SEMIGROUP THEORY

VICKY G

1. The Basic Concept

Definition: A *semigroup* is a pair $(S, *)$ where S is a non-empty set and $*$ is an associative binary operation on S. [i.e. $*$ is a function $S \times S \to S$ with $(a, b) \mapsto a*b$ and for all $a, b, c \in S$ we have $a * (b * c) = (a * b) * c$].

We abbreviate "$(S, *)$" by "S" and often omit $*$ in "$a * b$" and write "ab". By induction $a_1 a_2 \dots a_n$ is unambiguous. Thus we write a^n for

$$\underbrace{aa \dots a}_{n \text{ times}}.$$

Index Laws: We have that for all $n, m \in \mathbb{N} = \{1, 2, \dots\}$ the following index laws hold

$$a^n a^m = a^{n+m}$$
$$\left(a^n\right)^m = a^{nm}.$$

Definition: A *monoid* M is a semigroup with an identity, i.e. there exists $1 \in M$ such that $1a = a = a1$ for all $a \in M$.

Putting $a^0 = 1$ then the index laws hold for all $n, m \in \mathbb{N}^0$.

Note. The identity of a monoid is unique.

Definition: A *group* G is a monoid such that for all $a \in G$ there exists a $b \in G$ with $ab = 1 = ba$.

Example 1.1. Groups are monoids and monoids are semigroups. Thus we have

$$\text{Groups} \subset \text{Monoids} \subset \text{Semigroups}.$$

The one element trivial group $\{e\}$ with multiplication table

	e
e	e

is also called the *trivial semigroup* or *trivial monoid*.

Example 1.2. A ring is a semigroup under $\times$. A ring with identity is a monoid.

EXAMPLE 1.3. $\mathbb{N}$ is a monoid under $\times$. $\mathbb{N}$ forms a semigroup under $+$ and $\mathbb{N}^0$ is a monoid under $+$ and $\times$.

EXAMPLE 1.4. Let I, J be non-empty sets and set $T = I \times J$ with the binary operation

$$(i,j)(k,\ell) = (i,\ell).$$

Then T is a semigroup called the *rectangular band* on $I \times J$. To verify that T is a semigroup we need to check that the associativity law holds. So

$$\big((i,j)(k,\ell)\big)(m,n) = (i,\ell)(m,n) = (i,n),$$
$$(i,j)\big((k,\ell)(m,n)\big) = (i,j)(k,n) = (i,n),$$

for all $(i,j),(k,\ell),(m,n) \in T$ and hence multiplication is associative.

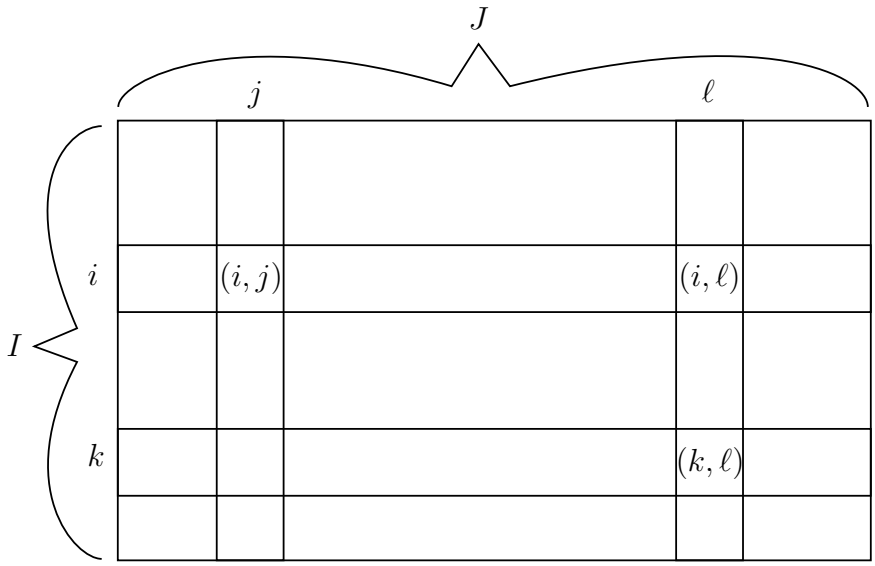


FIGURE 1. The rectangular band.

Notice: $(i,j)^2 = (i,j)(i,j) = (i,j)$, i.e. every element is an idempotent. This can't be looked at from ring theory because any ring where every element is an idempotent means that the ring is commutative. However, the rectangular band does *not* have to be commutative.

1.1. **Adjoining an Element**

Let S be a semigroup, which is *not* a monoid. Find a symbol not in S, call it "1". We now extend the definition of $*$ on S to $S \cup \{1\}$ by

$$\begin{aligned} a * b &= ab && \text{if } a, b \in S, \\ a * 1 = a = 1 * a & && \text{for all } a \in S, \\ 1 * 1 &= 1. \end{aligned}$$

Then $*$ is associative (check this). Thus we have managed to extend multiplication in S to $S \cup \{1\}$. For an arbitrary semigroup S the monoid S^1 is defined by

$$S^1 = \begin{cases} S & \text{if } S \text{ is a monoid,} \\ S \cup \{1\} & \text{if } S \text{ is not a monoid.} \end{cases}$$

So, S^1 is "S with a 1 adjoined if necessary".

EXAMPLE 1.5. Let T be the rectangular band on $\{a\} \times \{b, c\}$. Then $T^1 = \{1, (a, b), (a, c)\}$, which has multiplication table

	1	(a,b)	(a,c)
1	1	(a,b)	(a,c)
(a,b)	(a,b)	(a,b)	(a,c)
(a,c)	(a,c)	(a,b)	(a,c)

EXAMPLE 1.6 (The Bicyclic Semigroup / Monoid). If $A \subseteq \mathbb{Z}$, such that $|A| < \infty$, then $\max A$ is the biggest element in A. We also use this notation to represent

$$\max\{a, b\} = \begin{cases} a & \text{if } a \geqslant b, \\ b & \text{if } b \geqslant a. \end{cases}$$

We note some further things about max:

- $\max\{a, 0\} = a$ if $a \in \mathbb{N}^0$,
- $\max\{a, b\} = \max\{b, a\}$,
- $\max\{a, a\} = a$,
- $\max\big\{a, \max\{b, c\}\big\} = \max\{a, b, c\} = \max\big\{\max\{a, b\}, c\big\}$.

Thus we have that $(\mathbb{Z}, \max)$ is a semigroup and $(\mathbb{N}^0, \max)$ is a monoid.

Note. The following identities hold for all $a, b, c \in \mathbb{Z}$

$$(\star) \begin{cases} a + \max\{b, c\} = \max\{a + b, a + c\}, \\ \max\{b, c\} = a + \max\{b - a, c - a\}. \end{cases}$$

Put $B = \mathbb{N}^0 \times \mathbb{N}^0$. Now, on B we define a binary operation by

$$(a, b)(c, d) = (a - b + t, d - c + t),$$

where $t = \max\{b, c\}$. We claim that B together with this operation forms a semigroup/monoid called the *Bicyclic Semigroup/Monoid*.

Proof. With $(a,b),(c,d) \in B$ and $t = \max\{b,c\}$ we have $t - b \geqslant 0$ and $t - c \geqslant 0$. Thus we have $a - b + t \geqslant a$ and $d - c + t \geqslant d$. Therefore, in particular $(a - b + t, d - c + t) \in B$ so multiplication is closed. We have that $(0,0) \in B$ and for any $(a,b) \in B$ we have

$$\begin{aligned}(0,0)(a,b) &= (0 - 0 + \max\{0,a\}, b - a + \max\{0,a\}),\\ &= (0 - 0 + a, b - a + a),\\ &= (a,b),\\ &= (a,b)(0,0).\end{aligned}$$

Therefore $(0,0)$ is the identity of B. We need to check associativity of max. Let (a,b), (c,d), $(e,f) \in B$. Then

$$\begin{aligned}\big((a,b)(c,d)\big)(e,f) &= \big(a - b + \max\{b,c\}, d - c + \max\{b,c\}\big)(e,f),\\ &= \big(a - b - d + c + \max\{d - c + \max\{b,c\}, e\}\\ &\qquad f - e + \max\{d - c + \max\{b,c\}, e\}\big).\\ (a,b)\big((c,d)(e,f)\big) &= (a,b)\big(c - d + \max\{d,e\}, f - e + \max\{d,e\}\big),\\ &= (a - b + \max\{b, c - d + \max\{d,e\}\}\\ &\qquad f - e - c + d + \max\{b, c - d + \max\{d,e\}\}\big).\end{aligned}$$

Now we have to show that

$$\begin{aligned}\cancel{a - b} - d + c + \max\big\{d - c + \max\{b,c\}, e\big\} &= \cancel{a - b} + \max\big\{b, c - d + \max\{d,e\}\big\},\\ \cancel{f - e} + \max\big\{d - c + \max\{b,c\}, e\big\} &= \cancel{f - e} - c + d + \max\big\{b, c - d + \max\{d,e\}\big\}.\end{aligned}$$

We can see that these equations are the same and so we only need to show

$$c - d + \max\big\{d - c + \max\{b,c\}, e\big\} = \max\big\{b, c - d + \max\{d,e\}\big\}.$$

Now, we have from $(\star)$ that

$$\max\big\{\max\{b,c\}, c - d + e\big\} = \max\big\{b, c - d + \max\{d,e\}\big\}.$$

The RHS of this equation is

$$\begin{aligned}\max\big\{b, c - d + \max\{d,e\}\big\} &= \max\big\{b, \max\{c - d + d, c - d + e\}\big\},\\ &= \max\big\{b, \max\{c, c - d + e\}\big\},\\ &= \max\{b, c, c - d + e\},\\ &= \max\big\{\max\{b,c\}, c - d + e\big\}.\end{aligned}$$

Therefore multiplication is associative and hence B is a semigroup/monoid. □

EXAMPLE 1.7. $\mathcal{T}_X$ is a semigroup. See the examples class for proof.

1.2. **Easy Facts / Definitions**

A semigroup S is *commutative* if $ab = ba$ for all $a, b \in S$. For example $\mathbb{N}$ with $+$ is commutative. B is not because

$$(0,1)(1,0) = (0-1+1, 0-1+1) = (0,0),$$
$$(1,0)(0,1) = (1-0+0, 1-0+0) = (1,1).$$

Thus we have $(0,1)(1,0) \neq (1,0)(0,1)$. Notice that in B; $(a,b)(b,c) = (a,c)$. It is important to see that in general we have NO cancellation in Semigroups. Thus we have that

$$ac = bc \not\Rightarrow a = b,$$
$$ca = cb \not\Rightarrow a = b.$$

For example in the rectangular band on $\{1,2\} \times \{1,2\}$ we have

$$(1,1)(1,2) = (1,2) = (1,2)(1,2)$$

but $(1,1) \neq (1,2)$. A semigroup is *cancellative* if

$$ac = bc \Rightarrow a = b,$$
$$ca = cb \Rightarrow a = b,$$

are true for all $a, b, c \in S$. For example, a group is cancellative (indeed, any subsemigroup of a group is cancellative). $\mathbb{N}^0$ is a cancellative monoid, which is not a group.

1.3. **Zeros**

A zero "0" of a semigroup S is an element such that, for all $a \in S$,

$$0a = a = a0.$$

Adjoining a Zero

Let S be a semigroup, then pick a new symbol "0". Let $S^0 = S \cup \{0\}$; define a binary operation $\cdot$ on S^0 by

$$a \cdot b = ab \qquad \text{for all } a \in S,$$
$$0 \cdot a = 0 = a \cdot 0 \qquad \text{for all } a \in S,$$
$$0 \cdot 0 = 0.$$

Then $\cdot$ is associative, so S^0 is a semigroup with zero. We say that "S is a semigroup with a zero adjoined".

2. Reminder of Familiar Ideas

Example 2.1 (Function). Let $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$ then we define a function $f : A \to B$ by $f(1) = a$, $f(2) = a$, $f(3) = c$. We can also describe this using two row notation

$$f = \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}.$$

We write xf rather than $f(x)$. Here $1f = a = 2f$, $3f = c$.

Binary Operations

Let A be a set. A binary operation $*$ on A is a function from $A \times A \to A$. We write $a * b$ for $(a, b)*$.

Composition of Functions

Let $f : A \to B$ and $g : B \to C$ then we define the composition of these functions, $f \circ g : A \to C$, to be

$$a(f \circ g) = (af)g.$$

Now given another function $h : C \to D$ then the composition of these functions is associative. For any $a \in A$ we have

$$\begin{aligned} a\big((f \circ g) \circ h\big) &= \big(a(f \circ g)\big)h, \\ &= \big((af)g\big)h, \\ &= (af)(g \circ h), \\ &= a\big(f \circ (g \circ h)\big). \end{aligned}$$

Identity Function

For any set X we define the identity function $I_X : X \to X$ such that for all $x \in X$

$$xI_X = x.$$

Also, if $f : X \to Y$ a function then

$$I_X \circ f = f = f \circ I_Y.$$

Let X be a set such that $X \neq \emptyset$. Recall that $\mathcal{S}_X = \{\alpha : X \to X \mid \alpha \text{ is a bijection}\}$ is a group under $\circ$, called the *symmetric group* on X. Usually write $\mathcal{S}_n$ for $\mathcal{S}_{\underline{n}}$ where $\underline{n} = \{1, 2, \ldots, n\}$.

Theorem 2.1 (Cayley)**.** *If G is a group then there exists a 1:1 homomorphism $\theta : G \to \mathcal{S}_G$.*

Definition: $\mathcal{T}_X = \{\alpha \mid \alpha \text{ is a function } X \to X\}$.

We write $\mathcal{T}_n$ for $\mathcal{T}_{\underline{n}}$. This has size n^n because that's how many ways there are of choosing a function on n elements. $\mathcal{T}_X$ is a monoid with identity I_X called the *full transformation* monoid / semigroup on X.

Claim. Clearly $\mathcal{S}_X \subseteq \mathcal{T}_X$ and if $|X| \geqslant 2$ then $\mathcal{S}_X \neq \mathcal{T}_X$.

Proof. For any $n \in X$ let $c_n \in \mathcal{T}_X$ be the *constant map* on n, i.e. $yc_x = x$ for all $y \in X$. Note that $\operatorname{Im} c_n = \{n\}$ and if $|X| \geqslant 2$ then c_n is neither one-to-one nor onto, so $c_x \in \mathcal{S}_X \setminus \mathcal{T}_X$. Now notice $\alpha c_x = c_x$ for all $\alpha \in \mathcal{T}_X$.

We show this by letting $y \in X$, then

$$y(\alpha c_x) = (y\alpha)c_x = x = yc_x.$$

Hence $\alpha c_x = c_x$. Thus c_x is a *right zero* for $\mathcal{T}_X$. Furthermore $\alpha c_x = \beta c_x$ for all $\alpha, \beta \in \mathcal{T}_X$ so $\mathcal{T}_X$ is not cancellative for $|X| \geqslant 2$. □

If $\alpha \in \mathcal{S}_n$ then α can be written in "two row" notation or as a product of disjoint cycles. For example

$$\begin{aligned}\alpha &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in \mathcal{S}_5 \\ &= (123)(45).\end{aligned}$$

We can also express this pictorially as the cycle diagram of α. For $\mathcal{T}_X$ we can use "two row" notation. For example if $\alpha \in \mathcal{T}_5$ is given by $1\alpha = 2, 2\alpha = 2, 3\alpha = 3, 4\alpha = 1, 5\alpha = 1$. Then,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 3 & 1 & 1 \end{pmatrix}.$$

For example,

$$c_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 2 & 2 & 2 \end{pmatrix} \in \mathcal{T}_5.$$

We have map diagrams for $\mathcal{T}$.

