose that S is a semigroup and that $X = S^1$, then there exists a faithful representation

$$\varphi : S \to \mathrm{End}(X).$$

Proof. See [1, Theorem 1.1.2]. Simply stated,

$$\begin{aligned} S &\hookrightarrow \mathrm{End}(S^1) \\ a &\longmapsto [\varphi_a : x \mapsto xa]\,. \end{aligned}$$

□

Theorem 1.1.4 Let S be a semigroup, the following propositions are equivalent:

- ◇ S is a rectangular band;
- ◇ every $a \in S$ is an idempotent, and $abc = ac$ for all a, b, c in S;
- ◇ there exists a left zero semigroup L, and a right zero semigroup R, such that $S \simeq L \times R$;
- ◇ there exists two sets A, B such that $S \simeq A \times B$, in witch $A \times B$ is a semigroup with the multiplication defined as $(a_1, b_1)(a_2, b_2) = (a_1, b_2)$.

Proof. See [1, Theorem 1.1.3]. □

1.2 Monogenic Subsemigroup

To study the monogenic subsemigroup, we introduce the following concepts. Suppose a is an element in S, which has a finite order if not specified.

Definition 1.2.1

(1) $\langle a \rangle := \langle \{a\} \rangle_{\mathrm{smg}}$;

(2) $\mathrm{ord}(a) := |\langle a \rangle|$;

(3) $\mathrm{idx}(a) := \min\{m \in \mathbb{Z}_{\geq 1} : \exists n \in \mathbb{Z}_{\geq 1}(a^m = a^n \wedge m \neq n)\}$;

(4) a semigroup is called *periodic* if all its elements are of finite order.

Let $m = \mathrm{idx}(a)$, $r = \mathrm{prd}$, clearly, $a, a^2, \cdots, a^{m+r-1}$ are mutually different, and $\langle a \rangle = \{a, \cdots, a^{m+r-1}\}$.

Let K_a be $\{a^m, \cdots, a^{m+r-1}\}$, we assert that it is a cyclic group. Consider the quotient ring $\mathbb{Z}/r\mathbb{Z}$, obviously, $\{[m], \cdots, [m + r - 1]\} = \mathbb{Z}/r\mathbb{Z}$. Thus, there exists $0 \leq g \leq r - 1$ such that $[m + g] = [1]$, which implies $\forall k([k] = [k(m + g)])$. Since $a^{(m+g)k} = a^{m+hr}a^{k-m} = a^m a^{k-m}$ for all $k > m$, the $a^{(m+g)k}$ exhaust K_a.

Proposition 1.2.2 Suppose a and b are elements of finite order in the same or different subsemigroups, then

$$\langle a \rangle \simeq \langle b \rangle \Leftrightarrow (\mathrm{idx}(a), \mathrm{prd}(a)) = (\mathrm{idx}(b), \mathrm{prd}(b)).$$

Proof. Suppose $\mathrm{idx}(a) = \mathrm{idx}(b) = m$ and $\mathrm{prd}(a) = \mathrm{ord}(b) = r$, the mapping defined below is an isomorphism.

$$\begin{aligned} \{a, \cdots, a^{m+r-1}\} &\xrightarrow{\sim} \{b, \cdots, b^{m+r-1}\} \\ a^k &\longmapsto b^k \end{aligned}$$

For the reverse, assume $\langle a \rangle \xrightarrow[\phi]{\sim} \langle b \rangle$, where ϕ maps a to b^ξ, it is straightforward to verify that $\langle b^\xi \rangle = \langle b \rangle$ and that $\mathrm{idx}(a) = \mathrm{idx}(b^\xi)$ and $\mathrm{prd}(a) = \mathrm{prd}(b^\xi)$. If $\xi = 1$, the proof is over. Otherwise, if $\xi > 1$, then there exists $\mu \geq 1$ such that $b^{\xi\mu} = b$, thus $\mathrm{idx}(b) = 1$, which implies $\langle b \rangle$ is a cyclic group. Hence, $\langle a \rangle$ is also a cyclic group with the generator $\phi^{-1}(b) = a^\zeta$. Since a is a generator, similarly, there exists an integer ν that makes $a^{\zeta\nu} = a$, and it follows that $\mathrm{idx}(a) = 1$. Thereby, $\mathrm{prd}(a) = |\langle a \rangle| = |\langle b \rangle| = \mathrm{prd}(b)$. □

Proposition 1.2.3 For any pair $(m, r) \in \mathbb{Z}^2_{\geq 1}$, there exists a semigroup S containing an element with idx of m and prd of r.

