Fundamentals of Semigroup Theory

Hyapp

2022-5-27

1 Introductory ideas

The definitions will be refer to all book, but 1.8 is refered to only in Section 3.5.

Throughout the book, mapping symbols are written on the right.

1.1 Basic definitions

Definition 1.1 (Semigroup)**.** A groupoid $(S, \mu), S \neq \emptyset, \mu$ is a map : $S \times S \to S$ and μ is associative

$$\forall x, y, z \in S, ((x, y)\mu, z)\mu(x, (y, z)\mu)\mu \tag{1}$$

The notation of operator μ could be notated as multiplication.

$$(xy)z = x(yz)$$

When the multiplication of semigroup is clear from the context, we shall write simply S rather that $(S, .)$

Definition 1.2 (Order of Set)**.** The cardinal number of set S, $|S|$.

Definition 1.3 (Commutative (abelian) semigroup)**.** $\forall x, y \in S, xy = yx$

Definition 1.4 (Identity)**.** $1 \in S, \forall x \in S \to 1x = x1 = x$

S has at most one identity element

$$\forall x \in S, x1' = 1'x = x \to 1' = 11' = 1$$

Definition 1.5 (Monoid)**.** $S, 1 \in S$

Symbol 1.1.1 (S^1)**.**

$$S^1 = \begin{cases} S & \text{if } 1 \in S \\ S \cup \{1\} & \text{if } 1 \notin S \end{cases}$$

Definition 1.6 (Zero Element)**.** A semigroup S. $|S| > 1.\forall x \in S, 0x = x0 = 0$

It's easy to add a 0 to semigroup.

Example 1.1.1 (Trivial Semigroups)**.**

Symbol 1.1.2 (S^0)**.**

$$S^0 = \begin{cases} S & \text{if } 0 \in S \\ S \cup \{0\} & \text{if } 0 \notin S \end{cases}$$

Remark 1. The semigroup's extentions of 1 and 0 is not work on group. G is a group, $G \cup \{0\}$ is a semigroup but not a group yet.

Definition 1.7 (Left/Right zero semigroup)**.**

$$\text{Left:} \quad S \neq \emptyset, \forall a, b \in S, ab = a$$

Right is analogue.

Example 1.1.2 (Semigroups)**.**

$$I = [0,1]\,, xy = \min(x,y)$$

$$\{0\}, 0 \text{ is both Identity and Zero}$$

Definition 1.8 (Multiplication of Set)**.**

$$AB = \{ab : a \in A \wedge b \in B\}$$

Notes: $A^2 \neq \{a^2 : a \in A\}$

$$Ab = A\{b\}$$

Example 1.1.3 (Monoid and Multiplication)**.**

$$1 \notin S \to 1 \notin S^1$$

$$1 \notin \begin{cases} S^1 a & = Sa \cup \{a\} \\ aS^1 & = aS \cup \{a\} \\ S^1 a S^1 & = SaS \cup Sa \cup aS \cup \{a\} \end{cases}$$

Definition 1.9 (Group)**.** If a semigroup S has the property that

$$(\forall a \in S) aS = S \wedge Sa = S$$

This definition is equivalent to the common definition of group.

Proof.

$$Sa = S \to \exists s \in S, sa = a \to s \text{ is the left identity element of } a$$
$$\forall x \in S, ax = sax = s(ax) \to s \text{ s is a left identity element of } ax$$
$$ax = S$$
$$\to s \text{ is the left identity element of } S$$
$$\to \text{analogue, } s \text{ is the identity element of } S$$
$$\to E \in S;$$
$$aS = S \to \exists b \in S, ba = E$$
$$\to b = a^{-1}$$
$$\to S \text{ is a group}$$

□

Definition 1.10 (0-Group)**.** G is a group,$G^0 = G \cup \{0\}$ is a semigroup.

Proposition 1.1.1 (There is no $0 - group$ different from $G \cup \{0\}$)**.**

$$\text{A semigroup with zero is a } 0 - group \Leftrightarrow (\forall a \in S \setminus \{0\}) aS = S \wedge Sa = S$$

Proof. Sufficiency

$$\begin{gathered} S = G^0, a \in G = S \setminus \{0\} \to aG = Ga = G \\ aS = aG \cup a\{0\} = aG \cup \{0\} \\ Sa = Ga \cup \{0\}a = Ga \cup \{0\} \\ \to aS = Sa = S \end{gathered}$$

Necessity

$$\begin{gathered} (\forall a \in S \setminus \{0\}) aS = Sa = S \\ \text{Let } G = S \setminus \{0\} \text{Suppose } \exists a, b \neq 0 \in G \to ab = 0 \\ \to S^2 = (Sa)(bS) = S(ab)S = S\{0\}S = \{0\} \\ \to S = aS \subset S^2 = \{0\} \\ \text{It is a contradiction.} \\ \to \forall a, b \in G \to ab \in G \\ \forall a \in G, aG = aS \setminus a\{0\} = aS \setminus \{0\} = S \setminus \{0\} = G \\ \forall a \in G, Ga = Sa \setminus \{0\}a = Sa \setminus \{0\} = S \setminus \{0\} = G \\ \to G \text{ is a group.} \end{gathered}$$

□

Definition 1.11 (Subsemigroup)**.** $T \subset S \wedge T \neq \emptyset \wedge \forall x, y \in T \to xy \in T$ or $T^2 \subset T$

Definition 1.12 (Idempotent)**.** $e \in S, e^2 = e$

Example 1.1.4 (Subgroups)**.** $\{0\}, \{1\}, \{e\}$ are all subgroups.