3. Subsemigroups / Submonoids

Definition: Let S be a semigroup and $\emptyset \neq T \subset S$. Then T is a *subsemigroup* of S if $a, b \in T \Rightarrow ab \in T$. If S is a monoid then T is a *submonoid* of S if T is a subsemigroup and $1 \in T$.

Example 3.1. $(\mathbb{N}, +)$ is a subsemigroup of $(\mathbb{Z}, +)$.

EXAMPLE 3.2. $R = \{c_x \mid x \in X\}$ is a subsemigroup of $\mathcal{T}_X$ called the *right zero semigroup.*

Proof. $c_x c_y = c_y$ for all $x, y \in X$. □

EXAMPLE 3.3 (Bicyclic Monoid). Put $E(B) = \{(a, a) \mid a \in \mathbb{N}^0\}$, the set of all idempotents in B. We claim that $E(B)$ is a commutative submonoid of B. Clearly we have $(0, 0) \in E(B)$ and for $(a, a), (b, b) \in E(B)$ we have

$$\begin{aligned}(a,a)(b,b) &= (a-a+t, b-b+t) && \text{where } t = \max\{a,b\},\\ &= (t,t),\\ &= (b,b)(a,a).\end{aligned}$$

3.1. **Morphisms**

Definition: Let S, T be semigroups then $\theta : S \to T$ is a semigroup (homo)*morphism* if, for all $a, b \in S$,

$$(ab)\theta = a\theta b\theta.$$

If S, T are monoids then θ is a monoid (homo)*morphism* if θ is a semigroup morphism and $1_S\theta = 1_T$.

EXAMPLE 3.4. $\theta : B \to \mathbb{Z}$ given by $(a, b)\theta = a - b$ is a monoid morphism because

$$\begin{aligned}\big((a,b)(c,d)\big)\theta &= (a-b+t, d-c+t)\theta && t = \max\{b,c\},\\ &= (a-b)-(d-c),\\ &= (a-b)+(c-d),\\ &= (a,b)\theta + (c,d)\theta.\end{aligned}$$

Furthermore $(0, 0)\theta = 0 - 0 = 0$.

EXAMPLE 3.5. Let $T = I \times J$ be the rectangular band then define $\alpha : T \to \mathcal{T}_J$ by $(i, j)\alpha = c_j$. Then we have

$$\begin{aligned}\big((i,j)(k,\ell)\big)\alpha &= (i,\ell)\alpha,\\ &= c_\ell,\\ &= c_j c_\ell,\\ &= (i,j)\alpha(k,\ell)\alpha.\end{aligned}$$

So, α is a morphism.

Definition: A bijective morphism is an *isomorphism.*

Isomorphisms preserve algebraic properties (e.g. commutativity). Suppose $f : S \to T$ is a morphism then with $A \subseteq S$ we have

$$Af = \{af \mid a \in A\}.$$

If $A = S$ then Sf is the image, $\operatorname{Im} f$, of S. So, if A is a subsemigroup of S then Af will be a subsemigroup of T. Now, conversely, if $B \subseteq T$ then we define

$$Bf^{-1} = \{s \in S \mid sf \in B\}.$$

If B is a subsemigroup of T then Bf^{-1} is either $\emptyset$ or Bf^{-1} is a subsemigroup of S, i.e. endomorphisms *pull back* subsemigroups.

Embeddings

Let $\alpha : S \to T$ be a morphism. From the handout, $\operatorname{Im}\alpha$ is a subsemigroup of T. If α is 1:1 then $\alpha : S \to \operatorname{Im}\alpha$ is an isomorphism and S is *embedded* in T.

Theorem 3.1 (The "Cayley Theorem" – for Semigroups)**.** *Every semigroup is embedded in some $\mathcal{T}_X$*

Proof. Let S be a semigroup and set $X = S^1$. We need a 1:1 morphism $S \to \mathcal{T}_X$. For $s \in S$, we define $\rho_s \in \mathcal{T}_X$ by $x\rho_s = xs$. Now, define $\alpha : S \to \mathcal{T}_X$ by $s\alpha = \rho_s$. First show that α is 1:1. If $s\alpha = t\alpha$ then $\rho_s = \rho_t$ and so $x\rho_s = x\rho_t$ for all $x \in S^1$; in particular $1\rho_s = 1\rho_t$ and so $1s = 1t$ hence $s = t$ and α is 1:1.

Let $u, b \in S$. For any $x \in X$ we have

$$x(\rho_u\rho_v) = (x\rho_u)\rho_v) = (xu)v = x(uv) = x\rho_{uv}.$$

Hence $\rho_u\rho_v = \rho_{uv}$ and so $u\alpha v\alpha = \rho_u\rho_v = \rho_{uv} = (uv)\alpha$. Therefore α is a morphism. Hence $\alpha : S \to \mathcal{T}_X$ is an embedding. □

Theorem 3.2 (The "Cayley Theorem" - for Monoids)**.** *Let S be a monoid then there exists an embedding $S \hookrightarrow \mathcal{T}_X$ for some X.*

Proof. We know from the proof of the Cayley Theorem for Semigroups that $\alpha : S \to \mathcal{T}_X$, given by $s\alpha = \rho_s$ where $x\rho_s = xs$, is a semigroup embedding. In the proof above we had $X = S^1 \Rightarrow X = S$ because S is a monoid. We must check that α is a monoid morphism, i.e. we need to check $1\alpha = I_X$. Now $1\alpha = \rho_1$ and for all $x \in X = S$ we have

$$x\rho_1 = x1 = x = xI_X$$

and so $1\alpha = \rho_1 = I_X$. □

Theorem 3.3 (The Cayley Theorem - for Groups)**.** *Let S be a group. Then there exists an embedding $S \hookrightarrow \mathcal{S}_X$ for some X.*

Proof. Exercise. □

3.2. Idempotents

Definition: $e \in S$ is an idempotent if $e^2 = e$. Also we define the set of idempotents in S to be

$$E(S) = \{e \in S \mid e^2 = e\}.$$

Now, $E(S)$ may be empty, e.g. $E(S) = \emptyset$ ($\mathbb{N}$ under $+$) but $E(S)$ may also be S. If $S = I \times J$ is a rectangular band then for any $(i, j) \in S$ we have $(i, j)^2 = (i, j)(i, j) = (i, j)$ and so $E(S) = S$.

Definition: If $E(S) = S$, then S is a *band*.

For the bicyclic semigroup B we have $E(B) = \{(a, a) \mid a \in \mathbb{N}^0\}$ – from exercises 1. If S is a monoid then $1 \in E(S)$. If S is a cancellative monoid, then 1 is the *only* idempotent: for if $e^2 = e$ then $ee = e1$ and so $e = 1$ by cancellation. In particular for S a group we have $E(S) = \{1\}$.

Lemma 3.1. *Suppose $ef = fe$ for all $f, e \in E(S)$. Then $E(S) = \emptyset$ or $E(S)$ is a subsemigroup.*

Proof. Let $e, f \in E(S)$. Then $(ef)^2 = efef = eeff = ef$ and hence $ef \in E(S)$. □

Definition: A commutative band is a *semilattice*.

From Lemma 3.1 if idempotents in S commute then $E(S)$ is empty or it's a semilattice.

Example 3.6. $E(B) = \{(a, a) \mid a \in \mathbb{N}^0\}$ is a semilattice.

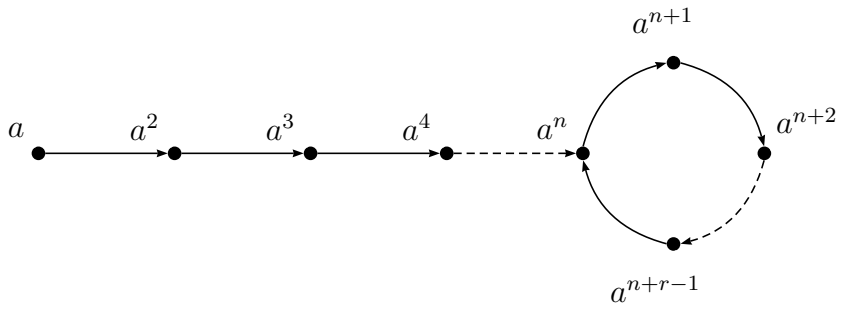
Example 3.7. A rectangular band $I \times J$ is *not* a semilattice (unless $|I| = |J| = 1$) since $(i, j)(k, \ell) = (k, \ell)(i, j) \Leftrightarrow i = k$ and $j = \ell$.

Definition: Let $a \in S$. Then we define $\langle a \rangle = \{a^n \mid n \in \mathbb{N}\}$, which is a commutative subsemigroup of S. We call $\langle a \rangle$ the *monogenic* subsemigroup of S generated by a.

Proposition. $\langle a \rangle \cong (\mathbb{N}, +)$ or $\langle a \rangle$ is finite.

Proof. If $a^i \neq a^j$ for all $i, j \in \mathbb{N}$ with $i \neq j$ then $\theta : \langle a \rangle \to \mathbb{N}$ defined by $a^i\theta = i$ is an isomorphism. Suppose that in the list of elements $a, a^2, a^3, \ldots$ there is a repetition, i.e. $a^i = a^j$ for some $i < j$. Let k be *least* such that $a^k = a^n$ for some $n < k$. Then $k = n + r$ for some $n, r \in \mathbb{N}$ – where n is the *index* of a, r is the *period* of a. Then the elements $a, a^2, a^3, \ldots, a^{n+r-1}$ are all distinct and $a^n = a^{n+r}$.

We can express this pictorially by a map diagram.



Notice that

$$a^{n+2r} = a^{n+r+r} = a^{n+r}a^r = a^n a^r = a^{n+r} = a^n$$

and hence $a^{n+rk} = a^n$ for all $k \in \mathbb{N}^0$. Let $u \in \mathbb{N}^0$. Write $u = qr + t$ with $0 \leqslant t < r$, $q, t \in \mathbb{N}^0$. Then $a^{n+u} = a^{n+qr+t} = a^{n+qr}a^t = a^n a^t = a^{n+t}$ and so we have

$$\langle a \rangle = \{a, a^2, \ldots, a^{n+r-1}\} \quad \text{and} \quad |\langle a \rangle| = n + r - 1. \qquad \square$$

Lemma 3.2 (The Idempotent Power Lemma)**.** *If $\langle a \rangle$ is finite, then it contains an idempotent.*

Proof. Let n, r be the index and period of a. Choose $s \in \mathbb{N}^0$ with $s \equiv -n \pmod{r}$. Then $s + n \equiv 0 \pmod{r}$ and so $s + n = kr$ for $k \in \mathbb{N}$. Then

$$(a^{n+s})^2 = a^{n+n+s+s} = a^{n+kr+s} = a^{n+kr}a^s = a^n a^s = a^{n+s}$$

and so $a^{n+s} \in E(S)$. In fact, $\{a^n, a^{n+1}, \ldots, a^{n+r-1}\}$ is a group with identity a^{n+s}. $\square$

Corollary 3.1. *Any finite semigroup contains an idempotent.*

3.3. Idempotents in $\mathcal{T}_X$

We know $c_x c_y = c_y$ for all $x, y \in X$ and hence $c_x c_y = c_x$ for all $x \in X$. Therefore $c_x \in E(\mathcal{T}_X)$ for all $x \in X$.

Example 3.8. Let us define an element

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix} \in E(\mathcal{T}_X)$$

and a subset $Z \subseteq X$. The "restriction of α to Z", denoted "$\alpha\,|_Z$" is the map $\alpha_Z : Z \to Y$ such that $Z(\alpha_Z) = Z\alpha$.

Example 3.9. Let us define an element

$$\alpha = \begin{pmatrix} a & b & c & d \\ 1 & 1 & 1 & 2 \end{pmatrix} \Rightarrow \alpha|_{\{c,d\}} = \begin{pmatrix} c & d \\ 1 & 2 \end{pmatrix}$$

We can see that α is *not* one-to-one but $\alpha|_{\{c,d\}}$ is.

Let $\alpha \in \mathcal{T}_X$ (i.e. $\alpha : X \to X$). Recall that $\operatorname{Im}\alpha = \{x\alpha : x \in X\} \subseteq X$.

EXAMPLE 3.10. In $\mathcal{T}_3$ we have $\operatorname{Im} c_1 = \{1\}$, $\operatorname{Im} I_3 = \{1,2,3\}$ then

$$\operatorname{Im}\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 3\end{pmatrix} = \{2,3\}.$$

Lemma 3.3 (The $E(\mathcal{T}_X)$ Lemma)**.** *An element $\varepsilon \in \mathcal{T}_X$ is idempotent $\Leftrightarrow \varepsilon|_{\operatorname{Im}\varepsilon} = I_{\operatorname{Im}\varepsilon}$.*

Proof. $\varepsilon|_{\operatorname{Im}\varepsilon}$ means for all $y \in \operatorname{Im}\varepsilon$ we have $y\varepsilon = y$. Then

$$\begin{aligned}
\varepsilon \in E(\mathcal{T}_X) &\Leftrightarrow \varepsilon^2 = \varepsilon,\\
&\Leftrightarrow x\varepsilon^2 = x\varepsilon && \text{for all } x \in X,\\
&\Leftrightarrow (x\varepsilon)\varepsilon = x\varepsilon && \text{for all } x \in X,\\
&\Leftrightarrow y\varepsilon = y && \text{for all } y \in \operatorname{Im}\varepsilon,\\
&\Leftrightarrow \varepsilon|_{\operatorname{Im}\varepsilon} = I_{\operatorname{Im}\varepsilon}.
\end{aligned}$$

□

EXAMPLE 3.11. Define an element

$$\alpha = \begin{pmatrix}1 & 2 & 3\\ 2 & 2 & 3\end{pmatrix} \in \mathcal{T}_3,$$

this has image, $\operatorname{Im}\alpha = \{2,3\}$. Now we can see that $2\alpha = 2$ and $3\alpha = 3$. Hence $\alpha \in E(\mathcal{T}_3)$.

