Chapter 1

Introduction

1.1 Basics

Some brief definitions are listed as follows.

(11BD1) S is a null semigroup if $\forall x, y \in S(xy = 0)$,

(11BD2) S is a left zero semigroup if $\forall x, y \in S(xy = x)$, the definition for right zero semigroup is obvious,

(11BD3) $I \subset S$ is a proper ideal if $\{0\} \subset I \subsetneq S$ and $IS \subset S \wedge SI \subset S$,

(11BD4) given a set X, the full transformation semigroup is defined as $(\mathrm{End}_{\mathsf{Set}}(X), \circ)$, where $\circ$ refers the composition of functions,

(11BD5) a morphism $S \xrightarrow[\mathsf{Smg}]{\phi} \mathrm{End}(X)$ is a *representation* of S, and φ is faithful if it is injective,

(11BD6) a semigroup S is a rectangular band if $\forall a, b \in S(aba = a)$,

(11BD7) $\langle\{a\}\rangle_{\mathrm{smg}}$ is called a *monogenic semigroup*.

Proposition 1.1.1 Suppose S is a semigroup, the propositions listed below are equivalent.

(a) S is a group,

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

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

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

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

Thus, we may conclude that 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 1.1.2 Suppose S is a semigroup, $X = S^1$, 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 1.1.3 Suppose S is a semigroup, the following propositions are equivalent.

- ◇ S is a rectangular band (11BD6),
- ◇ 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, and its order is finite if not specified.

(12MSD1) $\langle a \rangle := \langle \{a\} \rangle_{\mathrm{smg}}$,

(12MSD2) $\mathrm{ord}(a) := |\langle a \rangle|$,

(12MSD3) $\mathrm{idx}(a) := \min\{m \in \mathbb{Z}_{\geq 1} : \exists n \in \mathbb{Z}_{\geq 1}(a^m = a^n \wedge m \neq n)\}$,

(12MSD4) $\mathrm{prd}(a) := \min\{r \in \mathbb{Z}_{\geq 1} : a^{m+r} = a^m\}$,

(12MSD5) 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 1.2.1 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 $\mathrm{idx}(a) = \mathrm{idx}(b^\xi)$, $\mathrm{prd}(a) = \mathrm{prd}(b^\xi)$. If $\xi = 1$, the proof is over. On the other hand, 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 $\mathrm{idx}(a) = 1$. Furthermore, observe that $\mathrm{prd}(a) = |\langle a \rangle| = |\langle b \rangle| = \mathrm{prd}(b)$. □

Proposition 1.2.2 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. Some brief definitions are listed as follows.

(13RD1) $R(x) := \{y \in X : (x,y) \in R\}$,

(13RD2) $R(A) := \bigcup_{x \in A} R(x)$,

(13RD3) $R^{\mathrm{op}} := \{(y,x) : (x,y) \in R\}$,

(13RD4) $\Delta_X : \{(x,x) : x \in X\}$,

(13RD5) if it is not specified, R^n represents $R \circ \cdots \circ R$ (n times).

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. 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) $R^2 \subset R$.

On another hand, R is an equivalence relation is the conditions below are all hold,

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

Given a partial ordered set X, we have the following concepts, note that the definition of max/supre/upper-case is analogous.

- Suppose $U \subset X$, $m \in U$ is the *minimal* element if $\nexists a \in U(a < m)$,
- suppose $U \subset X$, $m \in U$ is the *minimum* element if $\forall a \in U(m \leq a)$,
- suppose $U \subset X$, $l \in X$ is the *lower bound* of U if $\forall a \in U(l \leq a)$.
- We say that X satisfies *minimal condition* if every nonempty subset of it has a minimal element.
- Suppose $U \subset X$, $i \in X$ is the *infimum*, denoted as $\inf U$, if i is the maximum element of all lower bounds of U.
- We say that X is a *complete lower semilattice* if $\forall U \subset X(\exists \inf U)$, and is a *lower semilattice* if $\forall \{x,y\} \subset X(\exists \inf\{x,y\})$. If X is a lower semilattice, the operation $(x,y) \mapsto \inf\{x,y\}$ forms a binary function, denoted as $(\cdot) \wedge (\cdot)$, as for the upper-case, we denote $x \vee y$ by $\sup\{x,y\}$.
- We say that X is a *lattice* if it's both an upper semilattice and a lower semilattice.