Remark 2 (No trivial subgroup's condition)**.**

$$T \subset S, (\forall a \in T) aT = T \wedge Ta = T$$

Definition 1.13 (Left/Right Ideal, Ideal)**.**

$$A : A \subset S \wedge A \neq \emptyset \begin{cases} SA \subseteq A : \text{Right Ideal} \\ AS \subseteq A : \text{Left Ideal} \end{cases}$$

Ideal : Both left and right ideal.

Remark 3. Every ideal is a subsemigroup, but the converse is not the case.

Definition 1.14 (Proper)**.** Ideal : $I : \{0\} \subset I \subset S$. Symbol '$\subset$' is strictly.

Definition 1.15 (Morphism.Homomorphism)**.** S, T are semigroups.

$$\text{A map } \phi : S \to T, \forall x, y \in S, (xy)\phi = (x)\phi(y)\phi$$

Remark 4 (Morphism of monoid has better properties)**.**

$$(S, ., 1_S), (T, ., 1_T) \text{ are monoids.} \phi \text{ is a morphism} \rightarrow 1_S\phi = 1_T$$

Proof.

$$\forall x \in S, (x)\phi = (1_S x)\phi = (1_S)\phi(x)\phi$$
$$\rightarrow (1_S)\phi \text{ is the left identity of S}$$
$$\text{The right analogue is same.}$$
$$\rightarrow (1_S)\phi = 1_T$$

□

Definition 1.16 (Monomorphism)**.** S, T are semigroups, A morphism $\phi : S \rightarrow T \wedge \phi$ is one-one.

This definition is equivalent to the 'categorical' definition of a monomorphism as a right cancellative morphism. (The function symbol in this book is right.)

$$\forall \text{semigroups } U, \forall \text{morphisms } \alpha, \beta : U \rightarrow S, \alpha\phi = \beta\phi \Rightarrow \alpha = \beta$$

Definition 1.17 (Isomorphism)**.**

$$\phi . \exists \phi^{-1} : T \rightarrow S. \rightarrow \phi\phi^{-1} = I_S \wedge \phi^{-1}\phi = I_T . S \simeq T$$

Definition 1.18 (Endomorphism, Automorphism)**.**

$$\text{A morphism } \phi : S \rightarrow S\text{: Endomorphism}$$
$$\text{An Endomorphism } \phi \text{ is onto and one-one : Automorphism}$$

Definition 1.19 (Direct(cartesian) product;Projection morphism)**.**

$$\text{Semigroups:} S, T . S \times T \text{ is } (s, t)(s', t') = (ss', tt')$$

General notion of direct product.

$$\text{The product of } \{S_i : i \in I\}$$
$$\text{All maps } p : I \rightarrow \bigcup_{i \in I} S_i . ip \in S_i, P = \{p\}$$
$$\text{Define the multiplication } i(pq) = (ip)(iq)$$
$$\rightarrow P \text{ is a semigroup}$$

Projection morphism $\pi_i : P \rightarrow S, p\pi_i = ip(p \in P)$

Moreover, if T is a semigroup and if there are morphisms $\tau_i : T \rightarrow S_i(i \in I) \rightarrow \exists! \gamma : T \rightarrow P, \forall i \in I, \gamma\pi_i = \tau_i$. The map $\gamma := \forall t \in T, (i)(t\gamma) = t\tau_i, (i \in I)$

P is the product of the semigroups S_i said in categroy.

Proof. The isomorphism of $P \to \prod S_i$

$$\begin{aligned}
&\phi : P \to \prod S_i.p\phi = Ip\\
&\forall p \in P, p\phi = Ip = s \in \prod S_i\\
\Rightarrow &\forall p_1 \neq p_2, p_1\phi = Ip_1 \neq Ip_2 = p_2\phi\\
\Rightarrow &\phi \text{ is one-one}\\
&\forall s \in \prod S_I \to \exists p \in P, Ip = s\\
\Rightarrow &\phi \text{ is onto}\\
\Rightarrow &\phi \text{ is bijective}
\end{aligned}$$

Definition 1.20 (Permutation(Symmetric) group; Full transformation semigroup)**.** Set X.

$$\begin{cases}(\mathcal{G}, \circ) := \text{All permutations of } X & \text{Symmetric group}\\ (\mathcal{T}, \circ) := \text{All maps of } X & \text{Full transformation semigroup}\end{cases}$$

$\mathcal{G}_X$, consisting of all bijections from X onto X, is a subgroup of $\mathcal{T}_X$.
$|\mathcal{G}_X| = n!; |\mathcal{T}_X| = n^n$

Definition 1.21 (Transformation semigroup. Representation of S. Faithful Representation)**.**

$$\begin{cases}S \text{ is a subsemigroup of } \mathcal{T}_X & \text{Transformation semigroup}\\ \text{A morphism } \phi : S \to \mathcal{T}_X & \text{Representation of S (by maps).}\\ \text{A representation of S } \phi \text{ is one-one} & \text{Faithful ...}\end{cases}$$

The first S and second S is different.

Theorem 1.1.1. If S is a semigroup and $X = S^1$ then there is a faithful representation $\phi : S \to \mathcal{T}_X$.