EXAMPLE 3.12. We can similarly create another idempotent in $\mathcal{T}_5$,

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 5 & 3 & 3 & 5\end{pmatrix} \in E(\mathcal{T}_5).$$

Using Lemma 3.3 we can now list all the idempotents in $\mathcal{T}_3$. We start with the constant maps, i.e. $\varepsilon \in E(\mathcal{T}_3)$ such that $|\operatorname{Im}\varepsilon| = 1$. These are

$$\begin{pmatrix}1 & 2 & 3\\ 1 & 1 & 1\end{pmatrix}, \quad \begin{pmatrix}1 & 2 & 3\\ 2 & 2 & 2\end{pmatrix}, \quad \begin{pmatrix}1 & 2 & 3\\ 3 & 3 & 3\end{pmatrix}.$$

Now consider all elements $\varepsilon \in E(\mathcal{T}_3)$ such that $|\operatorname{Im}\varepsilon| = 2$. These are

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 2 & 3\end{pmatrix}, \quad \begin{pmatrix}1 & 2 & 3\\ 1 & 1 & 3\end{pmatrix}, \quad \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 3\end{pmatrix}, \quad \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 3\end{pmatrix}, \quad \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 1\end{pmatrix}, \quad \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 2\end{pmatrix}.$$

Now there is only one idempotent such that $|\operatorname{Im}\varepsilon| = 3$, that is the identity map

$$\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}.$$

4. Relations

Definition: A (binary) *relation* ρ on A is a subset of $A \times A$.

Convention: we may write "$a\rho b$" for "$(a, b) \in \rho$".

4.1. **Partial Orders**

We define a partial ordering $\leqslant$ on $\mathbb{R}$.

$$\begin{aligned} a \leqslant a & \qquad \text{for all } a \in \mathbb{R}, \\ a \leqslant b \text{ and } b \leqslant c \Rightarrow a \leqslant c & \qquad \text{for all } a, b, c \in \mathbb{R}, \\ a \leqslant b \text{ and } b \leqslant a \Rightarrow a = b & \qquad \text{for all } a, b \in \mathbb{R}. \end{aligned}$$

Notice that for any $a, b \in \mathbb{R}$ we have $a \leqslant b$ or $b \geqslant a$. For X a set then $\mathcal{P}(X)$ is the set of all subsets of X. Now $\subseteq$ is a partial order on $\mathcal{P}(X)$. We have

$$\begin{aligned} A \subseteq A & \qquad \text{for all } A \in \mathcal{P}(X) \\ A \subseteq B \text{ and } B \subseteq C \Rightarrow A \subseteq C & \qquad \text{for all } A, B, C \in \mathcal{P}(X) \\ A \subseteq B \text{ and } B \subseteq A \Rightarrow A = B & \qquad \text{for all } A, B \in \mathcal{P}(X) \end{aligned}$$

Notice that if $|X| > 2$ and $x, y \in X$ with $x \neq y$ then $\{x\} \not\subseteq \{y\}$ and $\{y\} \not\subseteq \{x\}$. If $\omega = A \times A$ is the UNIVERSAL relation on A, so $x\omega y$ for all $x, y \in A$, then $[x] = A$ for all $x \in A$. We have that

$$\iota = \big\{(a, a) \mid a \in A\big\}$$

is the EQUALITY relation and so $x\iota y \Leftrightarrow x = y$ and so $[x] = \{x\}$ for all $x \in A$.

4.2. **Algebra of Relations**

If ρ, λ are relations on A, then so is $\rho \cap \lambda$. For all $a, b \in A$ we have

$$\begin{aligned} a(\rho \cap \lambda)b &\Leftrightarrow (a, b) \in (\rho \cap \lambda) \\ &\Leftrightarrow (a, b) \in \rho \text{ and } (a, b) \in \lambda \\ &\Leftrightarrow a\rho b \text{ and } a\lambda b. \end{aligned}$$

We note that $\rho \subseteq \lambda$ means $a\rho b \Rightarrow a\lambda b$. Note $\iota \subseteq \rho \Rightarrow \rho$ is reflexive and so $\iota \subseteq \rho$ for any equivalence relation ρ. We see that ι is the smallest equivalence relation on A and ω is the largest equivalence relation on A. We note that

$$[a] = \{b \in A \mid a\rho b\}.$$

If ρ is an equivalence relation then $[a]$ is the equivalence-class, a ρ-class, of a.

Lemma 4.1. *If ρ, λ are equivalence relations on A then so is $\rho \cap \lambda$.*

Proof. We have $\iota \subseteq \rho$ and $\iota \subseteq \lambda$, then $\iota \subseteq \rho \subseteq \lambda$, so $\rho \cap \lambda$ is reflexive. Suppose $(a, b) \in \rho \cap \lambda$. Then $(a, b) \in \rho$ and $(a, b) \in \lambda$. So as ρ, λ are symmetric, we have $(b, a) \in \rho$ and $(b, a) \in \lambda$ and hence $(b, a) \in \rho \cap \lambda$. Therefore $\rho \cap \lambda$ is symmetric. By a similar argument we have $\rho \cap \lambda$ is transitive. Therefore $\rho \cap \lambda$ is an equivalence relation. □

Denoting by $[a]_\rho$ the ρ-class of a and $[a]_\lambda$ the λ-class of a we have that,

$$\begin{aligned}
[a]_{\rho\cap\lambda} &= \{b \in A \mid b\rho \cap \lambda a\}, \\
&= \{b \in A \mid b\rho a \text{ and } b\lambda a\}, \\
&= \{b \in A \mid b\rho a\} \cap \{b \in A \mid b\lambda a\}, \\
&= [a]_\rho \cap [a]_\lambda.
\end{aligned}$$

We note that $\rho \cup \lambda$ need not be an equivalence relation. On $\mathbb{Z}$ we have

$$\begin{aligned}
3 &\equiv 1 \pmod 2, \\
1 &\equiv 4 \pmod 3.
\end{aligned}$$

If $\big(\equiv (\mathrm{mod}\, 2)\big) \cup \big(\equiv (\mathrm{mod}\, 3)\big)$ were to be transitive then we would have

$$\left.\begin{aligned}
(3,1) &\in \big(\equiv (\mathrm{mod}\, 2)\big) \cup \big(\equiv (\mathrm{mod}\, 3)\big) \\
(1,4) &\in \big(\equiv (\mathrm{mod}\, 2)\big) \cup \big(\equiv (\mathrm{mod}\, 3)\big)
\end{aligned}\right\} \Rightarrow (3,4) \in \big(\equiv (\mathrm{mod}\, 2)\big) \cup \big(\equiv (\mathrm{mod}\, 3)\big)$$
$$\Rightarrow 3 \equiv 4 \pmod 2 \quad \text{or} \quad 3 \equiv 4 \pmod 3$$

but this is a contradiction!

Kernels

Let $\alpha : X \to Y$ be a function. Define a relation $\ker \alpha$ on X by the rule

$$a \ker \alpha b \Leftrightarrow a\alpha = b\alpha.$$

We may sometimes write $a \equiv_\alpha b$. It is clear that $\ker \alpha$ is an equivalence relation on X. The $\ker \alpha$ classes partition X into disjoint subsets; a, b lie in the same class iff $a\alpha = b\alpha$.

Example 4.1. Let $\alpha : \underline{6} \to \underline{4}$ where

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 3 & 2 & 2 & 1 \end{pmatrix}$$

$\ker \alpha$ is the *kernel of* α.

Definition: An equivalence relation ρ on a semigroup S is a *congruence* if

$$(a\rho b \text{ and } c\rho d) \Rightarrow ac\rho bd.$$

Lemma 4.2 (The Kernel Lemma)**.** *Let $\theta : S \to T$ be a semigroup morphism. Then* $\ker\theta$ *is a congruence on S.*

Proof. We know $\ker\theta$ is an equivalence relation on S. Suppose $a, b, c, d \in S$ with

$$a \ker\theta b \text{ and } c \ker\theta d.$$

Then $a\theta = b\theta$ and $c\theta = d\theta$, so

$$(ac)\theta = a\theta c\theta = b\theta d\theta = (bd)\theta.$$

Therefore $ac \ker\theta bd$, so that $\ker\theta$ is a congruence. □

Let ρ be a congruence on S. Then we define

$$S/\rho = \big\{[a] \mid a \in S\big\}.$$

Define a binary relation on S/ρ by

$$[a][b] = [ab].$$

We need to make sure that this is a well-defined relation. If $[a] = [a']$ and $[b] = [b']$ then $a\rho a'$ and $b\rho b'$; as ρ is a congruence we have $ab\rho a'b'$ and hence $[ab] = [a'b']$. Hence our operation is well defined. Let $[a], [b], [c] \in S/\rho$ then we have

$$\begin{aligned}
[a]\big([b][c]\big) &= [a][bc], \\
&= \big[a(bc)\big], \\
&= \big[(ab)c\big], \\
&= [ab][c], \\
&= \big([a][b]\big)[c].
\end{aligned}$$

If S is a monoid, then so is S/ρ because we have

$$[1][a] = [1a] = [a] = [a1] = [a][1]$$

for any $a \in S$. Hence we conclude that S/ρ is a semigroup and if S is a monoid, then so is S/ρ. We call S/ρ the *factor semigroup* (or monoid) of S by ρ. Now, define $\nu_\rho : S \to S/\rho$ by

$$s\nu_\rho = [s].$$

Then we have

$$\begin{aligned} s\nu_\rho t\nu_\rho &= [s][t] && \text{definition of } \nu_\rho, \\ &= [st] && \text{definition of multiplication in } S/\rho, \\ &= (st)\nu_\rho && \text{definition of } \nu_\rho. \end{aligned}$$

Hence ν_ρ is a semigroup morphism. We now want to examine the kernel of ν_ρ and so

$$\begin{aligned} s \ker \nu_\rho t &\Leftrightarrow s\nu_\rho = t\nu_\rho && \text{definition of } \ker \nu_\rho, \\ &\Leftrightarrow [s] = [t] && \text{definition of } \nu_\rho, \\ &\Leftrightarrow s\rho t && \text{definition of } \rho. \end{aligned}$$

Therefore $\rho = \ker \nu_\rho$ and so every congruence is the kernel of a morphism.

Theorem 4.1 (The Fundamental Theorem of Morphisms for Semigroups)**.** *Let $\theta : S \to T$ be a semigroup morphism. Then $\ker \theta$ is a congruence on S, $\operatorname{Im} \theta$ is a subsemigroup of T and $S/\ker \theta \cong \operatorname{Im} \theta$.*

Proof. Define $\bar{\theta} : S/\ker \theta \to \operatorname{Im} \theta$ by $[a]\bar{\theta} = a\theta$. We have

$$\begin{aligned} [a] = [b] &\Leftrightarrow a \ker \theta b \\ &\Leftrightarrow a\theta = b\theta \\ &\Leftrightarrow [a]\bar{\theta} = [b]\bar{\theta}. \end{aligned}$$

Hence $\bar{\theta}$ is well defined and one-to-one. For any $x \in \operatorname{Im} \theta$ we have $x = a\theta = [a]\bar{\theta}$ and so $\bar{\theta}$ is onto. Finally,

$$\big([a][b]\big)\bar{\theta} = [ab]\bar{\theta} = (ab)\theta = a\theta b\theta = [a]\bar{\theta}[b]\bar{\theta}.$$

Therefore $\bar{\theta}$ is an isomorphism and $S/\ker \theta \cong \operatorname{Im} \theta$. Note that the analogous result holds for monoids. □

5. Ideals

Notation

If $A, B \subseteq S$ then we write

$$\begin{aligned} AB &= \{ab \mid a \in A, b \in B\}, \\ A^2 = AA &= \{ab \mid a, b \in A\}. \end{aligned}$$

Note. A is a subsemigroup if and only if $A \neq \emptyset$ and $A^2 \subseteq A$.

We write aB for $\{a\}B = \{ab \mid b \in B\}$. For example

$$AaB = \{xay \mid x \in A, y \in B\}.$$

Facts:

(1) $A(BC) = (AB)C$ therefore $\mathcal{P}(S) = \{S \mid A \subseteq S\}$ is a semigroup – the *power semigroup* of S.
(2) $A \subseteq B \Rightarrow AC \subseteq BC$ and $CA \subseteq CB$ for all $A, B, C \in \mathcal{P}(S)$.
(3) $AC = BC \not\Rightarrow A = B$ and $CA = CB \not\Rightarrow A = B$, i.e. the power semigroup is not cancellative.

Definition: Let $\emptyset \neq I \subseteq S$ then I is a *right ideal* if $IS \subseteq I$ (i.e. $a \in I, s \in S \Rightarrow as \in I$). Then I is a *left ideal* if $SI \subseteq I$. Finally I is a *(two sided) ideal* if $IS \cup SI \subseteq I$.

Any (left/right) ideal is a subsemigroup. If S is commutative, all 3 concepts coincide.

EXAMPLE 5.1. Some examples of ideals.

(1) Let $i \in I$ then $\{i\} \times J$ is a right ideal in a rectangular band $I \times J$.
(2) We define a right ideal $\{(x, y) \mid x \geqslant m, y \in \mathbb{N}^0\}$ in the bicyclic semigroup B (m fixed).
(3) $Y \subseteq X$ then we have $\{\alpha \in \mathcal{T}_X \mid \operatorname{Im} \alpha \subseteq Y\}$ is a left ideal of $\mathcal{T}_X$.
(4) For any $n \in \mathbb{N}$ we define

$$S^n = \{a_1 a_2 \dots a_n \mid a_i \in S\}.$$

This is an ideal of S. If S is a monoid then $S^n = S$ for all n, since for any $s \in S$ we can write

$$s = s\underbrace{11\dots1}_{n-1} \in S^n.$$

(5) If S has a zero 0, then $\{0\}$ (usually written 0), is an ideal.

Definition: For a semigroup S we have:

(1) S is *simple* if S is the only ideal.
(2) if S has a zero 0, then S is *0-simple* if S and $\{0\}$ are the only ideals and $S^2 \neq 0$.

EXAMPLE 5.2. Let G be a group and I a left ideal. Let $g \in G, a \in I$ then we have

$$g = (ga^{-1})a \in I$$

and so $G = I$. Therefore G has no proper left/right ideals. Hence G is simple.

Exercise: G^0 is 0-simple

EXAMPLE 5.3. We have $(\mathbb{N}, +)$ is a semigroup. Now define $I_n \subseteq (\mathbb{N}, +)$ to be

$$I_n = \{n, n+1, n+2, \dots\},$$

which is an ideal. Hence $\mathbb{N}$ is not simple.

Note. $\{2, 4, 6, \dots\}$ is a subsemigroup but *not* an ideal.

EXAMPLE 5.4. The bicyclic semigroup B is simple.

Proof. Let $I \subseteq B$ be an ideal, say $(m,n) \in I$. Then $(0,n) = (0,m)(m,n) \in I$. Thus $(0,0) = (0,n)(n,0) \in I$. Let $(a,b) \in B$. Then

$$(a,b) = (a,b)(0,0) \in I$$

and hence $B = I \Rightarrow B$ is simple. □

5.1. **Principle Ideals**

We make note of how the S^1 notation can be used. For example

$$\begin{aligned} S^1A &= \{sa \mid s \in S^1, a \in A\}, \\ &= \{sa \mid s \in S \cup \{1\}, a \in A\}, \\ &= \{sa \mid s \in S, a \in A\} \cup \{1a \mid a \in A\}, \\ &= SA \cup A. \end{aligned}$$

In particular, if $A = \{a\}$ then $S^1a = Sa \cup \{a\}$. So,

$$\begin{aligned} S^1a = Sa &\Leftrightarrow a \in Sa, \\ &\Leftrightarrow a = ta \end{aligned}$$

for some $t \in S$. We have $S^1a = Sa$ for $a \in S$ if:

- S is a *monoid* (then $a = 1a$).
- $a \in E(S)$ (then $a = aa$).
- a is *regular*, i.e. there exists $x \in S$ with $a = axa$ (then $a = (ax)a$).

