SEMIGROUP THEORY
A LECTURE COURSE

VICTORIA GOULD

1. The Basic Concept

Definition 1.1. 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 $a * (b * c) = (a * b) * c$].

n	Semigroups	Groups
1	1	1
2	4	1
3	18	1
4	126	2
5	1160	1
6	15973	2
7	836021	1
8	1843120128	5
9	52989400714478	2

The number (whatever it means) of semigroups and groups of order n

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 For all $n, m \in \mathbb{N} = \{1, 2, \dots\}$:

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

Definition 1.2. 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 $n, m \in \mathbb{N}^0 = \{0, 1, 2, \dots\}$.

Note. The identity of a monoid is unique.

Definition 1.3. A *group* G is a monoid such that for all $a \in G$ there exists a $b \in G$ with $ab = 1 = ba$.

Example 1.4. 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

$$\begin{array}{c|c} & e \\ \hline e & e \end{array}$$

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

Example 1.5. A ring is a semigroup under $\times$. If the ring has an identity then this semigroup is a monoid.

Example 1.6. (1) $(\mathbb{N}, \times)$ is a monoid.
(2) $(\mathbb{N}, +)$ is a semigroup.
(3) $(\mathbb{N}^0, \times)$ and $(\mathbb{N}^0, +)$ are monoids.

Example 1.7. Let I, J be non-empty sets and set $T = I \times J$ with the binary operation

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

Note

$$\begin{aligned} \big((i, j)(k, \ell)\big)(m, n) &= (i, \ell)(m, n) = (i, n), \\ (i, j)\big((k, \ell)(m, n)\big) &= (i, j)(k, n) = (i, n), \end{aligned}$$

for all $(i, j), (k, \ell), (m, n) \in T$ and hence multiplication is associative.
Then T is a semigroup called the *rectangular band* on $I \times J$.

Notice: $(i, j)^2 = (i, j)(i, j) = (i, j)$, i.e. every element is an idempotent.

This shows that not every semigroup is the multiplicative semigroup of a ring, since any ring where every element is an idempotent is commutative. However, a rectangular band does not *have to be commutative.*

Adjoining an Identity Let S be a semigroup. Find a symbol not in S, call it "1". On $S \cup \{1\}$ we define $*$ by

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

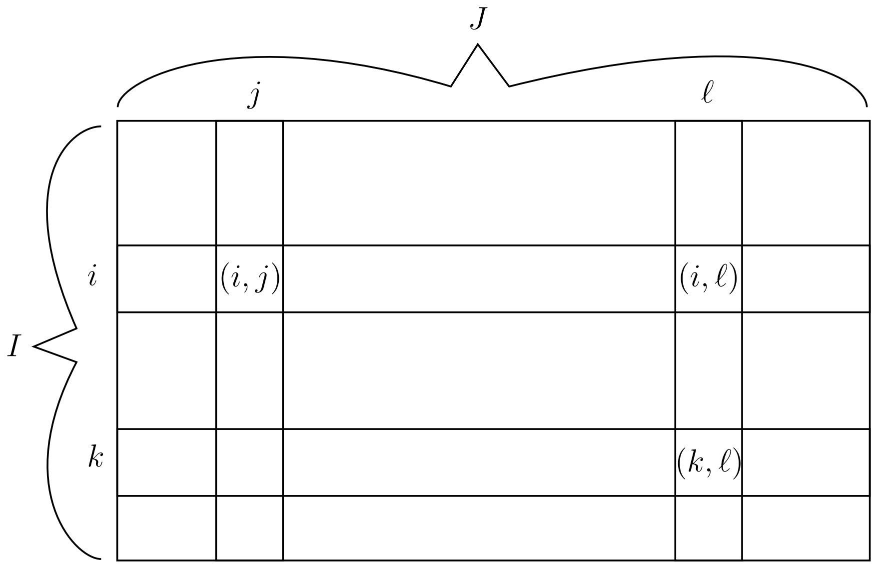


FIGURE 1. The rectangular band.

Then $*$ is associative (check this) so $S \cup \{1\}$ is a monoid with identity 1. Multiplication in $S \cup \{1\}$ extends that in S.
The monoid S^1 is defined by

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

DEFINITION 1.8. S^1 is "*S with a 1 adjoined if necessary*".

EXAMPLE 1.9. 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)

The Bicyclic Semigroup/Monoid B

If $A \subseteq \mathbb{Z}$, such that $|A| < \infty$, then $\max A$ is the greatest element in A. i.e.

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

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 $(\mathbb{Z}, \max)$ where $\max(a,b) = \max\{a,b\}$ is a semigroup and $(\mathbb{N}^0, \max)$ is a monoid.

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

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

Put $B = \mathbb{N}^0 \times \mathbb{N}^0$. On B we define a 'binary operation' by

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

where $t = \max\{b,c\}$.

Proposition 1.10. *B is a monoid with identity $(0,0)$.*

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 verify associativity.
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

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

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 this is equivalent to

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

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 monoid. □

Definition 1.11. With the above multiplication, B is called the *Bicyclic Semigroup/Monoid*.