Proof.

$$\begin{gathered}
\forall a \in S, \rho_a : S^1 \to S^1 := x\rho_a = xa.(x \in S^1)\\
\exists \alpha : S \to \mathcal{T}_X := a\alpha = \rho_a(a \in S)\\
a\alpha = b\alpha \to \rho_a = \rho_b \to \forall x \in S^1, xa = xb \to 1a = 1b \to a = b\\
\to \alpha \text{ is one-one}\\
\forall x \in S^1, x(\rho_a\rho_b) = (x\rho_a)\rho_b = (xa)b = x(ab) = x\rho_{ab} \to (a\alpha)(b\alpha) = (ab)\alpha\\
\to \alpha \text{ is a morphism}\\
\to \alpha \text{ is a faithful representation of } S
\end{gathered}$$

□

The representation α introduced in this proof is called extended right regular representation.

Definition 1.22 (Rectangular band)**.** $\forall a, b \in S, aba = a$

Theorem 1.1.2. Let S be a semigroup. Then the four conditions are equivalent.

$$S \text{ is a rectangular band}$$
$$\forall s \in s, s^2 = s; \forall a, b, c \in S \to abc = ac$$
$$\exists \text{ left zero ... } L, \text{right zero ... } R \to S \simeq L \times R$$
$$S \simeq A \times B, A \neq \emptyset, B \neq \emptyset. \text{multiplication: } (a_1, b_1)(a_2, b_2) = (a_1, b_2)$$

Proof. $1 \to 2$

$$\forall x \in S, x = xxx = x^3 \to xx = x^3x = x^4$$
$$x^4 = x(xx)x = x \to x = x^4 = x^2$$
$$\to x \text{ is idempotent.}$$
$$\forall a, b, c \in S, ac = (aba)(cbc) = a(bacb)c = abc$$

$$2 \to 3$$

$$\text{Fix an element } c \in S. L = Sc, R = cS$$
$$\forall x = zc, y = tc, x, y \in L \to xy = zctc = zc^2 = zc = x$$
$$\to L \text{ is a left zero ...}$$
$$\to R \text{ is a right zero ...}$$
$$\phi : S \to L \times R := x\phi = (xc, cx)(x \in S)$$
$$(xc, cx) = (yc, cy) \to x = x^2 = xcx = ycx = ycy = y^2 = y$$
$$\to \phi \text{ is one-one.}$$
$$\forall (ac, cb) \in L \times R, (ac, cb) = (abc, cab) = (ab)\phi$$
$$\to \phi \text{ is onto.}$$
$$\forall x, y \in S$$
$$(xy)\phi = (xyc, cxy) = (xc, yc) = (xcyc, cxcy) = (xc, cx)(yc, cy) = (x\phi)(y\phi)$$
$$\to \phi \text{ is a morphism.}$$
$$\to S \simeq L \times R$$

$$3 \to 4$$

$$S = L \times R. \text{L is left zero ... and R is right zero ...}$$
$$\text{Multiplication: } (a, b)(c, d) = (ac, bd) = (a, d)$$

$$4 \to 1$$

$$\begin{aligned}
&S = A \times B, \text{with multiplication: } (a,b)(c,d) = (a,d) \\
&\forall a = (x,y), b = (p,q) \in S \\
&\to aba = (x,y)(p,q)(x,y) = (x,q)(x,y) = (x,y) = a \\
&\to S \text{ is a rectangular band.}
\end{aligned}$$

$$\begin{tikzcd}
(c,b) \arrow[r, dash] \arrow[d, dash] & (c,d) \arrow[d, dash] \\
(a,b) \arrow[r, dash] & (a,d)
\end{tikzcd}$$

1.2 Monogenic semigroups

Symbol 1.2.1 ($\langle A \rangle$, Generators)**.**

$$A \subset S, U_i \text{ are all subgroups that } A \subset U_i . \langle A \rangle := \bigcap_{i \in I} U_i$$

$\langle A \rangle$ has two properties:

$$\begin{cases} A \subseteq \langle A \rangle \\ \text{Subsemigroup } U, A \subset U \to \langle A \rangle \subseteq U \end{cases}$$

If $\langle A \rangle = S$ we say that A is a set of generators, or a generating set, of S.

Example 1.2.1. Finite A.

$A = \{a\}. \langle A \rangle = \{a, a^2, a^3, ...\}$.

If we need a submonoid of S generated by S, the A always contains 1.

$\langle A \rangle = \{1, a, a^2, ...\}$

Definition 1.23 (Monogenic semigroup)**.** $S = \langle a \rangle$ is said to be a monogenic semigroup.

$\langle a \rangle$ is said to be a monogenic subsemigroup of S generated by the element a.

Order of element $a = |\langle a \rangle|$

The analogue of monogenic in group-theoretic terminology named 'cyclic'. We must judge whether monogenic semigroups are 'round' enough to merit the description 'cyclic'.

Definition 1.24 (Finite/Infinite order)**.** Period, Index.

$a \in S, \langle a \rangle = \{a, a^2, ...\}$.

If $a^m = a^n \to m = n$, that $\langle a \rangle \simeq (N, +)$. We say that $(\langle a \rangle, \cdot)$ is an infinite monogenic semigroup, and a has infinite order in S.

$$\begin{aligned}
\text{Index: } &\min(\{x \in N : a^x = a^y, x \neq y\}) \\
\text{Period: } &\min(\{x \in N : a^{m+x} = a^m\})
\end{aligned}$$

Example 1.2.2. Some properties of finite period geenrator.'

a is an element with index m and period $r \rightarrow a^m = a^{m+r}$. Moreover, $(\forall q \in N)a^m = a^{m+qr}$.