But in $(\mathbb{N}, +)$ we have $1 \notin 1 + \mathbb{N}$. Dually,

$$aS^1 = aS \cup \{a\}$$

and similarly

$$S^1aS^1 = SaS \cup aS \cup Sa \cup \{a\}.$$

For $\emptyset \neq I \subseteq S$ then we have I is an ideal $\Leftrightarrow S^1IS^1 \subseteq I$.

Claim. aS^1 is the "smallest" right ideal containing a.

Proof. $a = a1 \in aS^1$ and $(aS^1)S = a(S^1S) \subseteq aS^1$. So, aS^1 is a right ideal containing a. If $a \in I$ and I is a right ideal, then $aS^1 \subseteq IS^1 = I \cup IS \subseteq I$. Then aS^1 is the *principal right ideal generated by* a. S^1a is the *principal left ideal generated by* a. S^1aS^1 is the smallest ideal containing a – it's the called the *principal ideal generated by* a. □

If S is commutative then $aS^1 = S^1a = S^1aS^1$.

EXAMPLE 5.5. In a group G we have

$$aG^1 = G = G^1a = G^1aG^1$$

for all $a \in G$.

EXAMPLE 5.6. In $\mathbb{N}$ under addition we have

$$I_n = \{n, n+1, n+2, \dots\} = \text{“}n + \mathbb{N}^1\text{”}$$

EXAMPLE 5.7. B is simple, so

$$B(m,n)B = B^1(m,n)B^1 = B$$

Claim. $(m,n)B = (m,n)B^1 = \big\{(x,y) \mid x \geqslant m, y \in \mathbb{N}^0\big\}$

Proof. We have

$$\begin{aligned}(m,n)B &= \big\{(m,n)(u,v) \mid (u,v) \in B\big\} \\ &\subseteq \big\{(x,y) \mid x \geqslant m, y \in \mathbb{N}^0\big\}.\end{aligned}$$

Let $x \geqslant m$ then

$$\begin{aligned}(m,n)\big(n + (x-m), y\big) &= \big(m - n + n + (x-m), y\big), \\ &= (x,y).\end{aligned}$$

Therefore $(x,y) \in (m,n)B \Rightarrow \big\{(x,y) \mid x \geqslant m, y \in \mathbb{N}^0\big\} \subseteq (m,n)B$. hence we have proved our claim. □

Dually we have $B(m,n) = \big\{(x,y) \mid x \in \mathbb{N}^0, y \geqslant n\big\}$.

Lemma 5.1 (Principle Left Ideal Lemma)**.** *The following statements are equivalent;*

i) $S^1a \subseteq S^1b$,
ii) $a \in S^1b$,
iii) $a = tb$ *for some* $t \in S^1$,
iv) $a = b$ *or* $a = tb$ *for some* $t \in S$.

Note. If $S^1a = Sa$ and $S^1b = Sb$, then the Lemma can be adjusted accordingly.

Proof. It is clear that (i) ⇒ (iii) ⇒ (iv) ⇒ (i) and so we prove (i) ⇔ (ii).

(i) ⇒ (ii): If $S^1a \subseteq S^1b$ then $a = 1a \in S^1a \subseteq S^1b \Rightarrow a \in S^1b$.

(ii) ⇒ (i): If $a \in S^1b$, then as S^1a is the smallest left ideal containing a, and as S^1b is a left ideal we have $S^1a \subseteq S^1b$. □

Lemma 5.2 (Principle Right Ideal Lemma)**.** *The following statements are equivalent:*

i) $aS^1 \subseteq bS^1$,
ii) $a \in bS^1$,

iii) $a = bt$ *for some* $t \in S^1$,
iv) $a = b$ *or* $a = bt$ *for some* $t \in S$.

Note. If $aS = aS^1$ and $bS = bS^1$ then $aS \subseteq bS \Leftrightarrow a \in bS \Leftrightarrow a = bt$ for some $t \in S$.

Definition: The relation $\mathcal{L}$ on a semigroup S is defined by the rule

$$a\mathcal{L}b \Leftrightarrow S^1a = S^1b$$

for any $a, b \in S$.

Note.

(1) $\mathcal{L}$ is an equivalence.
(2) If $a\mathcal{L}b$ and $c \in S$ then $S^1a = S^1b$, so $S^1ac = S^1bc$ and hence $ac\mathcal{L}bc$, i.e. $\mathcal{L}$ is right compatible.
(3) a right (left) compatible equivalence is a *right* (*left*) *congruence*. Thus $\mathcal{L}$ is a right congruence.

Corollary 5.1. *We have that*

$$\boxed{a\mathcal{L}b \Leftrightarrow \exists\, s, t \in S^1 \text{ with } a = sb \text{ and } b = ta.}$$

Proof. We start with $a\mathcal{L}b$

$$\begin{aligned} a\mathcal{L}b &\Leftrightarrow S^1a = S^1b \\ &\Leftrightarrow S^1a \subseteq S^1b \text{ and } S^1b \subseteq S^1a \\ &\Leftrightarrow \exists\, s, t \in S^1 \text{ with } a = sb, b = ta \end{aligned}$$

by the Principle Left Ideal Lemma. We note that this statement about $\mathcal{L}$ can be used as a definition of $\mathcal{L}$. □

Remark.

(1) $a\mathcal{L}b \Leftrightarrow a = b$ or there exists $s, t \in S$ with $a = sb$, $b = ta$.
(2) If $Sa = S^1a$ and $Sb = S^1b$, then $a\mathcal{L}b \Leftrightarrow \exists\, s, t \in S$ with $a = sb$, $b = ta$.

Dually, the relation $\mathcal{R}$ is defined on S by

$$\begin{aligned} a\mathcal{R}b &\Leftrightarrow aS^1 = bS^1, \\ &\Leftrightarrow \exists\, s, t \in S^1 \text{ with } a = bs \text{ and } b = at, \\ &\Leftrightarrow a = b \text{ or } \exists\, s, t \in S \text{ with } a = bs \text{ and } b = at. \end{aligned}$$

We can adjust this if $aS^1 = aS$ as before. Now $\mathcal{R}$ is an *equivalence*; it is *left compatible* and hence a *left congruence*.

Definition: We define the relation $\mathcal{H} = \mathcal{L} \cap \mathcal{R}$ and note that $\mathcal{H}$ is an equivalence.

The relations $\mathcal{L}, \mathcal{R}, \mathcal{H}$ are in fact three of *Greens' relations*.

EXAMPLE 5.8. If S is commutative, $\mathcal{L} = \mathcal{R} = \mathcal{H}$. In a group G,

$$G^1a = G = G^1b \quad \text{and} \quad aG^1 = G = bG^1 \quad \text{for all } a, b \in G.$$

So $a\mathcal{L}b$ and $a\mathcal{R}b$ for all $a, b \in G$. Therefore $\mathcal{L} = \mathcal{R} = \omega = G \times G$ and hence we must have $\mathcal{H} = \omega$.

EXAMPLE 5.9. In $\mathbb{N}$ under $+$ we have

$$a + \mathbb{N}^1 = \{a, a+1, \dots\}$$

and so $a + \mathbb{N}^1 = b + \mathbb{N}^1 \Leftrightarrow a = b$. Hence $\mathcal{L} = \mathcal{R} = \mathcal{H} = \iota$.

EXAMPLE 5.10. In B we know

$$(m, n)B = \left\{(x, y) \mid x \geqslant m, y \in \mathbb{N}^0\right\}$$

and so we have

$$(m, n)B = (p, q)B \Leftrightarrow m = p.$$

Hence $(m, n)\mathcal{R}(p, q) \Leftrightarrow m = p$. Dually,

$$(m, n)\mathcal{L}(p, q) \Leftrightarrow n = q.$$

Thus $(m, n)\mathcal{H}(p, q) \Leftrightarrow (m, n) = (p, q)$, which gives us $\mathcal{H} = \iota$.

5.2. $\mathcal{L}$ and $\mathcal{R}$ in $\mathcal{T}_X$

Claim. $\alpha\mathcal{T}_X \subseteq \beta\mathcal{T}_X \Leftrightarrow \operatorname{Ker}\beta \subseteq \operatorname{Ker}\alpha$. [Recall $\operatorname{Ker}\alpha = \left\{(x, y) \in X \times X \mid x\alpha = y\alpha\right\}$].

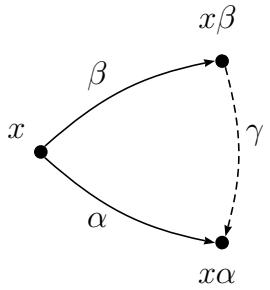
Proof. ($\Rightarrow$) Suppose $\alpha\mathcal{T}_X \subseteq \beta\mathcal{T}_X$. Then $\alpha = \beta\gamma$ for some $\gamma \in \mathcal{T}_X$. Let $(x, y) \in \operatorname{Ker}\beta$. Then

$$x\alpha = x(\beta\gamma) = (x\beta)\gamma = (y\beta)\gamma = y(\beta\gamma) = y\alpha.$$

Hence $(x, y) \in \operatorname{Ker}\alpha$ and so $\operatorname{Ker}\beta \subseteq \operatorname{Ker}\alpha$.

($\Leftarrow$) Suppose $\operatorname{Ker}\beta \subseteq \operatorname{Ker}\alpha$. Define $\gamma : X \to X$ by

$$(x\beta)\gamma = x\alpha$$



Thus we have $y\gamma = x_o$, $y \notin \operatorname{Im}\beta$ where x_0 is fixed. If $z = x\beta = y\beta$, then $(x, y) \in \operatorname{Ker}\beta \subseteq \operatorname{Ker}\alpha$ so $x\alpha = y\alpha$. Hence γ is well-defined. So $\gamma \in \mathcal{T}_X$ and $\beta\gamma = \alpha$. Therefore $\alpha \in \beta\mathcal{T}_X$ so that by the Principle Ideal Lemma, $\alpha\mathcal{T}_X \subseteq \beta\mathcal{T}_X$. □

Corollary 5.2 ($\mathcal{R} - \mathcal{T}_X$-Lemma)**.** $\alpha\mathcal{R}\beta \Leftrightarrow \operatorname{Ker}\alpha = \operatorname{Ker}\beta$.

Proof. We have

$$\begin{aligned}\alpha\mathcal{R}\beta &\Leftrightarrow \alpha\mathcal{T}_X = \beta\mathcal{T}_X \\ &\Leftrightarrow \alpha\mathcal{T}_X \subseteq \beta\mathcal{T}_X \text{ and } \beta\mathcal{T}_X \subseteq \alpha\mathcal{T}_X \\ &\Leftrightarrow \operatorname{Ker}\beta \subseteq \operatorname{Ker}\alpha \text{ and } \operatorname{Ker}\alpha \subseteq \operatorname{Ker}\beta \\ &\Leftrightarrow \operatorname{Ker}\alpha = \operatorname{Ker}\beta.\end{aligned}$$

□

Fact: $\mathcal{T}_X\alpha \subseteq \mathcal{T}_X\beta \Leftrightarrow \operatorname{Im}\alpha \subseteq \operatorname{Im}\beta$ (Exercise 4).

Corollary 5.3 ($\alpha - \mathcal{T}_X$-Lemma)**.** $\alpha\mathcal{L}\beta \Leftrightarrow \operatorname{Im}\alpha = \operatorname{Im}\beta$.

Consequently $\alpha\mathcal{H}\beta \Leftrightarrow \operatorname{Ker}\alpha = \operatorname{Ker}\beta$ and $\operatorname{Im}\alpha = \operatorname{Im}\beta$.

Example 5.11. Let us define

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix} \in E(\mathcal{T}_3)$$

Now we have $\operatorname{Im}\varepsilon = \{2, 3\}$. We can see that $\operatorname{Ker}\epsilon$ has classes $\{1, 2\}, \{3\}$. So

$$\begin{aligned}\alpha\mathcal{H}\varepsilon &\Leftrightarrow \operatorname{Im}\alpha = \operatorname{Im}\varepsilon \text{ and } \operatorname{Ker}\alpha = \operatorname{Ker}\epsilon \\ &\Leftrightarrow \operatorname{Im}\alpha = \{2, 3\} \text{ and } \operatorname{Ker}\alpha \text{ has classes } \{1, 2\}, \{3\}.\end{aligned}$$

So we have

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 2 \end{pmatrix} \qquad \text{or} \qquad \alpha = \varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix}$$

	ε	α
ε	ε	α
α	α	ε

which is the table of a 2-element group. Thus the $\mathcal{H}$-class of ε is a group.

5.3. **Subgroups of Semigroups**

S is a semigroup, $H \subseteq S$. Then H is a *subgroup* of S if it is a group under (the restriction of) the binary operation on S to H; i.e.

- $a, b \in H \Rightarrow ab \in H$
- $\exists\, e \in H$ with $ea = a = ae$ for all $a \in H$
- $\forall\, a \in H\ \exists\, b \in H$ with $ab = e = ba$

Remark.

(1) S does not have to be a monoid. Even if S *is* a monoid, e does not have to be 1. However, e must be an idempotent, i.e. $e \in E(S)$.
(2) If H is a subgroup with identity e, then e is the *only* idempotent in H.

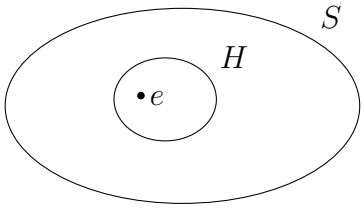


FIGURE 2. e is the only idempotent in H.

(3) If $e \in E(S)$, then $\{e\}$ is a trivial subgroup.
(4) $\mathcal{S}_X$ is a subgroup of $\mathcal{T}_X$; $\{\varepsilon, \alpha\}$ (as above) is a subgroup of $\mathcal{T}_3$. Notice

$$\begin{aligned} \alpha \mathcal{H} I_X &\Leftrightarrow \operatorname{Im}\alpha = \operatorname{Im} I_X \text{ and } \operatorname{Ker}\alpha = \operatorname{Ker} I_X, \\ &\Leftrightarrow \operatorname{Im}\alpha = X \text{ and } \operatorname{Ker}\alpha = \iota, \\ &\Leftrightarrow \alpha \text{ is onto and } \alpha \text{ is 1:1}, \\ &\Leftrightarrow \alpha \in \mathcal{S}_X. \end{aligned}$$

Therefore $\mathcal{S}_X$ is the $\mathcal{H}$-class of I_X.

Definition: L_a is the $\mathcal{L}$-class of a; R_a is the $\mathcal{R}$-class of a and H_a is the $\mathcal{H}$-class of a.

Now $L_a = L_b \Leftrightarrow a \mathcal{L} b$ and $H_a = L_a \cap R_a$. In B, $L_{(2,3)} = \{(x, 3) \mid x \in \mathbb{N}^0\}$.

5.4. **Maximal Subgroup Theorem**

Let $e \in E(S)$. Then H_e is the maximal subgroup of S with identity e.