Proof. See [1, p.12]. Simply stated, the correspondence is given by $(m, r) \mapsto (12 \cdots m + 1) \in S_{m+r}$. □

1.3 Relations

Given a set X, the power set $P(X^2)$ equipped with the multiplication defined as

$$R_1 \circ R_2 := \left\{(a,b) \in X^2 : \exists c \in X((a,c) \in R_1) \wedge (c,b) \in R_2\right\},$$

where R_i is the element in $P(X^2)$, forms a semigroup. To see this, it is suffices to verify $\circ$ is associative, which is obvious. Besides this, some brief definitions are listed as follows:

Definition 1.3.1

(1) $R(x) := \{y \in X : (x,y) \in R\}$;

(2) $R(A) := \bigcup_{x \in A} R(x)$;

(3) $R^{\mathrm{op}} := \{(y,x) : (x,y) \in R\}$;

(4) $\Delta_X : \{(x,x) : x \in X\}$;

(5) if it is not specified, R^n represents $R \circ \cdots \circ R$ (n times);

(6) given a morphism $f : S \to S'$, then $\ker f := \{(x,y) \in S^2 : f(x) = f(y)\}$.

It can be easily verified that $(R_1 \circ R_2)^{\mathrm{op}} = R_2^{\mathrm{op}} \circ R_1^{\mathrm{op}}$, thus, $(R^n)^{\mathrm{op}} = (R^{\mathrm{op}})^n$. A commonly used conclusion is

$$(a,b) \in R^n \Leftrightarrow \exists (t_i)_{i=1}^n \in X^n \left(a = t_1 \to t_2 \to \cdots \to t_n = b\right),$$

where $t_i \to t_{i+1}$ means $t_i R t_{i+1}$.

We then introduce the definitions of partial orders and equivalent relations from this perspective.

Definition 1.3.2 A partial order is a relation satisfies the following conditions:

- ⋄ (reflective) $\Delta_X \subset R$;
- ⋄ (anti-symmetric) $R \cap R^{\mathrm{op}} = \Delta_X$;
- ⋄ (transitive) $R^2 \subset R$.

Besides, an equivalence relation satisfies:

- ⋄ (reflective) $\Delta_X \subset R$;
- ⋄ (symmetric) $R^{\mathrm{op}} \subset R$;
- ⋄ (transitive) $R^2 \subset R$.

Definition 1.3.3 Let $(S, \leq)$ be a partial-ordered set, U is a subset of S.

(1) $\min U$ is the minimal element of U if $\min U \in U$ and $\nexists a \in U(a < \min U)$;

(2) $\min^* U$ is the minimum element of U if $\min^* U \in U$ and $\forall a \in U(\min^* U \leq a)$;

(3) l is the lower bound of U if $\forall a \in U(l \leq a)$;

(4) $\inf U := \max^*\{l : \text{lower bounds of U}\}$ is the infimum of U;

(5) we say that S satisfies *minimal condition* if every nonempty subset of it has a minimal element;

(6) we say that S is a *complete lower semilattice* if $\forall U \subset X(\exists \inf U)$, and is a *lower semilattice* if $\forall \{x,y\} \subset X(\exists \inf\{x,y\})$;

(7) if S is a lower semilattice, the operation $(x,y) \mapsto \inf\{x,y\}$, as a binary function, denoted as $(\cdot) \wedge (\cdot)$, satisfies the condition of associativity; and for the upper-case, we denote $x \vee y$ by $\sup\{x,y\}$;

(8) we say that S is a *lattice* if it's both an upper semilattice and a lower semilattice.