$\langle a\rangle = \{a, a^2, ..., a^m, a^{m+1}, ..., a^{m+r-1}\}.|\langle a\rangle| = m + r - 1.$

Definition 1.25 (Kernel of $\langle a\rangle$)**.** $K_\alpha = \{a^m, ..., a^{m+r-1}\}$

Proposition 1.2.1. K_a is a subsemigroup, indeed a ideal, of $\langle a\rangle$. a^{m+u}.

Proof. $K_a\langle a\rangle = \langle a\rangle K_a = \{a^{m+1}, ..., a^{2m+r-1}\} = K_a$ □

K_a is a subgroup, indeed a cyclic group.

Proof.

$$
\begin{aligned}
& ea^x = a^x \rightarrow e = a^{qr} \\
& \leftarrow \exists q \rightarrow a^q r \in K_a \\
& \rightarrow e \in K_a; \\
& \forall u, v \in N, \exists x \in N \rightarrow a^{m+u}a^{m+x} = a^{m_+v} \\
& \leftarrow x \equiv v - u - m \mod r \text{ and } 0 \leq x \leq r - 1. \\
& \rightarrow \forall a^x \in K_a, \exists a^y \in K_a \rightarrow a^{x+y} = e \\
& \rightarrow K_a \text{ is a group.} \\
& \\
& \leftarrow \exists g, 0 \leq g \leq r - 1 \wedge m + g \equiv 1 \mod r \\
& \rightarrow i = a^{m+g}, K_a = i, i^2, ..., i^{r-1} \\
& \rightarrow K_a \text{ is a cyclic group.}
\end{aligned}
$$

□

Example 1.2.3. Some monogenic semigroups.

$$X = \{1, 2, ..., 7\}, \alpha = \binom{1,2,3,4,5,6,7}{2,3,4,5,6,7,5} \in \mathcal{T}_X$$

$$\alpha^2 = \binom{1,2,3,4,5,6,7}{3,4,5,6,7,5,6}$$

$$\alpha^3 = \binom{1,2,3,4,5,6,7}{4,5,6,7,5,6,7}$$

$$\alpha^4 = \binom{1,2,3,4,5,6,7}{5,6,7,5,6,7,5}$$

$$\alpha^5 = \binom{1,2,3,4,5,6,7}{6,7,5,6,7,5,6}$$

$$\alpha^6 = \binom{1,2,3,4,5,6,7}{7,5,6,7,5,6,7}$$

$$\alpha^7 = \binom{1,2,3,4,5,6,7}{5,6,7,5,6,7,5}$$

α has index 4 and period 3. $K_\alpha = \{\alpha^4, \alpha^5, \alpha^6\}$.

	α^4	α^5	α^6
α^4	α^5	α^6	α^4
α^5	α^6	α^4	α^5
α^6	α^4	α^5	α^6

$6 \equiv 0 \mod 3 \to \alpha^6$ is the identity, $4 \equiv 1 \mod 3 \to \alpha^4$ is the generator. $(\alpha^4)^2 = \alpha^5, (\alpha^4)^3 = \alpha^6$. Visualize $\langle\alpha\rangle$:

$$\begin{tikzcd}
& & & & 6 \arrow[dl] \\
1 \arrow[r] & 2 \arrow[r] & 3 \arrow[r] & 4 \arrow[dr] & \\
& & & & 5 \arrow[uu]
\end{tikzcd}$$

Theorem 1.2.1 ($\langle a\rangle \simeq (N, +)$ or $\{a, a^2, .., a^m, ..., a^{m+r-1}\}$)**.** is all.

1. $\{x : a^x = a^y, x \neq y\} = \emptyset \to \langle a\rangle \simeq (N, +)$;
2. $\exists$ index m, period r with:

$$a^m = a^m + r$$
$$\forall u, v \in N^0, a^{m+u} = a^{m+v} \Leftrightarrow u \equiv v \mod r$$
$$\langle a\rangle = \{a, a^2, ..., a^{m+r-1}\}$$
$$K_a = \{a^m, ..., a^{m+r-1}\} \text{ is a cyclic subgroup of } \langle a\rangle$$

Remark 5 (Finite semigroup)**.** $\langle a\rangle \simeq \langle b\rangle$

It is easy to see $\langle a \rangle \simeq \langle b \rangle \Leftrightarrow$ they have same index and period. We note monogenic semigroup $M(m, r)$ with index m and period r. $M(1, r)$ is the cyclic group of order r.

Periodic semigroup: $\forall a \in S, |\langle a \rangle|$ is finite.

Finite semigroup is always periodic.

Proposition 1.2.2. Every periodic semigroup has a idempotent.

In a periodic semigroup every element has a power which is idempotent. Every periodic semigroup–in particular, in evert finite semigroup, there is at least one idempotent.

Proof. $\forall a \in S \rightarrow |\langle a \rangle| < \infty \rightarrow \exists I \in K_a$ □

Otherwise, the idempotent may not exist.

1.3 Ordered sets, semilattices and lattices

Definition 1.26 (Order, Partial Order)**.** A binary relation ω on set X. If

1.reflexive	$\forall x \in X, (x, x) \in \omega$
2.antisymmetric	$\forall x, y \in X, (x, y) \in \omega \wedge (y, x) \in \omega \rightarrow x = y$
3.transitive	$\forall x, y, z \in X, (x, y) \in \omega \wedge (y, z) \in \omega \rightarrow (x, z) \in \omega$

Traditionally one writes $x \leq y$ rather than $(x, y) \in \omega$.