Lemma 5.3 (Principle Ideal for Idempotents)**.** *Let $a \in S$, $e \in E(S)$. Then*

(i) $S^1 a \subseteq S^1 e \Leftrightarrow ae = a$
(ii) $aS^1 \subseteq eS^1 \Leftrightarrow ea = a$.

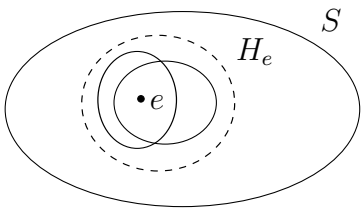


FIGURE 3. Existence of a Maximal Subgroup.

Proof. (We prove part (i) only because (ii) is dual). If $ae = a$, then $a \in S^1e$ so $S^1a \subseteq S^1e$ by the Principle Ideal Lemma. Conversely, if $S^1a \subseteq S^1e$ then by the Principle Ideal Lemma we have $a = te$ for some $t \in S^1$. Then

$$ae = (te)e = t(ee) = te = a.$$

□

Corollary 5.4. *Let $e \in ES$. Then we have*

$$\begin{aligned} a\mathcal{R}e &\Rightarrow ea = a, \\ a\mathcal{L}e &\Rightarrow ae = a, \\ a\mathcal{H}e &\Rightarrow a = ae = ea. \end{aligned}$$

Idempotents are left/right/two-sided identities for their $\mathcal{R}/\mathcal{L}/\mathcal{H}$-classes.

Proof. Let G be a subgroup with idempotent e. Then for any $a \in G$ we have $ea = a = ae$ and there exists $a^{-1} \in G$ with $aa^{-1} = e = a^{-1}a$. Then

$$\left.\begin{aligned} ea &= a \\ aa^{-1} &= e \end{aligned}\right\} \Rightarrow a\mathcal{R}e$$

$$\left.\begin{aligned} ae &= a \\ a^{-1}a &= e \end{aligned}\right\} \Rightarrow a\mathcal{L}e$$

$$\Rightarrow a\mathcal{H}e.$$

Therefore $G \subseteq He$. □

Theorem 5.1 (Maximal Subgroup Theorem)**.** *Let $e \in E(S)$. Then $\mathcal{H}_e$ is the maximal subgroup of S with identity e.*

Proof. We have shown G a subgroup with identity $e \Rightarrow G \subseteq \mathcal{H}_e$. We know $\mathcal{H}_e$ is a subgroup with identity, e. We know that e is an identity for $\mathcal{H}_e$. Suppose $a, b \in \mathcal{H}_e$. Then $b\mathcal{H}e$, so $b\mathcal{R}e$ hence $ab\mathcal{R}ae$ ($\mathcal{R}$ is left compatible) so $ab\mathcal{R}ae = a\mathcal{R}e$. Also, $a\mathcal{L}e \Rightarrow ab\mathcal{L}eb = b\mathcal{L}e$ hence $ab\mathcal{H}e$ so $ab \in \mathcal{H}_e$. It remains to show that for all $a \in \mathcal{H}_e$ there exists $b \in \mathcal{H}_e$ with $ab = e = ba$.

Let $a \in \mathcal{H}_e$ by definition of $\mathcal{H} = \mathcal{R} \cap \mathcal{L}$ there exists $s, t \in S^1$ with

$$\underbrace{at = e}_{a\mathcal{R}e} \underbrace{= sa}_{a\mathcal{L}e}.$$

We have $e = ee = ate$

$$e \cdot ee = eee = a(ete) = (ese)a.$$

Let $b = ete$, $c = ese$ so $b, c \in S$ and $eb = be = b$, $ec = ce = c$. Also $e = ab = ca$. Now

$$b = eb = (ca)b = c(ab) = ce = c.$$

Finally,

$$\underbrace{eb = b \quad ba = e}_{b\mathcal{R}e} \qquad \underbrace{be = b \quad ab = e}_{b\mathcal{L}e}$$

so $b\mathcal{H}e \Rightarrow b \in \mathcal{H}_e$. Hence $\mathcal{H}_e$ is a subgroup. □

Let's take 2 distinct idempotents $e, f \in E(S)$ with $e \neq f$. Since $\mathcal{H}_e$ and $\mathcal{H}_f$ are subgroups $\mathcal{H}_e \neq \mathcal{H}_f \Rightarrow \mathcal{H}_e \cap \mathcal{H}_f = \emptyset$.

Corollary 5.5 (Maximal Subgroup Theorem)**.** *Let $a \in S$. Then (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii) $\Rightarrow$ (iv).*

(i) *a lies in a subgroup,*
(ii) *$a\mathcal{H}e$, some $e \in E(S)$,*
(iii) *$\mathcal{H}_a$ is a subgroup,*
(iv) *$a\mathcal{H}a^2$.*

Proof. (i) $\Rightarrow$ (ii) $a \in G \Rightarrow G \subseteq \mathcal{H}_e$ where $e^2 = e$ is the identity for G. Therefore $a \in \mathcal{H}_e$ so $a\mathcal{H}e$.

(ii) $\Rightarrow$ (iii) $a\mathcal{H}e \Rightarrow \mathcal{H}_a = \mathcal{H}_e$ and by MST $\mathcal{H}_e$ is a subgroup.

(iii) $\Rightarrow$ (i) $a \in \mathcal{H}_a$.

(iii) $\Rightarrow$ (iv) If $\mathcal{H}_a$ is a subgroup, then certainly $\mathcal{H}_a$ is closed. Hence $a, a^2 \in \mathcal{H}_a$ therefore $a\mathcal{H}a^2$. □

Theorem 5.2 (Green's Theorem)**.** *$a \in S$, then a lies in a subgroup iff $a\mathcal{H}a^2$.*

Proof. see later. □

Subgroups of $\mathcal{T}_n$

We use Green's Theorem to show the following

Claim. α lies in a subgroup of $\mathcal{T}_n \Leftrightarrow$ the map diagram has no tails of length $\geqslant 2$.

Proof. α lies in a subgroup $\Leftrightarrow \alpha\mathcal{H}\alpha^2 \Leftrightarrow \alpha\mathcal{L}\alpha^2$, $\alpha\mathcal{R}\alpha^2 \Leftrightarrow \operatorname{Im}\alpha = \operatorname{Im}\alpha^2$, $\operatorname{Ker}\alpha = \operatorname{Ker}\alpha^2$. We know $\operatorname{Im}\alpha^2 \subseteq \operatorname{Im}\alpha$ (as $\mathcal{T}_n\alpha^2 \subseteq \mathcal{T}_n\alpha$). Let ρ be an equivalence on a set X. Put

$$\frac{X}{\rho} = \{[x] \mid x \in X\}$$

for $X = \{1, 2, \ldots, n\} = \underline{n}$ and $\alpha \in \mathcal{T}_n$

$$|\underline{n}/\operatorname{Ker}\alpha| = |\operatorname{Im}\alpha|.$$

Claim (Mini Claimette). For $\alpha \in \mathcal{T}_n$, $\operatorname{Im}\alpha = \operatorname{Im}\alpha^2 \Rightarrow \operatorname{Ker}\alpha = \operatorname{Ker}\alpha^2$.

Proof. $\operatorname{Ker}\alpha \subseteq \operatorname{Ker}\alpha^2$ ($\alpha\mathcal{T}_n \subseteq \alpha\mathcal{T}_n$) so,

$$x \operatorname{Ker}\alpha y \Leftrightarrow (x, y) \in \operatorname{Ker}\alpha \Rightarrow (x, y) \in \operatorname{Ker}\alpha^2$$

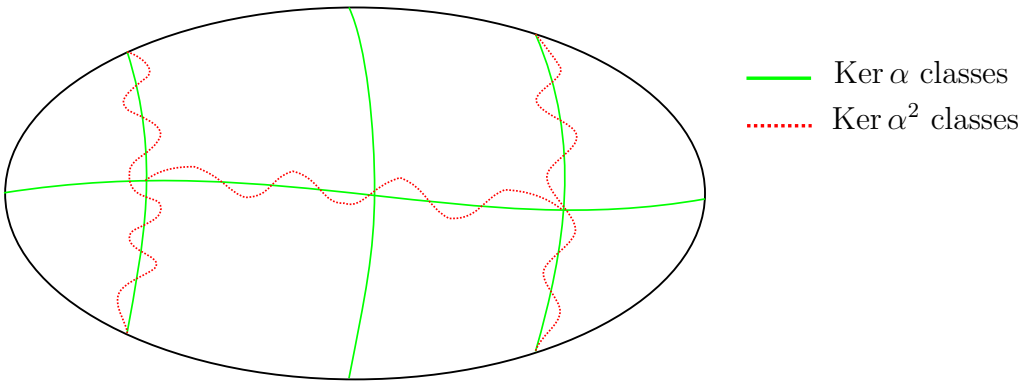


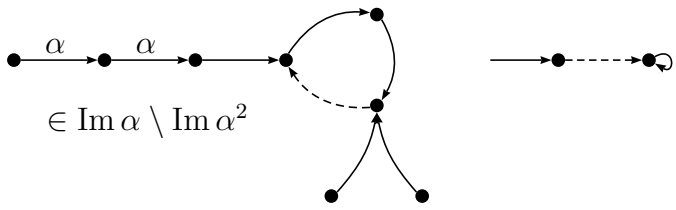
FIGURE 4. The classes of $\operatorname{Ker}\alpha$ and $\operatorname{Ker}\alpha^2$.

Suppose $\operatorname{Im}\alpha = \operatorname{Im}\alpha^2$. If $\operatorname{Ker}\alpha \subset \operatorname{Ker}\alpha^2$ then there exists $(u, v) \in \operatorname{Ker}\alpha^2 \setminus \operatorname{Ker}\alpha$. Then

$$|\operatorname{Im}\alpha^2| = \left|\frac{n}{\operatorname{Ker}\alpha^2}\right| < \left|\frac{n}{\operatorname{Ker}\alpha}\right| = |\operatorname{Im}\alpha|$$

a contradiction. Hence $\operatorname{Ker}\alpha = \operatorname{Ker}\alpha^2$. □

Hence: α lies in a subgroup $\Leftrightarrow \operatorname{Im}\alpha = \operatorname{Im}\alpha^2$. An arbitrary element of $\mathcal{T}_n$



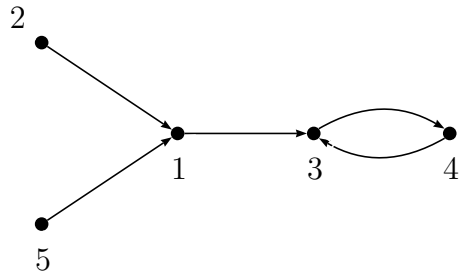
So, $\operatorname{Im}\alpha = \operatorname{Im}\alpha^2 \Leftrightarrow \nexists$ tails of length $\geqslant 2$. □

EXAMPLE 5.12.

(1) We take an element of $\mathcal{T}_5$ to be

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 3 & 1 \end{pmatrix} \in \mathcal{T}_5.$$

This has map diagram

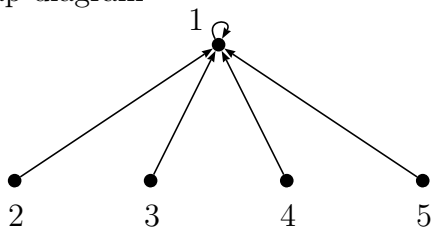


Now α has no tails with length $\geqslant 2$ and therefore α doesn't lie in any subgroup.

(2) Let us take the constant element $c_1 \in \mathcal{T}_5$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} = c_1.$$

This has the following map diagram



Now α has no tails of length $\geqslant 2$, therefore α lies in a subgroup and hence α lies in $\mathcal{H}_\alpha$. Note $\alpha^2 = \alpha$.

Now for any β

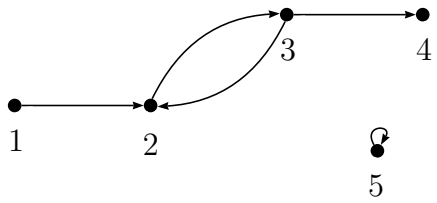
$$\begin{aligned} \beta \in \mathcal{H}_\alpha &\Leftrightarrow \beta \mathcal{H} \alpha, \\ &\Leftrightarrow \beta \mathcal{R} \alpha \text{ and } \beta \mathcal{L} \alpha, \\ &\Leftrightarrow \operatorname{Ker} \beta = \operatorname{Ker} \alpha \text{ and } \operatorname{Im} \beta = \operatorname{Im} \alpha, \\ &\Leftrightarrow \operatorname{Ker} \beta \text{ has classes } \{1,2,3,4,5\} \text{ and } \operatorname{Im} \beta = \{1\}, \\ &\Leftrightarrow \beta = \alpha. \end{aligned}$$

Therefore the maximal subgroup containing α is $\mathcal{H}_\alpha = \{\alpha\}$.

(3) Take the element

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 3 & 3 & 5 \end{pmatrix}.$$

This has map diagram



No tails of length $\geqslant 2$. Therefore α lies in a subgroup. Hence α lies in a maximal subgroup. Hence the maximal subgroup containing α is $\mathcal{H}_\alpha$. For any β

$$\begin{aligned} \beta \in \mathcal{H}_\alpha &\Leftrightarrow \beta \mathcal{H} \alpha, \\ &\Leftrightarrow \beta \mathcal{R} \alpha \text{ and } \beta \mathcal{L} \alpha, \\ &\Leftrightarrow \operatorname{Ker} \beta = \operatorname{Ker} \alpha \text{ and } \operatorname{Im} \beta = \operatorname{Im} \alpha, \\ &\Leftrightarrow \operatorname{Im} \beta = \{2,3,5\} \text{ and } \operatorname{Ker} \beta \text{ has classes } \{1,3\},\{2,4\},\{5\}. \end{aligned}$$

We now figure out what the elements of $\mathcal{H}_\alpha$. We start with the idempotent. We know that the image of the idempotent is $\{2,3,5\}$ and that idempotents are identities on their images. Thus we must have

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & 2 & 3 & & 5 \end{pmatrix}.$$

We also know that 1 and 3 go to the same place and 2 and 4 go to the same place. Thus we must have

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 3 & 2 & 5 \end{pmatrix}.$$

We now have what the idempotent is and then the other elements of $\mathcal{H}_\alpha$ are:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 2 & 3 & 5 \end{pmatrix} = \sigma_5$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 5 & 2 & 3 \end{pmatrix} \qquad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 3 & 5 & 2 \end{pmatrix}$$

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 5 & 3 & 2 \end{pmatrix} \qquad \rho^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 2 & 5 & 3 \end{pmatrix}$$

.

These are all 6 elements because there are 3 options for the image

$$\binom{3}{2}\binom{2}{2} = 6.$$

Check $\mathcal{H}_\alpha \simeq \mathrm{S}_3$.

5.5. $\mathcal{D}$ and $\mathcal{J}$

Recall $S^1aS^1 = \{xay \mid x, y \in S^1\}$.

Definition: We say that a is $\mathcal{J}$ related to b if and only if

$$\begin{aligned} a\mathcal{J}b &\Leftrightarrow S^1aS^1 = S^1bS^1 \\ &\Leftrightarrow \exists\, s,t,u,v \in S^1 \text{ with } a = sbt \quad b = uav \end{aligned}$$

Note. If $a\mathcal{L}b$, then $S^1a = S^1b$ so

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

and so $a\mathcal{J}b$, i.e. $\mathcal{L} \subseteq \mathcal{J}$, dually $\mathcal{R} \subseteq \mathcal{J}$.