In addition, in a lower semilattice, it can be verified that

- $x \leq y \Leftrightarrow x = x \wedge y$,
- $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, that is, $(X, \wedge)$ forms a semigroup.

Proposition 1.3.1 Given a set X, a partition $\mathcal{A}$ is a family of disjoint subsets of X satisfying $\bigsqcup \mathcal{A} = X$. Then, there exists a bijection

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

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

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

1.4 Congruences

Let S be a semigroup, R is a relation on S, we define some notations for convenient:

(14SRD1) $aR = a \cdot R := \{(ax, ay) : (x, y) \in R\}$, for the reverse, $Ra := \{(xa, ya) : (x, y) \in R\}$, in addition, $aRb := \{(axb, ayb) : (x, y) \in R\}$.

(14SRD2) $S^1R = S^1 \cdot R := \bigcup_{a\in S^1} aR$, the definition of RS^1 is analogous, furthermore, S^1RS^1 represents $\bigcup_{(a,b)\in S^1\times S^1} aRb$.

(14SRD3) $RR = R \cdot R := \{(x_1x_2, y_1y_2) : (x_i, y_i) \in R \wedge i \in \{1, 2\}\}$,

(14SRD4) $R^{\cdot n} := R \cdot R \cdots R$ (n times).

Definition 1.4.1

- We say that R is *left compatible* if $S^1R \subset R$, similar to *right compatible*.
- We say that R is *compatible* if $S^1R \subset R \wedge RS^1 \subset R$.

We assert that the last definition above, $S^1R \subset R \wedge RS^1 \subset R$, is equivalent to $RR \subset R$. Since $\Delta_S \subset R$, $RR \subset R$ ensures for all $a \in S^1$ 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 colimit of a functor from a small filtered category to the category of rings (see [2, §4.8, §5.5]). Its core, precisely, is the concept of congruence in semigroup theory.

Proposition 1.4.2 Suppose R is an equivalence relation on a semigroup S, then

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

The following constructions are also important.

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

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

(c) $\langle R\rangle_{\text{cog}} := \langle S^1RS^1\rangle_{\text{eqv}}$ is the smallest congruence containing R.

Proof. The proof for (a) is on [1, Proposition 1.4.9], the proof for (b) and (c) can be found in p.25-p.26 in the same book. □

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

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

Thus, both symbol $\wedge$ and $\vee$ on lattice $\text{Eqv}(S)$ and $\text{Eqv}(S)$ represent the same operations of sets. Some conclusions can be found in [1, p.28], Suppose R_1, R_2 are equivalences, then

(14CP1) $R_1 \vee R_2 = \langle R_1 \cup R_2\rangle_{\text{eqv}} = \bigcup_{n\in\mathbb{Z}_{\geq 1}} (R_1 \cup R_2)^n = \bigcup_{n\in\mathbb{Z}_{\geq 1}} (R_1 \circ R_2)^n$,

(14CP2) $R_1 \circ R_2 = R_2 \circ R_1 \Rightarrow R_1 \vee R_2 = R_1 \circ R_2$.

1.5 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 1.5.1 Suppose Y is a relation on free semigroup $\mathbf{F}(X)$, let

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

If there exists an epimorphism $\phi : \mathbf{F}(X) \to S$, a semigroup, such that $\ker\phi = \langle Y\rangle_{\text{cog}}$, 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 (cit. on pp. 2, 4).

[2] 李文威. *代数学方法*. 北京大学出版社, 2023 (cit. on p. 4).