Definition 1.27 (Total order)**.** Partial order (X, ω) $(\forall x, y \in X) x \leq X \vee y \leq x$

Definition 1.28 (Minimal, Minimum)**.**

$$a \text{ :minimal } (\forall y \in Y) y \leq a \Rightarrow y = a$$
$$b \text{ :minimum } (\forall y \in Y) b \leq y$$

In patrial ordered set it is perfectly possible to have minimal elements that are not minimum.

Proposition 1.3.1 (Let $Y \neq \emptyset, Y \subset X, (X, \leq)$)**.** Then

$$Y \text{ has at most one minimum element.}$$
$$Y \text{ is totally ordered} \rightarrow \text{ 'minimal'='minimum'.}$$

Definition 1.29 (Minimal condition, Well-ordered)**.** $(X, \leq)$

Minimal condition: Every non-empty subset of X has a minimal element.

Well-ordered: A totally ordered set X with minimal condition.

Definition 1.30 (Analogue, Maximal, Maximum, Maximal condition)**.** .

Definition 1.31 (Lower bound, the Greatest lower bound(meet))**.** $Y \subset X, Y \neq \emptyset$

$$\begin{aligned} \text{Lower bounds: } & \{c \in S, \forall y \in Y, c \leq Y\} \\ \text{meet: } & \text{ maximum element of } \{\text{c}\} \end{aligned}$$

Note: meet $d = \bigwedge\{y : y \in Y\}$. If $Y = \{a, b\}, d = a \wedge b$.

Definition 1.32 (Upper bound, the least upper bound(join))**.** analogue

Definition 1.33 (Lower semilattice, Complete lower semilattice)**.**

$$\begin{aligned} \text{lower semilattice: } & \forall a, b \in X, a \wedge b \in X \\ \text{complete lower ...: } & \text{lower ...}, \forall Y \subset X, \exists \bigwedge\{y : y \in Y\} \end{aligned}$$

Definition 1.34 (Upper semilattice, Complete upper semilattice)**.** analogue

Definition 1.35 (lattice, complete lattice, sublattice)**.**

$$\begin{aligned} \text{lattice : } & X \text{ both upper and lower semilattice.} \\ \text{complete ... : } & X \text{both complete upper and complete lower semilattice.} \\ \text{sublattice : } & Y \subset X, Y \neq \emptyset . \forall a, b \in Y, a \wedge b, a \vee b \in Y \end{aligned}$$

Note: lattice: $X = (X, \leq, \wedge, \vee)$

Proposition 1.3.2 (The multiplication and $\wedge$ of lattice)**.** .
Let $(E, \leq)$ be a lower semilattice. Then $(E, \wedge)$ is a commutative semigroup consisting entirely of idempotents, and

$$(\forall a, b \in E) a \leq b \Leftrightarrow a \wedge b = a$$

Conversely, suppose that $(E, .)$ is a commutative semigroup of idempotents. Then the relation $\leq$ on E defined by

$$a \leq b \Leftrightarrow ab = a$$

is a partial order on E, with respect to which $(E, \leq)$ is a lower semilattice.

Proof. 1.

$$\begin{aligned} & \forall a, b \in E, a \wedge b \in E \\ & \forall a, b, c \in E, a \wedge (b \wedge c) = (a \wedge b) \wedge c \\ & \rightarrow E \text{ is a semigroup.} \\ & \forall a, b \in E, a \wedge b = b \wedge a \\ & \rightarrow E \text{ is commutative.} \\ & \forall a \in E, a \wedge a = a \\ & \rightarrow a \text{ is a idempotent.} \end{aligned}$$

2.

By the definition. $a^2 = a \to a \leq a$
$a \leq b \wedge b \leq a \to ab = a \wedge ba = b \to a = ab = ba = b$
$a \leq b \wedge b \leq c \to ab = a \wedge bc = b \to ac = (ab)c = a(bc) = ab = a$
$\to a \leq c$
$\to \leq$ is a partial order.

$\forall a, b \in E, ab \leq a \wedge ab \leq b \to ab$ is a lower bound.
$\forall c \leq a, c \leq b, c(ab) = (ca)b = cb = c \to c \leq ab$
$\to ab = a \wedge b$
$\to E$ is a lower lattice.

$\square$

This proposition is that the notions of 'lower semilattice' and 'commutative semigroup of idempotents' are equivalent.

Symbol 1.3.1 (Hasse diagrams)**.** !!! Wait for learning TikZ.
The bigger element is always upper to lower one.
If $a \leq b, \forall x \in E, a < x < b$ is impossible, paint a line bettwen a and b

1.4 Binary relations; equivalences

Definition 1.36 (Equality(diagnoal) relation)**.** $1_X = \{(x, x) : x \in X\}$

Definition 1.37 ($\circ$ on $\mathcal{B}_X$)**.**

$$\forall \rho, \sigma \in \mathcal{B}_X, \rho \circ \sigma = \{(x, y) \in X \times X : (\exists z \in X)(x, z) \in \rho \wedge (z, y) \in \sigma\}$$

Proposition 1.4.1 (($\mathcal{B}_X, \circ$) is a semigroup)**.** $\forall \rho, \sigma, \tau \in \mathcal{B}_X$.

$$\begin{aligned}
&(x, y) \in (\rho \circ \sigma) \circ \tau \\
&\quad \Leftrightarrow (\exists \in X)(x, z) \in \rho \wedge (z, y) \in \tau \\
&\quad \Leftrightarrow (\exists z \in X)(\exists u \in X)(x, u) \in \rho, (u, z) \in \sigma \wedge (z, y) \in \tau \\
&\quad \Leftrightarrow (\exists u \in X)(x, u) \in \rho \wedge (u, y) \in \sigma \circ \tau \\
&\quad \Leftrightarrow (x, y) \in \rho \circ (\sigma \circ \tau) \\
&\quad \to (\rho \circ \sigma) \circ \tau = \rho \circ (\sigma \circ \tau)
\end{aligned}$$