Recall: S is *simple* if S is the only ideal of S. If S is simple and $a, b \in S$ then

$$S^1aS^1 = S = S^1bS^1 \qquad \text{so } a\mathcal{J}b$$

and $\mathcal{J} = \omega$ (the universal relation). Conversely if $\mathcal{J} = \omega$ and $InormS$, then pick any $a \in I$ and any $s \in S$. We have

$$s \in S^1sS^1 = S^1aS^1 \subseteq I.$$

Therefore $I = S$ and S is simple. Thus we have that S is simple $\Leftrightarrow \mathcal{J} = \omega$.

Similarly if S has a zero, then $\{0\}$ and $S \setminus \{0\}$ are the only $\mathcal{J}$-classes iff $\{0\}$ and S are the only ideals.

5.6. Composition of Relations

Definition: If ρ, λ are relations on A we define

$$\rho \circ \lambda = \big\{(x,y) \in A \times A \mid \exists\, z \in A \text{ with } (x,z) \in \rho \text{ and } (z,y) \in \lambda\big\}.$$

Claim. If ρ, λ are equivalence relations and if $\rho \circ \lambda = \lambda \circ \rho$ then $\rho \circ \lambda$ is an equivalence relation. Also, it's the smallest equivalence relation containing $\rho \cup \lambda$.

Proof. Put $\nu = \rho \circ \lambda = \lambda \circ \rho$

- for any $a \in A$, $a\rho a\lambda a$ so $a\nu a$ and ν is reflexive.
- Symmetric - an exercise.

- Suppose that $a\nu b\nu c$ then there exists $x, y \in A$ with

$$a\rho x\lambda b\lambda y\rho c.$$

From $x\lambda b\lambda y$ we have $x\lambda y$, so

$$a\rho x\lambda y\rho c.$$

Therefore $x\nu c$ hence there exists $z \in A$ such that $a\rho x\rho z\lambda c$, therefore $a\rho z\lambda c$ and hence $a\nu c$. Therefore ν is transitive.

We have shown that ν is an equivalence relation. If $(a, b) \in \rho$ then $a\rho b\lambda b$ so $(a, b) \in \nu$. Similarly if $(a, b) \in \lambda$ then $a\rho a\lambda b$ so $(a, b) \in \nu$. Hence $\rho \cup \lambda \subseteq \nu$.

Now, suppose $\rho \cup \lambda \subseteq \tau$ where τ is an equivalence relation. Let $(a, b) \in \nu$. Then we have $a\rho c\lambda b$ for some c. Hence $a\tau c\tau b$ so $a\tau b$ as τ is transitive. Therefore $\nu \subseteq \tau$. □

Definition: $\mathcal{D} = \mathcal{R} \circ \mathcal{L}$, i.e. $a\mathcal{D}b \Leftrightarrow \exists\, c \in S$ with $a\mathcal{R}c\mathcal{L}b$.

Lemma 5.4 (The $\mathcal{D}$ Lemma)**.** $\mathcal{R} \circ \mathcal{L} = \mathcal{L} \circ \mathcal{R}$

Proof. We prove $\Rightarrow$, the proof of $\Leftarrow$ being dual. Suppose that $a\mathcal{R} \circ \mathcal{L}b$. Then there exists $c \in S$ with

$$a\mathcal{R}c\mathcal{L}b$$

There exists $u, v, s, t \in S^1$ with

$$\underset{(1)}{a = cu} \qquad \underset{(2)}{c = av} \qquad \underset{(3)}{c = sb} \qquad \underset{(4)}{b = tc}.$$

Put $d = bu$ then we have

$$\underset{(1)}{a = cu} \underset{(3)}{= sbu} = sd,$$
$$\underset{(4)}{d = bu} \underset{(1)}{= tcu} = ta.$$

Therefore $a\mathcal{L}d$. Also

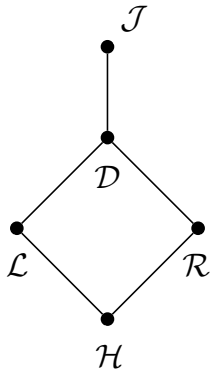
$$\underset{(4)}{b = tc} \underset{(2)}{= tav} \underset{(1)}{= tcuv} \underset{(4)}{= buv} = dv.$$

Therefore $b\mathcal{R}d$ and hence $a(\mathcal{L} \circ \mathcal{R})b$. □

Hence $\mathcal{D}$ is an equivalence relation – $\mathcal{D} = \mathcal{L} \vee \mathcal{R}$. Now by definition

$$\mathcal{H} = \mathcal{L} \cap \mathcal{R} \subseteq \mathcal{L} \subseteq \mathcal{D},$$
$$\mathcal{H} = \mathcal{L} \cap \mathcal{R} \subseteq \mathcal{R} \subseteq \mathcal{D}.$$

As $\mathcal{J}$ is an equivalence relation and $\mathcal{L} \cup \mathcal{R} \subseteq \mathcal{J}$ we must have $\mathcal{D} \subseteq \mathcal{J}$. This has Hasse Diagram



NOTATION: D_a is the $\mathcal{D}$ class of $a \in S$ and J_a is the $\mathcal{J}$-class of $a \in S$.

Note. $H_a \subseteq L_a \subseteq D_a \subseteq J_a$ and also $H_a \subseteq R_a \subseteq D_a \subseteq J_a$.

Egg-Box Pictures

Let D be a $\mathcal{D}$-class. Let $a \in D$ then $D = D_a$. Consider $R_u \cap L_v$. Since $u\mathcal{D}v$ there exists $h \in S$ with $u\mathcal{R}h\mathcal{L}v$. **No cell is empty**. Moreover

$$R_u \cap L_v = R_h \cap L_h = H_h.$$

Every class is a $\mathcal{H}$-class. As $\mathcal{D}$ is an equivalence, S is the union of such "egg-boxes".

5.7. Structure of $\mathcal{D}$-classes

Let S be a semigroup, $s \in S^1$. We define $\rho_s : S \to S$ by $a\rho_s = as$ for all $a \in S$

Lemma 5.5 (Green's Lemma)**.** *Let $a, b \in S$ be such that $a\mathcal{R}b$ and let $s, s' \in S$ be such that*

$$as = b \qquad \text{and} \qquad bs' = a.$$

Then $\rho_s : L_a \to L_b$ and $\rho_{s'} : L_b \to L_a$ are mutually inverse, $\mathcal{R}$-class preserving bijections (i.e. if $c \in L_a$, then $c\mathcal{R}c\rho_s$ and if $s \in L_b$ then $d\mathcal{R}d\rho_s$)

Proof. If $c \in L_a$ then

$$c\rho_s = cs\mathcal{L}as = b$$

because $\mathcal{L}$ is a right congruence. So $c\rho_s\mathcal{L}b$ therefore $\rho_s : L_a \to L_b$. Dually $\rho_{s'} : L_b \to L_a$.

Let $c \in K_a$. Then $c = ta$ for some $t \in S$. Now

$$c\rho_s\rho_{s'} = tas\rho_{s'} = tass' = tbs' = ta = c.$$

So $\rho_s\rho_{s'} = I_{L_a}$, dually, $\rho_{s'}\rho_s = I_{L_b}$.

Again, let $c \in L_a$. Then

$$cs = c \cdot s,$$
$$c = cs \cdot s'.$$

Therefore $c\mathcal{R}cs = c\rho_s$. □

Lemma 5.6 (Continuing Green's Lemma)**.** *For any $c \in L_a$ we have $\rho_s : H_c \to H_{cs}$ is a bijection with inverse $\rho_{s'} : H_{cs} \to H_c$. In particular – put $c = a$ then*

$$\rho_s : H_a \to H_b \qquad \text{and} \qquad \rho_s : H_b \to H_a$$

are mutually inverse bijections. For any $s \in S^1$, $\lambda_s : S \to S$ is given by $a\lambda_s = sa$.

Lemma 5.7 (Dual of Green's Lemma)**.** *Let $a, b \in S$ be such that $a\mathcal{L}b$ and let $t, t' \in S$ be such that $ta = b$ and $t'b = a$. Then $\lambda_t : R_a \to R_b$, $\lambda_{t'} : R_b \to R_a$ are mutually inverse $\mathcal{L}$-class preserving bijections. In particular, for any $c \in R_a$ we have $\lambda_t : H_c \to H_{tc}$, $\lambda_{t'} : H_{tc} \to H_c$ are mutually inverse bijections. So, if $c = a$ we have $\lambda_t : H_a \to H_b$, $\lambda_{t'} : H_b \to H_a$ are mutually inverse bijections.*

Corollary 5.6. *If $a\mathcal{D}h$ then there exists a bijection $H_a \to H_b$*

Proof. If $a\mathcal{D}b$ then there exists $h \in S$ with $a\mathcal{R}h\mathcal{L}b$. There exists a bijection $H_a \to H_h$ by Green's Lemma and we also have that there exists a bijection $H_h \to H_b$ by the Dual of Green's Lemma. Therefore there exists a bijection $H_a \to H_b$. □

Thus any two $\mathcal{H}$-classes in the same $\mathcal{D}$-class have the same cardinality.

Theorem 5.3 (Green's Theorem – Strong Version)**.** *Let H be an $\mathcal{H}$-class of a semigroup S. Then either $H^2 \cap H = \emptyset$ or H is a subgroup of S.*

Proof. Suppose $H^2 \cap H \neq \emptyset$ then there exists $a, b, c \in H$ with $ab = c$. Since $a\mathcal{R}c$, $\rho_b : H_a \to H_c$ is a bijection. But $H_a = H_c = H$ so $\rho_b : H \to H$ is a bijection. Hence $Hb = H$. Dually, $aH = H$.

Since $b \in H$, $b = db$ for some $d \in H$. As $b\mathcal{R}d$, $d = bs$ for some $s \in S^1$ and then $bs = dbs \Rightarrow d = d^2$. Hence H contains an idempotent (so by the Maximal Subgroup Theorem, it's a subgroup).

We have d is an identity for H. Let $h, k \in H$. Then $h\mathcal{L}d$ so

$$hd = h \Rightarrow \lambda_h : H \to H$$

is a bijection. Hence $k\lambda_h = hk \in H$. So H is closed. Let $a \in H$, then $a^2 \in H$, hence $aH = H = Ha$. So, there exists $a', a'' \in H$ with

$$d = aa' = a''a$$

and we have

$$a'' = a''d = a''(aa') = (a''a)a' = da' = a'.$$ □

Corollary 5.7.

(i) $a\mathcal{H}a^2 \Leftrightarrow H_a$ *is a subgroup,*
(ii) $e \in E(S) \Rightarrow H_e$ *is a subgroup.*

Proof.

(i) We know H_a is a subgroup $\Rightarrow a, a^2 \in H_a$ so $a\mathcal{H}a^2$. If $a\mathcal{H}a^2$, then $a^2 \in H_a \cap (H_a)^2$. Hence $H_a \cap (H_a)^2 \neq \emptyset$. So, by Green H_a is a subgroup. □

6. Rees Matrix Semigroups

Construction: Let G be a group, I, Λ be non-empty sets and $P = (p_{\lambda i})$ a matrix. P is a $\Lambda \times I$ matrix over $G \cup \{0\}$ such that every row / column of P contains at least one non-zero entry.

Definition: $m^0 = m^0(G; I, \Lambda; P)$ is the set

$$I \times G \times \Lambda \cup \{0\}$$

with binary operation given by $0n = 0 = n0$ for all $n \in m^0$ and

$$(i, a, \lambda)(k, b, \mu) = \begin{cases} 0 & \text{if } p_{\lambda k} = 0, \\ (i, ap_{\lambda k}b, \mu) & \text{if } p_{\lambda k} \neq 0. \end{cases}$$

Then m^0 is a semigroup with zero 0 – a Rees Matrix Semigroup over G.

Definition: $a \in S$ is *regular* if there exists $x \in S$ with

$$a = axa.$$

S is *regular* if every $a \in S$ is regular.

If S is regular then $a\mathcal{R}b \Leftrightarrow aS = bS \Leftrightarrow$ there exists $s, t \in S$ with $a = bs$ and $b = at$, etc.

6.1. Rees Matrix Facts

Let $m^0 = m^0(G; I, \Lambda; P)$ be a Rees Matrix Semigroup over a group G. Then

(1) (i, a, λ) is idempotent $\Leftrightarrow p_{\lambda i} \neq 0$ and $p_{\lambda i} = a^{-1}$.
(2) m^0 is regular.
(3) $(i, a, \lambda)\mathcal{R}(j, b, \mu) \Leftrightarrow i = j$.
(4) $(i, a, \lambda)\mathcal{L}(j, b, \mu) \Leftrightarrow \lambda = \mu$.
(5) $(i, a, \lambda)\mathcal{H}(j, b, \mu) \Leftrightarrow i = j$ and $\lambda = \mu$.
(6) The $\mathcal{D} = \mathcal{J}$-classes are $\{0\}$ and $m^0 \setminus \{0\}$ (so 0 and m^0 are the only ideals).
(7) m^0 is 0-simple.
(8) The rectangular property;

$$\left.\begin{array}{l} xy\mathcal{D}x \Leftrightarrow xy\mathcal{R}x \\ xy\mathcal{D}y \Leftrightarrow xy\mathcal{L}y \end{array}\right\} \forall\, x, y \in m^0$$

(9) Put $H_{i\lambda} = \{(i, a, \lambda) \mid a \in G\}$ by (5) we have $H_{i\lambda}$ is an $\mathcal{H}$-class ($H_{i\lambda} = H_{(i,e,\lambda)}$). If $\rho_{\lambda i} \neq 0$ we know $(i, \rho_{\lambda i}^{-1}, \lambda)$ is an idempotent $\Rightarrow H_{i\lambda}$ is a group, by the Maximal Subgroup Theorem. The identity is $(i\rho_{\lambda i}^{-1}, \lambda)$ and $(i, a, \lambda)^{-1} = (i, \rho_{\lambda i}^{-1} a^{-1}, \rho_{\lambda i}^{-1}, \lambda)$.

(10) If $\rho_{\lambda i} \neq 0$ and $\rho_{\mu j} \neq 0$ then (exercise) $H_{i\lambda} \simeq H_{j\mu}$ (the bijection is $(i, a, \lambda) \mapsto (j, a, \mu)$). The homomorphism is a bit more sophisticated.

Proof.

(1) We have that

$$\begin{aligned}(i, a, \lambda) \in E(m^0) &\Leftrightarrow (i, a, \lambda) = (i, a, \lambda)(i, a, \lambda),\\ &\Leftrightarrow (i, a, \lambda) = (i, ap_{\lambda i}a, \lambda),\\ &\Leftrightarrow a = ap_{\lambda i}a,\\ &\Leftrightarrow p_{\lambda i} \neq 0 \text{ and } p_{\lambda i} = a^{-1}.\end{aligned}$$

(2) $0 = 000$ so 0 is regular. Let $(i, a, \lambda) \in m^0 \setminus \{0\}$ then there exists $j \in I$ with $p_{\lambda j} \neq 0$ and there exists $\mu \in \Lambda$ with $p_{\mu i} \neq 0$. Now,

$$(i, a, \lambda)(j, p_{\lambda j}^{-1} a^{-1} p_{\mu i}^{-1}, \mu)(i, a, \lambda) = (i, a, \lambda)$$

and hence m^0 is regular.