Proposition 1.3.4 A semilattice $(S, \leq, \wedge)$ satisfies the following conditions:

- $\forall x \in S(x \wedge x = x)$;
- $\forall x, y \in S(x \wedge y = y \wedge x)$
- $\forall x, y, z \in S((x \wedge y) \wedge z = x \wedge (y \wedge z))$;
- $\forall x, y \in S(x = x \wedge y \Leftrightarrow x \leq y)$.

Thus, $(S, \wedge)$ forms a commutative semigroup, in which every element is idempotent. Conversely, suppose $(S, \cdot)$ is a semigroup satisfies

- $\forall x \in S(xx = x)$;
- $\forall x, y \in S(xy = yx)$;

then we can define a partial-order that $x \leq y \Leftrightarrow x = x \cdot y$. And so $(S, \leq, \cdot)$ forms a semilattice, where $x \cdot y = \inf\{x, y\}$.

Proposition 1.3.5 Given a set X, a partition $\mathcal{A}$ is a family of disjoint subsets of X satisfying $\bigsqcup \mathcal{A} = X$. There exists a bijection

$$\{R \in P(X^2) : \text{equivalence relation}\} \xleftrightarrow{1:1} \{\mathcal{A} \in P(X) : \text{partition}\}$$

$$R \longmapsto \{R(x)\}_{x \in X}$$

$$[R : (x, y) \in R \Leftrightarrow \exists A \in \mathcal{A}(x \in A \wedge y \in A)] \longleftarrow\!\shortmid \mathcal{A}$$

1.4 Congruences

Definition 1.4.1 Let $(S, \cdot)$ be a semigroup, R is a relation on S. We have the following operations:

(1) $aR = a \cdot R := \{(ax, ay) : (x, y) \in R\}$, dually, $Ra := \{(xa, ya) : (x, y) \in R\}$, in addition, $aRb := \{(axb, ayb) : (x, y) \in R\}$;

(2) $S^1R = S^1 \cdot R := \bigcup_{a \in S^1} aR$, $S^1RS^1 = \bigcup_{(a,b) \in S^1 \times S^1} aRb$;

(3) $RR = R \cdot R := \{(x_1x_2, y_1y_2) : (x_i, y_i) \in R \wedge i \in \{1, 2\}\}$; furthermore, $R^{\cdot n} := R \cdot R \cdots R$ (n times).

Definition 1.4.2 (...)

(1) R is *left compatible* if $S^1R \subset R$;

(2) dually, R is *right compatible* if $RS^1 \subset R$;

(3) R is a *congruence* (R is compatible) if $S^1R \subset R \wedge RS^1 \subset R$, which is equivalent to $RR \subset R$.

The proof for the last assertion (3) is as follows. Since $\Delta_S \subset R$, $RR \subset R$ for any $a \in S^1$ and $(x, y) \in S$, $(ax, ay) \in R$. Conversely, assume $(x_1x_2, y_1y_2) \in RR$. Since $S^1R \subset R \wedge RS^1 \subset R$, we obtain that $(x_1x_2, x_1y_2) \in R$ and $(x_1y_2, x_2y_2) \in R$. Thus, $(x_1x_2, y_1y_2) \in R$.

The conclusion below is often used in algebra, especially in situations where an equivalence relation and some operations are imposed on a set to give it an algebraic structure, for example, ideal of rings, the construction of amalgamated product and the construction of tensor product. Its core, precisely, is the concept of congruence in semigroup theory.

Proposition 1.4.3 Suppose R is an equivalence relation on a semigroup S, then

$$R(x)R(y) := R(xy) \text{ well defined} \Leftrightarrow R \text{ is a congruence.}$$

Proposition 1.4.4 The way to construct a certain relation is as follows.

(1) $\langle R\rangle_{\text{eqv}} := \bigcup_{n\in\mathbb{Z}_{\geq 1}} [R\cup\Delta_S\cup R^{\text{op}}]^n$ is the smallest equivalence relation containing R, where S can just be a set;

(2) $\langle R\rangle_{\text{cpt}} := S^1RS^1$ is the smallest compatible relation containing R;

(3) $\langle R\rangle_{\text{cge}} := \left\langle S^1RS^1\right\rangle_{\text{eqv}}$ is the smallest congruence containing R.