Remark 6 (The $\circ$ operator keeps order of relations)**.** $\forall \rho, \sigma, \tau \in \mathcal{B}_X$

$$\rho \subseteq \sigma \to \rho \circ \tau \subseteq \sigma \circ \tau \wedge \tau \circ \rho \subseteq \tau \circ \sigma$$

Definition 1.38 (Domain, Image, Converse)**.** in $\mathcal{B}_X$

$$\begin{aligned} \text{Domain: } & \text{dom}\rho = \{x \in X : (\exists y \in X)(x,y) \in \rho\} \\ \text{Image: } & \text{im}\rho = \{y \in X : (\exists x \in X)(x,y) \in \rho\} \\ \text{Converse: } & \rho^{-1} = \{(x,y) \in X \times X : (y,x) \in \rho\} \end{aligned}$$

By this definition, we immediate that, $\forall \rho, \sigma \in \mathcal{B}_X$:

$$\begin{aligned} \rho \subseteq \sigma \to \text{dom}\rho \subseteq \text{dom}\sigma \wedge \text{im}\rho \subseteq \text{im}\sigma \\ \text{dom}\rho^{-1} = \text{im}\rho, \text{im}\rho^{-1} = \text{dom}\rho \end{aligned}$$

Definition 1.39 ($x \in X, x\rho, A \subseteq X, A\rho$)**.** .

$$\begin{aligned} x\rho = \{y \in X : (x,y) \in \rho\} \\ A\rho = \bigcup \{a\rho : a \in A\} \end{aligned}$$

Definition 1.40 (Partial map, Restriction, Extension)**.**

$$\begin{aligned} \text{Partial map: } & \phi \in \mathcal{B}_X, \forall x \in \text{dom}\phi, |x\phi| = 1 \\ & \phi, \varphi \text{ are partial maps}, \phi \subseteq \psi \\ \text{Restriction: } & \phi \text{ is a restriction of } \psi, \phi = \psi|_{\text{dom}\phi} \\ \text{Extension: } & \psi \text{ is a extension of } \phi \end{aligned}$$

Empty relation is also a partial map.

Proposition 1.4.2 ($\mathcal{P}_X \subset \mathcal{B}_X$)**.** is a subsemigroup.

Proof. Let $\phi, \psi \in \mathcal{P}_X, (x, y_1), (x, y_2) \in \phi \circ \psi$.

$$\begin{aligned} \exists z_1, z_2 \in X \to & (x, z_1) \in \phi, (z_1, y_1) \in \psi, (x, z_2) \in \phi, (z_2, y_2) \in \psi \\ \to & z_1 = z_2 \to y_1 = y_2 \\ \to & \phi \circ \psi \in \mathcal{P}_X \end{aligned}$$

□

Proposition 1.4.3. $\phi, \psi \in \mathcal{P}_X$

$$\begin{aligned} \text{dom}(\phi \circ \psi) = [\text{im}\phi \cap \text{dom}\psi]\phi^{-1} \\ \text{im}(\phi \circ \psi) = [\text{im}\phi \cap \text{dom}\psi]\psi \\ (\forall x \in \text{dom}(\phi \circ \psi)) x(\phi \circ \psi) = (x\phi)\psi \end{aligned}$$

Proof. 1.

$$
\begin{aligned}
&\forall x \in \text{dom}(\phi \circ \psi) \to \exists y, z \in X, (x,z) \in \phi, (z,y) \in \psi \\
&\to z \in \text{im}\phi \cap \text{dom}\psi \\
&(z,x) \in \phi^{-1} \\
&\to x \in z\phi^{-1} \subseteq [\text{im}\phi \cap \text{dom}\psi]\phi^{-1} \\
&\text{Conversely} \\
&\forall x \in [\text{im}\phi \cap \text{dom}\psi]\phi^{-1} \\
&\to \exists z \in \text{im}\phi \cap \text{dom}\psi \to x \in z\phi^{-1} \to (x,z) \in \phi \\
&z \in \text{dom}\psi \\
&\to \exists y \in X, (z,y) \in \psi \\
&\to (x,y) \in \phi \circ \psi \\
&\Rightarrow \text{dom}(\phi \circ \psi) = [\text{im}\phi \cap \text{dom}\psi]\phi^{-1}
\end{aligned}
$$

2.

$$
\begin{aligned}
&\forall x \in \text{im}(\phi \circ \psi) \to \exists (y,x) \in \psi, \exists (z,y) \in \phi \\
&\to y \in \text{dom}\psi \cap \text{im}\phi \\
&(y,x) \in \psi \\
&\to x \in y\psi \subseteq [\text{im}\phi \cap \text{dom}\psi]\psi \\
&\text{Conversely} \\
&\forall x \in \text{im}(\phi \circ \psi) \\
&\to \exists y \in \text{im}\phi \cap \text{dom}\psi \to x \in y\psi \to (y,x) \in \psi \\
&y \in \text{im}\phi \\
&\to \exists z \in X, (z,y) \in \phi \\
&\to (z,x) \in \phi \circ \psi \\
&\Rightarrow \text{im}(\phi \circ \psi) = [\text{im}\phi \cap \text{dom}\psi]\psi
\end{aligned}
$$

The above proofs have used no special properties of partial maps.