(3) $\{0\}$ is an $\mathcal{R}$-class. If $(i, a, \lambda)\mathcal{R}(j, b, \mu)$ then there exists $(k, c, \nu) \in m^0$ with

$$(i, a, \lambda) = (j, b, \mu)(k, c, \nu) = (j, bp_{\mu k}c, \nu)$$

and so $i = j$. Conversely, if $i = j$, pick k with $p_{\mu k} \neq 0$. Then

$$(i, a, \lambda) = (j, b, \mu)(k, p_{\mu k}^{-1} b^{-1} a, \lambda)$$

and consequently $(i, a, \lambda)\mathcal{R}(j, b, \mu)$

(4) Dual.

(5) This comes from (3) and (4) above.

(6) $\{0\}$ is a $\mathcal{D}$-class and a $\mathcal{J}$-class. If $(i, a, \lambda), (j, b, \mu) \in m^0$ then

$$(i, a, \lambda)\mathcal{R}(i, a, \mu)\mathcal{L}(j, b, \mu)$$

so $(i, a, \lambda)\mathcal{D}(j, b, \mu)$ and so $(i, a, \lambda)\mathcal{J}(j, b, \mu)$. Therefore $\mathcal{D} = \mathcal{J}$ and $\{0\}$ and $m^0 \setminus \{0\}$ are the only classes.

(7) Let $i \in I$, then there exists $\lambda \in \Lambda$ with $p_{\lambda i} \neq 0$ so $(i, 1, \lambda)^2 \neq 0$. Therefore $(m^0)^2 \neq 0$ and so m^0 is 0-simple.

(8) The 2 $\mathcal{D}$-classes are zero and everything else. If $xy = x = 0$ then $xy\mathcal{D}x$ and $xy\mathcal{R}x$ always. If $xy\mathcal{R}x$ then $xy\mathcal{D}x$ as $\mathcal{R} \subseteq \mathcal{D}$. Suppose $xy\mathcal{D}$ and $xy, x \neq 0$. Then $y \neq 0$, so

$$x = (i, a, \lambda) \qquad y = (j, b, \mu)$$

say. Then as $xy = (i, a\rho_{\lambda j}b, \mu)$ so $xy\mathcal{R}x$. The result for $\mathcal{L}$ is dual. □

A finitary property is a property that captures finite nature.

Chain conditions

Definition: S a semigroup has M_L if there are no infinite chains

$$S^1a_1 \supset S^1a_2 \supset S^1a_3 \supset \dots$$

if principal left ideals. M_L is the *descending chain condition* (d.c.c.) on principal left ideals. Note that M_R is the dual of this.

Claim (The Chain Claim). S has $M_{\mathcal{L}}$ if and only if any chain

$$S^1a_1 \supseteq S^1a_2 \supseteq \dots$$

terminates stabilizes with

$$S^1a_n = S^1a_{n+1} = \dots$$

Proof. If every chain with $\supseteq$ terminates, then clearly we cannot have an ∞ strict chain

$$S^1a_1 \supset S^1a_2 \supset \dots$$

So S has M_L. Conversely; suppose S has M_L and we have a chain

$$S^1a_1 \supseteq S^1a_2 \supseteq \dots$$

The strict inclusions are at the j_ith steps

$$S^1a_1 = S^1a_2 = \dots = S^1a_{j_1} \supset S^1a_{j_1+1} = S^1a_{j_1+2} = \dots = S^1a_{j_2} \supset S^1a_{j_2+1} = \dots$$

Then $S^1a_{j_1} \supset S^1a_{j_2} \supset \dots$. As S has M_L, this chain is finite with length n say. Then

$$S^1a_{j_n+1} = S^1a_{j_n+2} = \dots$$

and our sequence has stabilised. □

Definition: The *ascending chain condition* (a.c.c.) on principal ideals on left / right ideals M^L (M^R) is defined as above but with the inclusions reversed. The analogue of the chain claim holds.

Example 6.1. Every finite semigroup has M_L, M_R, M^L, M^R. A chain

$$S^1a_1 \supset S^1a_2$$

is in particular, a chain of distinct subsets of S – but a finite semigroup S has at most $2^{|s|}$ subsets.

EXAMPLE 6.2. The Bicyclic semigroup B has M^L & M^R. We know $B(x,y) = \{(p,q) \mid q \geqslant y\}$ and so $B(x,y) \subseteq B(u,v) \Leftrightarrow y \geqslant v$, inclusion is strict if and only if $y > v$. If we had an ∞ chain

$$B(x_1,y_1) \subset B(x_2,y_2) \subset B(x_3,y_3) \subset \dots$$

then we would have

$$y_1 > y_2 > y_3 > \dots$$

hence M^L holds, dually M^R holds. However, since $0 < 1 < 2 < \dots$ we have

$$B(0,0) \supset B(1,1) \supset B(2,2) \supset \dots$$

so there exists ∞ descending chains. Hence B doesn't have M_L or M_R.

EXAMPLE 6.3. Let $m^0 = m^0(G;I;\Lambda;P)$ be a Rees Matrix Semigroup over a group G. Then m^0 has M_L, M_R, M^L and M^R.

Proof. We show that the length of the strict chains is at most 2. Suppose $\alpha m^0 \subseteq \beta m^0$. We could have $\alpha = 0$. If $\alpha \neq 0$ then $\alpha m^0 \neq \{0\}$ so $\beta \neq 0$ and we have $\alpha = (i,g,\lambda)$, $\beta = (j,h,\mu)$ and $\alpha = \beta\gamma$ for some $\gamma = (\ell,k,\nu)$ so that

$$(i,g,\lambda) = (j,h,\mu)(\ell,k,\nu) = (j,h\rho_{\mu\ell}k,\nu)$$

$\Rightarrow i = j$ and so $\alpha\mathcal{R}\beta$ and $\alpha m^0 = \beta m^0$. So we have $0m^0 \subset \alpha m^0$ for all non-zero α. But $\alpha \neq 0$, $\alpha m^0 \subseteq \beta m^0 \Rightarrow \alpha m^0 = \beta m^0$. Hence m^0 has M_R and M^R; dually m^0 has M_L and M^L. □

Definition: A 0-simple semigroup is *completely 0-simple* if it has M_R and M_L.

By above, any Rees Matrix Semigroup over a group is completely 0-simple. Our aim is to show that every completely 0-simple semigroup is isomorphic to a Rees Matrix Semigroup over a group.

Theorem 6.1 (The $\mathcal{D} = \mathcal{J}$ Theorem)**.** *Suppose*

$$(\star) \qquad \begin{cases} \forall\, a \in S,\, \exists\, n \in \mathbb{N} \text{ with } a^n \mathcal{L} a^{n+1}, \\ \forall\, a \in S,\, \exists\, m \in \mathbb{N} \text{ with } a^m \mathcal{R} a^{m+1}. \end{cases}$$

Then $\mathcal{D} = \mathcal{J}$.

EXAMPLE 6.4.

(1) If S is a band, $a = a^2$ for all $a \in S$ and so $(\star)$ holds.

Proof. We know $\mathcal{D} \subseteq \mathcal{J}$. Let $a, b \in S$ with $a\mathcal{J}b$. Then there exists $x, y, u, v \in S^1$ with

$$b = xay \qquad a = ubv.$$

Then

$$b = xay = (xu)b(vy) = (xu)(xubvy)(vy) = (xu)^2b(vy)^2 = \cdots = (xu)^nb(vy)^n$$

for all $n \in \mathbb{N}$. By $(\star)$ there exists n with $(xu)^n\mathcal{L}(xu)^{n+1}$. Therefore

$$b = (xu)^nb(vy)^n\mathcal{L}(xu)^{n+1}b(vy)^n = xu\big((xu)^nb(vy)^n\big) = xub.$$

Therefore $b\mathcal{L}xub$, so

$$S^1b = S^1xub \subseteq S^1ub \subseteq S^1b.$$

So $S^1b = S^1ub$ and $b\mathcal{L}ub$. Dually, $b\mathcal{R}bv$. Therefore $a = ubv\mathcal{R}ub\mathcal{L}b$. So $a\mathcal{D}b$ and $\mathcal{J} \subseteq \mathcal{D}$. Consequently, $\mathcal{D} = \mathcal{J}$. □

The Rectangular Property: Let S satisfy $(\star)$. Then for all $a, b \in S$ we have

(i) $a\mathcal{J}ab \Leftrightarrow a\mathcal{D}ab \Leftrightarrow a\mathcal{R}ab$,
(ii) $b\mathcal{J}ab \Leftrightarrow b\mathcal{D}ab \Leftrightarrow b\mathcal{L}ab$.

Proof. We prove (i), (ii) being dual. Now,

$$a\mathcal{J}ab \Leftrightarrow a\mathcal{D}ab$$

as $\mathcal{D} = \mathcal{J}$. Then $a\mathcal{R}ab \Rightarrow a\mathcal{D}ab$; as $\mathcal{R} \subseteq \mathcal{D}$. If $a\mathcal{J}ab$ then there exists $x, y \in S^1$ with

$$a = xaby = xa(by) = x^na(by)^n$$

for all n. Pick n with $(by)^n\mathcal{R}(by)^{n+1}$. Then

$$a = x^na(by)^n\mathcal{R}x^na(by)^{n+1} = x^na(by)^nby = aby$$

$\Rightarrow a\mathcal{R}aby$. Now $aS^1 = abyS^1 \subseteq abS^1 \subseteq aS^1$. Hence $aS^1 = abS^1$ and $a\mathcal{R}ab$. □

Lemma 6.1 (0-Simple Lemma)**.** *Let S have a 0 and $S^2 \neq 0$. Then the following are equal*

(i) *S is 0-simple,*
(ii) *$SaS = S$ for all $a \in S \setminus \{0\}$,*
(iii) *$S^1aS^1 = S$ for all $a \in S \setminus \{0\}$,*
(iv) *the $\mathcal{J}$-classes are $\{0\}$ and $S \setminus \{0\}$.*

Proof. (i) ⇔ (iv) is a standard exercise.

(ii) ⇒ (iii): Let $a \in S \setminus \{0\}$. Then

$$S = SaS \subseteq S^1aS^1 \subseteq S$$

and therefore $S = S^1aS^1$.

(iii) ⇒ (iv): We know $J_0 = \{0\}$. Let $a, b \in S \setminus \{0\}$. Then

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

and hence $a\mathcal{J}b$. Therefore $\{0\}$ and $S \setminus \{0\}$ are the only $\mathcal{J}$-classes.

(i) $\Rightarrow$ (ii): Since $S^2 \neq 0$ and S^2 is an ideal, then $S^2 = S$. Therefore

$$S^3 = SS^2 = S^2 = S \neq 0.$$

Let $I = \{x \in S \mid SxS = 0\}$. Clearly $0 \in I$ and hence $I \neq \emptyset$. If $x \in I$ and $s \in S$, then

$$0 \subseteq SxsS \subseteq SxS = 0.$$

Therefore $SxsS = 0$ and so $xs \in I$. Dually $sx \in I$; therefore I is an ideal. If $I = S$, then

$$\begin{aligned} S^3 &= SIS, \\ &= \bigcup_{x \in I} SxS, \\ &= 0. \end{aligned}$$

This is a contradiction, therefore $I \neq S$. Hence $I = 0$. Let $a \in S \setminus \{0\}$. Then SaS is an ideal and as $a \notin I$ we have $SaS \neq 0$. Hence $SaS = S$. □

Corollary 6.1. *Let S be completely 0-simple. Then S contains a non-zero idempotent.*

Proof. Let $a \in S \setminus \{0\}$. Then $SaS = S$, therefore there exists a $u, v \in S$ with $a = uav$. So,

$$a = uav = u^2av^2 = \cdots = u^nav^n$$

for all n. Hence $u^n \neq 0$ for all $n \in \mathbb{N}$. Pick n, m with $u^n \mathcal{R} u^{n+1}$, $u^m \mathcal{L} u^{m+1}$. Notice

$$u^{n+1} \mathcal{R} u^{n+2}$$

as $\mathcal{R}$ is a left congruence. Similarly,

$$u^{n+2} \mathcal{R} u^{n+3}$$

we deduce that $u^n \mathcal{R} u^{n+t}$ for all $t \geqslant 0$. Similarly $u^m \mathcal{L} u^{m+t}$ for all $t \geqslant 0$. Let $s = \max\{m, n\}$. Then $u^s \mathcal{R} u^{2s}$, $u^s \mathcal{L} u^{2s}$ so $u^s \mathcal{H} u^{2s} = (u^s)^2$. Hence u^s lies in a subgroup. Therefore $u^s \mathcal{H} e$ for some idempotent e. As $u^s \neq 0$ and $H_0 = \{0\}$, we have $e \neq 0$. □

Theorem 6.2 (Rees' Theorem - 1941)**.** *Let S be a semigroup with zero. Then S is completely 0-simple $\Leftrightarrow$ S is isomorphic to a Rees Matrix Semigroup over a group.*

Proof. If $S \cong m^0(G; I; \Lambda; P)$ where G is a group, we know m^0 is completely 0-simple (by Rees Matrix facts), hence S is completely 0-simple.

Conversely, suppose S is completely 0-simple. By the $\mathcal{D} = \mathcal{J}$ Theorem, $\mathcal{D} = \mathcal{J}$ (as S has M_R and M_L, it must have $(\star)$). As S is 0-simple, the $\mathcal{D} = \mathcal{J}$-classes are $\{0\}$ and $S \setminus \{0\}$. Let $D = S \setminus \{0\}$. By the Corollary to the 0-simple Lemma, D contains $e = e^2$.

Let $\{R_i \mid i \in I\}$ be the set of $\mathcal{R}$-classes in D (so I indexes the non-zero $\mathcal{R}$-classes). Let $\{L_\lambda \mid \lambda \in \Lambda\}$ be the set of $\mathcal{L}$-classes in D (so Λ index the non-zero $\mathcal{L}$-classes).

Denote the $\mathcal{H}$-class $R_i \cap L_\lambda$ by $H_{i\lambda}$. Since D contains an idempotent e, D contains the *subgroup* H_e (Maximum Subgroup Theorem or Green's Theorem). Without Loss of Generality assume $e \in H_{11}$. Put $G = H_{11}$, which is a group.

For each $\lambda \in \Lambda$ let $q_\lambda \in H_{1\lambda}$ (take $q_1 = e$). For each $i \in I$ let $r_i \in H_{i1}$ (take $r_1 = e$).

$$e = e^2, e\mathcal{R}q_\lambda \Rightarrow eq_\lambda = q_\lambda$$

By Green's Lemma,

$$\rho_{q_\lambda} : H_e = G \to H_{1\lambda}$$

is a bijection. Now, $e = e^2$, $e\mathcal{L}r_i$ so $r_i e = r_i$. By the dual of Green's Lemma

$$\lambda_{r_i} : H_{1\lambda} \to H_{i\lambda}$$

is a bijection. Therefore for any $i \in I$, $\lambda \in \Lambda$ we have

$$\rho_{q_\lambda}\lambda_{r_i} : G \to H_{i\lambda}$$

is a bijection.