Both set $\text{Eqv}(S)$ of equivalences and $\text{Cge}(S)$ of congruences on S are partially ordered by $\subset$. In fact, both are complete lattice. Take $\text{Cge}(S)$ as an example, for any subset $\mathcal{U}\subset\text{Cge}(S)$, it can be verified that $\inf\mathcal{U} = \bigcap\mathcal{U}$ and $\sup\mathcal{U} = \langle\bigcup\mathcal{U}\rangle_{\text{cge}}$. Notice that for any $R_1, R_2\in\text{Cge}(S)$

$$\langle R_1\cup R_2\rangle_{\text{cge}} = \langle R_1\cup R_2\rangle_{\text{eqv}}\,, \tag{1.1}$$

so, both symbol $\wedge$ and $\vee$ on lattice $\text{Eqv}(S)$ and $\text{Eqv}(S)$ represent the same operations of sets.

Proposition 1.4.5 Suppose R_1, R_2 are equivalences, then

- $R_1\vee R_2 = \langle R_1\cup R_2\rangle_{\text{eqv}} = \bigcup_{n\in\mathbb{Z}_{\geq 1}}(R_1\cup R_2)^n = \bigcup_{n\in\mathbb{Z}_{\geq 1}}(R_1\circ R_2)^n$;
- $R_1\circ R_2 = R_2\circ R_1 \Rightarrow R_1\vee R_2 = R_1\circ R_2$.

Proof. See [1, p.28]. □

1.5 Ideals

Definition 1.5.1 Let S be a semigroup and $I\in\text{Idl}(S)$ be a proper ideal, then

(1) re is a mapping from the set of proper ideal of S to $\text{Cge}(S)$, which is given by $I\mapsto I^2\cup\Delta_S =: \text{re}(I)$;

(2) elements in $\operatorname{im}\text{re}$ are called *Rees ideals*;

(3) a morphism ϕ is called a *Ress morphism* if $\ker\phi$ is a Ress ideal.

Based on this, we obtain some properties.

Proposition 1.5.2

(1) Every $\text{re}(I)$ is a congruence, thus,

(2) $S/\text{re}(I) = \{I\}\sqcup\{\{x\} : x\in S\smallsetminus I\}$ forms a semigroup;

(3) $I\in S/\text{re}(I)$ is a zero element;

(4) suppose I is a proper ideal, there exists a bijection

$$\begin{aligned}\{I\subset J\subsetneq S:\ \text{ideal}\} &\xleftrightarrow{1:1} \{\bar{J}\subset S/\text{re}(I):\ \text{ideal}\}\\ J &\longmapsto \text{re}\,I(J)\\ (\text{re}\,I)^{-1}(\bar{J}) &\longleftarrow\!\shortmid \bar{J}.\end{aligned}$$

1.6 Free Semigroup

The definition of free semigroup is similar to other algebraic structures, that is, the initial object in the comma category (j_X, U). To be specific, $(\mathbf{F}(X),\iota)$ is the free semigroup of set X, if for any (S,f), where S is a semigroup and $f: X\to S$ is a function, there exists unique semigroup morphism ϕ that makes the following diagram commutes.

$$\begin{tikzcd} X \arrow[r, "\iota"] \arrow[dr, "f"'] & \mathbf{F}(X) \arrow[d, "\exists!"', "\phi"] \\ & S \end{tikzcd}$$

The construction is also straightforward, we omit it here.

Definition 1.6.1 Suppose Y is a relation on free semigroup $\mathbf{F}(X)$, let

$$\langle X|Y\rangle := \mathbf{F}(X)/\left\langle Y\right\rangle_{\text{cge}}.$$

If there exists an epimorphism $\phi : \mathbf{F}(X) \to S$, a semigroup, such that $\ker\phi = \langle Y\rangle_{\text{cge}}$, and hence $\langle X|Y\rangle \simeq S$, we say that S is presented.

Bibliography

[1] John M Howie. *Fundamentals of Semigroup Theory.* Oxford University Press, 1995.