3.

$$
\begin{aligned}
&(x,y) \in \phi \circ \psi \Leftrightarrow \exists z(x,z) \in \phi \wedge (z,y) \in \psi \\
&\to z = x\phi, y = z\psi, y = x(\phi \circ \psi) \\
&\to x(\phi \circ \psi) = y = z\psi = (x\phi)\psi
\end{aligned}
$$

□

Definition 1.41 (Map, Function)**.** Partial map $\phi \wedge \text{dom}\phi = X$.

Proposition 1.4.4. $(\mathcal{T}_X = \{\phi : X \to X\}, \circ)$ is a subsemigroup of $(\mathcal{B}_X, \circ)$

Proposition 1.4.5. $X \neq \emptyset$

1. $\phi \in \mathcal{P}_X \to \phi^{-1} \in \mathcal{P}_X \Leftrightarrow \phi$ is one-one.
2. $\phi \in \mathcal{T}_X \to \phi^{-1} \in \mathcal{T}_X \Leftrightarrow \phi$ is bijective.

Remark 7 (Order relation)**.** ρ

$$\begin{aligned} \text{reflexive } & 1_X \subseteq \rho \\ \text{anti-symmetric } & \rho \cap \rho^{-1} = 1_X \\ \text{transitive } & \rho \circ \rho \subseteq \rho \end{aligned}$$

Remark 8 (Equivalence relation)**.** ρ

$$\begin{aligned} \text{reflexive } & 1_X \subseteq \rho \\ \text{symmetric } & \rho^{-1} = \rho \\ \text{transitive } & \rho \circ \rho = \rho \end{aligned}$$

Symmetric $\rho \subseteq \rho^{-1} \to \rho^{-1} \subseteq \rho \to \rho^{-1} = \rho$. Transitive $\rho = 1_X \circ \rho \subseteq \rho \circ \rho \to \rho \circ \rho = \rho$.

Remark 9.

$$\begin{aligned} & \rho \text{ is an equivalence on } X \\ & \Rightarrow X = \text{dom}1_X \subseteq \text{dom}\rho; X = \text{im}1_X \subseteq \text{im}\rho \\ & \Rightarrow \text{dom}\rho = \text{im}\rho = X \end{aligned}$$

Definition 1.42 (Partition)**.** of X A family $\pi = \{A_i \in X : i \in I\}$, if

$$\begin{aligned} & \forall i \in I, A_i \neq \emptyset \\ & \forall i, j \in I, A_i = A_j \vee A_i \cap A_j = \emptyset \\ & \bigcup \{A_i : i \in I\} = X \end{aligned}$$

Proposition 1.4.6. Partition and equivalence are closely related.

Let ρ be an equivalence on a set X. Then the family

$$\Phi(\rho) = x\rho : x \in X$$

of subset of X is a partition of X.

$$\forall \text{ equivalence } \rho \text{ on } X, \Psi(\Phi(\rho)) = \rho, \forall \text{ partition } \pi \text{ of } X, \Phi(\Psi(\pi)) = \pi$$

Definition 1.43 (ρ-classes,quotient set, natural map)**.** .

If ρ is an equivalence on X, we write $x\rho y$ or $x \equiv y \mod \rho$.

ρ-classes, (equivalence-classes):

The sets $x\rho$ that from the partition associated with the equivalence.

quotient set :

The set of ρ-classes, whose elements are the subsets $x\rho$.

Symbol 1.4.1 ($X/\rho, \rho^\natural$)**.**

$$X/\rho : \text{Quotient set of X}$$
$$\rho^\natural : \text{onto map:} X \to X/\rho$$

Proposition 1.4.7 (A relation ϕ, $\to \phi \circ \phi^{-1}$ is an equivalence)**.** .

Proof.

$\phi \circ \phi^{-1}$
$= \{(x, y) \in X \times X : (\exists z \in X)(x, z) \in \phi, (y, z) \in \phi\}$
$= \{(x, y) \in X \times X : x\phi = y\phi\}$
The reflexive, symmetric and transitive is clear.

□

Definition 1.44 (kernel of a relations)**.** .

$$\ker \phi = \phi \circ \phi^{-1}$$

Notice that $\ker \rho^\natural = \rho$

Remark 10.

$\rho_i : i \in I$ is a non-empty family of equivalences on a set X
$\to \bigcap\{\rho_i : i \in I\}$ is again an equivalence.

Definition 1.45 ($\mathbf{R^e}$)**.** .
$\mathbf{R}$ is any relation on X, The family of equivalences containing $\mathbf{R}$ is non-empty. Hence the intersection of all the equivalences containing $\mathbf{R}$ is an equivalence. We call it the equivalence generated by $\mathbf{R}$, denoted it by $\mathbf{R^e}$.

Definition 1.46 (transitive closure)**.** .
Let $\mathbf{S}$ be a relation on $X, 1_X \subseteq \mathbf{S}$, then

$$\mathbf{S} \subseteq \mathbf{S} \circ \mathbf{S} \subseteq \mathbf{S} \circ \mathbf{S} \circ \mathbf{S} \cdots$$

The relation $\mathbf{S}^\infty = \bigcup\{\mathbf{S}^n : n \in \mathbf{Z}^+\}$ is called the Transitive closure of the relation $\mathbf{S}$.

Lemma 1.4.1. Every reflexive relation $\mathbf{S}$, the relation $\mathbf{S}^\infty$ is the smallest transitive relation on X containing $\mathbf{S}$.

Proof.