Note. $a\rho_{q_\lambda}\lambda_{r_i} = r_i a q_\lambda$.

So, each element of $H_{i\lambda}$ has a unique expression as $r_i a q_\lambda$ where $a \in G$. Hence the mapping

$$\theta : (I \times G \times \Lambda) \cup \{0\} \to S$$

given by $0\theta = 0$, $(i, a, \lambda)\theta = r_i a q_\lambda$ is a bijection. Put $p_{\lambda i} = q_\lambda r_i$. If $p_{\lambda i} \neq 0$ then $q_\lambda r_i \mathcal{D} q_\lambda$. By the rectangular property $q_\lambda r_i \mathcal{R} q_\lambda \mathcal{R} e$. Also by the rectangular property, if $q_\lambda r_i \neq 0$ then as $q_\lambda r_i \mathcal{D} r_i$ we have

$$q_\lambda r_i \mathcal{L} r_i \mathcal{L} e.$$

Therefore $q_\lambda r_i = 0$ or $q_\lambda r_i \in G$. So, $P = (p_{\lambda i}) = (q_\lambda r_i)$ is a $\Lambda \times I$ matrix over $G \cup \{0\}$. For any $i \in I$, by the 0-simple Lemma we have $Sr_iS = S$. So, $ur_iv \neq 0$ for some $u, v \in S$. Say, $u = r_k b q_\lambda$ for some k, λ and b. Then

$$p_{\lambda i} = q_\lambda r_i \neq 0$$

as $r_k b q_\lambda r_i v \neq 0$. Therefore every element of P has a non-zero entry. Dually for rows. Therefore

$$m^0 = m^0(G; I; \Lambda; P)$$

is a Rees Matrix Semigroup over a group G. For any $x \in m^0$ ($x = 0$ or x a triple) then

$$(0x)\theta = 0\theta = 0 = 0(x\theta) = 0\theta x\theta.$$

Also, $(x0)\theta = x\theta 0\theta$. For (i, a, λ), $(k, b, \mu) \in m^0$ we have

$$\big((i,a,\lambda)(k,b,\mu)\big)\theta = \begin{cases} 0\theta & \text{if } p_{\lambda k} = 0, \\ (i, ap_{\lambda k}b, \mu)\theta & \text{if } p_{\lambda k} \neq 0, \end{cases}$$
$$= \begin{cases} 0 & \text{if } p_{\lambda k} = 0, \\ r_i a p_{\lambda k} b q_\mu & \text{if } p_{\lambda k} \neq 0, \end{cases}$$
$$= r_i a p_{\lambda k} b q_\mu,$$
$$= r_i a q_\lambda r_k b q_\mu,$$
$$= (i,a,\lambda)\theta(k,b,\mu)\theta.$$

Therefore θ is an isomorphism. □

7. Regular Semigroups

Definition: $a \in S$ is *regular* if $a = axa$ for some $x \in S$. S is *regular* if every $a \in S$ is regular.

Definition: $a' \in S$ is an *inverse* of a if $a = aa'a$ *and* $a' = a'aa'$. We denote $V(a)$ to be the set of inverses of a.

Caution: Inverses need not be unique. In a rectangular band $T = I \times \Lambda$ then

$$(i,j)(k,\ell)(i,j) = (i,j)$$
$$(k,\ell)(i,j)(k,\ell) = (k,\ell)$$

for any (i,j) and (k,ℓ). So every element is an inverse of every other element. If G is a group then $V(a) = \{a^{-1}\}$ for all $a \in G$.

Lemma 7.1 (Lemma R)**.** *a is regular $\Leftrightarrow V(a) \neq \emptyset$.*

Proof. If $V(a) \neq \emptyset$, clearly a is regular. Conversely suppose that a is regular. Then there exists $x \in S$ with $a = axa$. Put $a' = xax$. Then

$$aa'a = a(xax)a = (axa)xa = axa = a,$$
$$a'aa' = (xax)a(xax) = x(axa)(xax) = xa(xax) = x(axa)x = xax = a.$$

So $a' \in V(a)$. □

Note. If $a = axa$ then

$$(ax)^2 = (ax)(ax) = (axa)x = ax$$

so $ax \in E(S)$ and dually, $xa \in E(S)$. Moreover

$$a = axa \quad ax = ax \Rightarrow a\mathcal{R}ax,$$
$$a = axa \quad xa = xa \Rightarrow a\mathcal{L}xa.$$

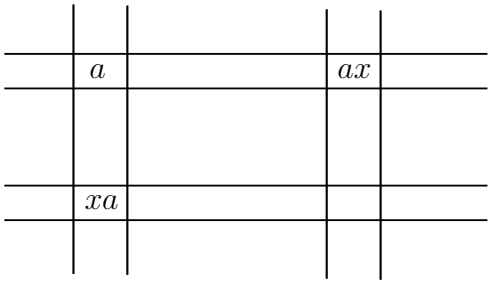


FIGURE 5. The egg box diagram of $E(S)$.

Definition: S is *inverse* if $|V(a)| = 1$ for all $a \in S$, i.e. every element has a unique inverse.

EXAMPLE 7.1.

(1) Groups are inverse; $V(a) = \{a^{-1}\}$,
(2) A rectangular band T is regular; but (as every element of T is an inverse of every other element) T is not inverse (unless T is trivial),
(3) If S is a band then S is regular as $e = e^3$ for all $e \in S$; S need not be inverse,
(4) B is regular because $(a, b) = (a, b)(b, a)(a, b)$ for all $(a, b) \in B$ then B is inverse – see later,
(5) m^0 is regular (see "Rees Matrix Facts"),
(6) $\mathcal{T}_X$ is regular (see Exercises),
(7) $(\mathbb{N}, +)$ is not regular as, for example $1 \neq 1 + a + 1$ for any $a \in \mathbb{N}$.

Theorem 7.1 (Inverse Semigroup Theorem)**.** *A semigroup S is inverse iff S is regular and $E(S)$ is a semilattice (i.e. $ef = fe$ for all $e, g \in E(S)$).*

Proof. ($\Leftarrow$) Let $a \in S$. As S is regular, a has an inverse by Lemma R. Suppose $x, y \in V(a)$. Then

$$a \underset{(1)}{=} axa \qquad x \underset{(2)}{=} xax \qquad a \underset{(3)}{=} aya \qquad y \underset{(4)}{=} yay,$$

so $ax, xa, ay, ya \in E(S)$. This gives us that

$$\begin{aligned} x &\underset{(2)}{=} xax \underset{(3)}{=} x(aya)x = (xa)(ya)x = (ya)(xa)x = y(axa)x \\ &\underset{(1)}{=} yax \underset{(3)}{=} y(aya)x = y(ay)(ax) = y(ax)(ay) = y(axa)y \underset{(1)}{=} yay \underset{(4)}{=} y. \end{aligned}$$

So $|V(a)| = 1$ and S is inverse. Conversely suppose S is inverse. Certainly S is regular. Let $e \in E(S)$. Then $e = e'$ as $e = eee$, $e = eee$. Let $x = (ef)'$. Consider fxe. Then

$$(fxe)^2 = (fxe)(fxe) = f(xefx)e = fxe$$

as $x = (ef)'$. So $(fxe) \in E(S)$ and therefore $fxe = (fxe)'$. We want to show that fxe and ef are mutually inverse, i.e.

$$ef(fxe)ef = ef^2xe^2f = efxef = ef,$$
$$(fxe)ef(fxe) = fxe^2f^2xe = fx(efx)e = fxe.$$

Therefore we have $ef = (fxe)' = fxe \in E(S)$. Therefore $E(S)$ is a band. Let $e, f \in E(S)$. Then

$$ef(fe)ef = ef^2e^2f = efef = ef,$$
$$fe(ef)fe = fe$$

similarly. Therefore we have $ef = (fe)' = fe$. □

Example 7.2.

(1) $E(B) = \{(a, a) \mid a \in \mathbb{N}^0\}$ because

$$(a, a)(b, b) = (t, t) = (b, b)(a, a)$$

where $t = \max\{a, b\}$. Therefore B is inverse and note $(a, b)' = (b, a.$

(2) $\mathcal{T}_X$ – we know $\mathcal{T}_X$ is regular. For $|X| \geqslant 2$ let $x, y \in X$ with $x \neq y$ we have $c_x, c_y \in E(\mathcal{T}_X)$. Then $c_xc_y \neq c_yc_x$ so $\mathcal{T}_X$ is not inverse.

(3) S a band – then S is regular. We have

$$\begin{aligned} S \text{ is inverse} &\Leftrightarrow ef = fe \text{ for all } e, f \in E(S), \\ &\Leftrightarrow ef = fe \text{ for all } e, f \in S, \\ &\Leftrightarrow S \text{ is a semilattice.} \end{aligned}$$

7.1. Green's Theory for Regular $\mathcal{D}$-classes

If $e \in E(S)$ then H_e is a subgroup of S (by the Maximal Subgroup Theorem or Green's Theorem). If $e\mathcal{D}f$ then $|H_e| = |H_f|$ (by the Corollary to Green's Lemmas). We will show that $H_e \cong H_f$.

Lemma 7.2. *We have that*

(i) *If $a = axa$ then $ax, xa \in E(S)$ and $a\mathcal{R}xa$,*
(ii) *If $b\mathcal{R}f \in E(S)$, then b is regular,*
(iii) *If $b\mathcal{L}f \in E(S)$, then b is regular.*

Proof.

(i) we know this.
(ii) If $b\mathcal{R}f$ then $fb = b$. Also, $f = bs$ for some $s \in S^1$. Therefore $b = fb = bsb$ and so b is regular.
(iii) this is dual to (ii).

□

Lemma 7.3 (Regular $\mathcal{D}$-class Lemma)**.** *If $a\mathcal{D}b$ then if a is regular, so is b.*

Proof. Let a be regular with $a\mathcal{D}b$. Then $a\mathcal{R}c\mathcal{L}b$ for some $c \in S$.

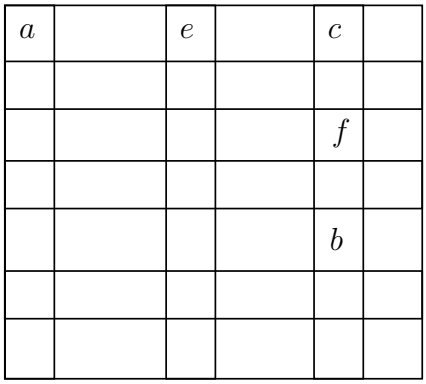
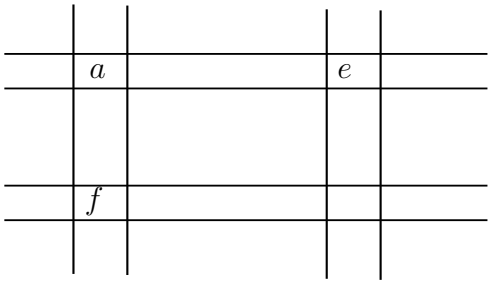


FIGURE 6. The egg box diagram of $\mathcal{D}$.

There exists $e = e^2$ with $e\mathcal{R}a\mathcal{R}c$ by (ii) above. By (ii), c is regular. By (i), $c\mathcal{L}f = f^2$. By (iii), b is regular. □

Corollary 7.1 (Corollary to Green's Lemmas)**.** *Let $e, f \in E(S)$ with $e\mathcal{D}f$. Then $H_e \cong H_f$.*

Proof. Suppose $e, f \in E(S)$ and $e\mathcal{D}f$. There exists $a \in S$ with $e\mathcal{R}a\mathcal{L}f$.



As $e\mathcal{R}a$ there exists $s \in S^1$ with $e = as$ and $ea = a$. So $a = asa$. Put $x = fse$. Then

$$ax = afse = ase = e^2 = e$$

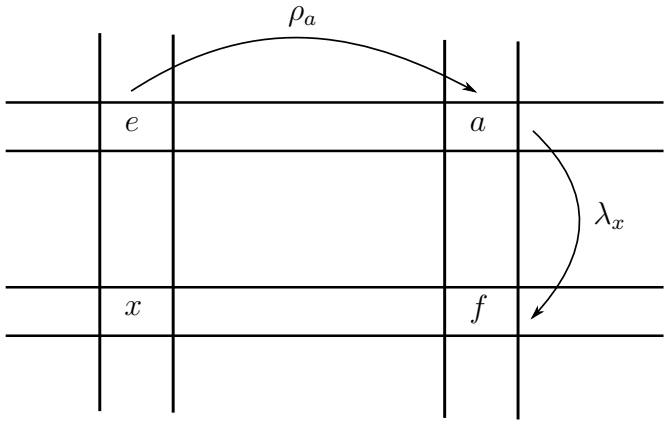
and so $a = ea = axa$. Since $a\mathcal{L}f$ there exists $t \in S^1$ with $ta = f$. Then

$$xa = fsea = fsa = tasa = ta = f.$$

Also

$$xax = fx = ffse = fse = x.$$

So we have the diagram



$$e = ax \qquad a = axa \qquad x = xax \qquad f = xa$$

We have $ea = a$ therefore $\rho_a : H_e \to H_a$ is a bijection. From $a\mathcal{L}f$ and $xa = f$ we have $\lambda_x : H_a \to H_f$ is a bijection. Hence $\rho_a\lambda_x : H_e \to H_f$ is a bijection. Let $h, j \in H_e$. Then

$$h(\rho_a\lambda_x)k(\rho_a\lambda_x) = (xha)(xka) = xh(ax)ka = xheka = xhka = hk(\rho_a\lambda_x).$$

So, $\rho_a\lambda_x$ is an isomorphism and $H_e \cong H_f$. □

Example 7.3.

(1) $m^0 = m^0(G; I; \Lambda; P)$ then $m^0 \setminus \{0\}$ is a $\mathcal{D}$-class. We have $H_{i\lambda} = \big\{(i, g, \lambda) \mid g \in G\big\}$. If $p_{\lambda i} \neq 0$, $H_{i\lambda}$ is a group $\mathcal{H}$-class. If $p_{\lambda i}, p_{\mu j} \neq 0$ then $H_{i\lambda} \cong H_{j\mu}$ (seen directly).
(2) B (the Bicyclic Monoid). B is bisimple. $E(B) = \big\{(a, a) \mid a \in \mathbb{N}^0\big\}$. Then $H_{(a,a)} = \big\{(a, a)\big\}$. Clearly $H_{(a,a)} \cong H_{(b,b)}$.
(3) In $\mathcal{T}_n$, then $\alpha\mathcal{D}\beta \Leftrightarrow \rho(\alpha) = \rho(\beta)$ where $\rho(\alpha) = |\operatorname{Im}(\alpha)|$. By the Corollary, if $\varepsilon, \mu \in E(\mathcal{T}_n)$ and $\rho(\varepsilon) = \rho(\mu) = m$ say, then $H_\varepsilon \cong H_\mu$. In fact $H_\varepsilon \cong H_\mu \cong \mathcal{S}_m$.