$\forall (x, y), (y, z) \in \mathbf{S}^\infty \to \exists m, n (x, y) \in \mathbf{S}^m \wedge (y, z) \in \mathbf{S}^n$
$\to (x, z) \in \mathbf{S}^{m+n} \subseteq \mathbf{S}^\infty$
$\forall \mathbf{T}$ is transitive relation containing $\mathbf{S}$.
$\to \mathbf{S}^2 = \mathbf{S} \circ \mathbf{S} \subseteq \mathbf{T} \circ \mathbf{T} \subseteq T$
$\to \forall n \in \mathbb{Z}^+, \mathbf{S}^n \subseteq T$
$\to \mathbf{S}^\infty \subseteq T$

$\square$

Proposition 1.4.8. $\mathbf{R^e} = [\mathbf{R} \cup \mathbf{R}^{-1} \cup 1_X]^\infty$

Proof.

$$\begin{aligned}
&\mathbf{E} = \mathbf{R} \cup \mathbf{R}^{-1} \cup 1_X]^\infty \text{ is transitive and contains } \mathbf{R}\\
&\to 1_X \subseteq \mathbf{R} \cup \mathbf{R^{-1}} \cup 1_X \subseteq \mathbf{E}\\
&\to \mathbf{E} \text{ is also reflaxive.}\\
&\mathbf{S} = \mathbf{R} \cup \mathbf{R}^{-1} \cup 1_X \text{ is symmetric.}\\
&\to \mathbf{S}^n = (\mathbf{S^{-1}})^n = (\mathbf{S^n})^{-1}\\
&\to \mathbf{S}^n \text{ is symmetric}\\
&\to \mathbf{S}^\infty \text{ is symmetric}\\
&\to \mathbf{E} \text{ is an equivalence relation containing } \mathbf{R}
\end{aligned}$$

Suppose that σ is an equivalence relation containing $\mathbf{R} \to 1_X \subseteq \sigma, \mathbf{R}^{-1} \subseteq \sigma^{-1} = \sigma$

$$\begin{aligned}
&\to \mathbf{S} = \mathbf{R} \cup \mathbf{R}^{-1} \cup 1_X \subseteq \sigma\\
&\to \mathbf{S} \circ \mathbf{S} \subseteq \sigma \circ \sigma = \sigma\\
&\to \forall n \in \mathbb{Z}^+, \mathbf{S}^n \subseteq \sigma\\
&\to \mathbf{S}^\infty \subseteq \sigma
\end{aligned}$$

Now, $\mathbf{E}$ is the smallest equivalence on X containing $\mathbf{R}$.

$$\to \mathbf{R^e} = [R \cup R^{-1} \cup 1_X]^\infty$$

$\square$

Proposition 1.4.9.

$$\begin{aligned}
(x, y) \in \mathbf{R^e} \Leftrightarrow &\text{ either } x = y\\
\text{or } x = z_1 \to &z_2 \to \cdots \to z_n \to y
\end{aligned}$$

in witch,$\forall i \in \{1, 2, \cdot, n-1\}$, either $(z_i, z_{i+1}) \in \mathbf{R}$ or $(z_{i+1}, z_i) \in \mathbf{R}$

1.5 Congruences

1.6 Free semigroups and monoids; presentations

1.7 Ideals and Rees congruences

1.8 Lattices of equivalences and congruences

1.9 Exercises

1. An element e is a semigroup S is called a *left identity* if $\forall x \in S \to ex = x$. Analogue is for *right identity.* An element z of S is called a *left zero* if $\forall x \in S, zx = z$. Analogue is for *right zero.*

Proof: If S has a left identity e and a right identity f, then $e = f$ and e is the unique two-sided identity for S.

Proof.

$$
\begin{gathered}
e = ef = f \Rightarrow e = f \\
\forall e' \neq e, e' = e'e = e \Rightarrow e' = e
\end{gathered}
$$

That semigroup has both left identity(ies) and right identity(ies) has only one identity.

Proof: If S has a left zero z and a right zero u, then $z = u$, and z is the unique two-sided zero for S.

Proof.

$$
\begin{gathered}
z = zu = u \Rightarrow z = u \\
\forall z' \neq z, z' = z'z = z \Rightarrow z' = z
\end{gathered}
$$

Proof: Give an example of a semigroup having two (at least) left identities and two (at least) right zeros.

$$
\{e_1, e_2\}
$$

$$
\text{Multiplication: } \begin{cases} e_1e_2 = e_2 \\ e_2e_1 = e_1 \\ e_1e_1 = e_1 \\ e_2e_2 = e_2 \end{cases}
$$

$$
\text{Association: } \begin{cases} e_1^3 = e_1 \\ e_2^3 = e_2 \\ (e_1e_1)e_2 = e_1e_2 = e_2 \quad e_1(e_1e_2) = e_1e_2 = e_2 \\ (e_1e_2)e_1 = e_2e_1 = e_1 \quad e_1(e_2e_1) = e_1e_1 = e_1 \\ (e_2e_1)e_1 = e_1e_1 = e_1 \quad e_2(e_1e_1) = e_2e_1 = e_1 \\ (e_2e_2)e_1 = e_2e_1 = e_1 \quad e_2(e_2e_1) = e_2e_1 = e_1 \\ (e_2e_1)e_2 = e_1e_2 = e_2 \quad e_2(e_1e_2) = e_2e_2 = e_2 \\ (e_1e_2)e_2 = e_2e_2 = e_2 \quad e_1(e_2e_2) = e_1e_2 = e_2 \end{cases}
$$

so e_1, e_2 are the left identities and the right zeros.

1.10 Notes