Example 1.12. For any set X, the set $\mathcal{T}_X$ of all maps $X\to X$ is a monoid. (See Lecture 3).

Definition 1.13. 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; $(a,b)(b,c)=(a,c)$.

Definition 1.14. A semigroup is *cancellative* if

$$ac=bc\Rightarrow a=b,\ \text{and}$$
$$ca=cb\Rightarrow a=b.$$

NOT ALL SEMIGROUPS ARE CANCELLATIVE

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

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

B is not cancellative as e.g.

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

Groups are cancellative (indeed, any subsemigroup of a group is cancellative). $\mathbb{N}^0$ is a cancellative monoid, which is not a group.

Definition 1.15. 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

$$\begin{aligned} a \cdot b &= ab && \text{for all } a \in S, \\ 0 \cdot a &= 0 = a \cdot 0 && \text{for all } a \in S, \\ 0 \cdot 0 &= 0. \end{aligned}$$

Then $\cdot$ is associative, so S^0 is a semigroup with zero 0.

Definition 1.16. S^0 is S *with a zero adjoined*.

2. Standard algebraic tools

Definition 2.1. Let S be a semigroup and $\emptyset \neq T \subseteq S$. 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 $1 \in T$.

Note T is then itself a semigroup/monoid.

Example 2.2. (1) $(\mathbb{N}, +)$ is a subsemigroup of $(\mathbb{Z}, +)$.
(2) $R = \{c_x \mid x \in X\}$ is a subsemigroup of $\mathcal{T}_X$, since

$$c_x c_y = c_y$$

for all $x, y \in X$.
R is a *right zero semigroup* (See Ex.1).
(3) Put $E(B) = \{(a,a) \mid a \in \mathbb{N}^0\}$.
From Ex. 1, $E(S) = \{\alpha \in B : \alpha^2 = \alpha\}$
Claim $E(B)$ 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

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

Definition 2.3. 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 2.4. (1) $\theta : B \to \mathbb{Z}$ given by $(a, b)\theta = a - b$ is a monoid morphism because

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

Furthermore $(0, 0)\theta = 0 - 0 = 0$.
(2) 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 2.5. A bijective morphism is an *isomorphism*.

Isomorphisms preserve algebraic properties (e.g. commutativity).

See handout for further information.

Embeddings Suppose $\alpha : S \to T$ is a morphism. Then Im α is a subsemigroup (submonoid) of T. If α is 1:1, then $\alpha : S \to \text{Im } \alpha$ is an isomorphism, so that $S \cong \text{Im } \alpha$. We say that S is *embedded* in T.

Theorem 2.6 (The "Cayley Theorem" – for Semigroups)**.** *Let S be a semigroup. Then S is embedded in $\mathcal{T}_{S^1}$.*

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 $s\alpha = \rho_s$.
We show 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.

We show α is a morphism: Let $u, v \in S$. For any $x \in X$ we have

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

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 2.7 (The "Cayley Theorem" - for Monoids)**.** *Let S be a monoid. Then there exists an embedding $S \hookrightarrow \mathcal{T}_S$.*

Proof. $S^1 = S$ so $\mathcal{T}_S = \mathcal{T}_{S^1}$. We know α is a semigroup embedding. We need only 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 2.8 (The Cayley Theorem - for Groups)**.** *Let S be a group. Then there exists an embedding $S \hookrightarrow \mathcal{S}_S$.*

Proof. Exercise. □

2.1. **Idempotents**

S will always denote a semigroup.

Definition 2.9. $e \in S$ is an *idempotent* if $e^2 = e$. We put

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

Now, $E(S)$ may be empty, e.g. $E(S) = \emptyset$ ($\mathbb{N}$ under $+$).
$E(S)$ 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 $E(S) = S$.

For the bicyclic semigroup B we have from Ex. 1

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

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 $E(S) = \{1\}$.

DEFINITION 2.10. If $E(S) = S$, then S is a *band*.

DEFINITION 2.11. If $E(S) = S$ and S is commutative, then S is a *semilattice*.

Lemma 2.12. *Let $E(S) \neq \emptyset$ and suppose $ef = fe$ for all $e, f \in E(S)$. Then $E(S)$ is a subsemigroup of S.*

Proof. Let $e, f \in E(S)$. Then

$$(ef)^2 = (ef)(ef) = e(fe)f = e(ef)f = (ee)(ff) = ef$$

and hence $ef \in E(S)$. $\square$

From Lemma 2.12 if $E(S) \neq \emptyset$ and idempotents in S commute then $E(S)$ is a semilattice.

EXAMPLE 2.13. (1) $E(B) = \{(a, a) \mid a \in \mathbb{N}^0\}$ is a semilattice.
(2) 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 2.14. 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 2.15. *Let $a \in S$. Then either*
(i) $|\langle a \rangle| = \infty$ and $\langle a \rangle \cong (\mathbb{N}, +)$ or
(ii) $\langle a \rangle$ is finite. In this case $\exists n, r \in \mathbb{N}$ such that

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

$\{a^n, a^{n+1}, \ldots, a^{n+r-1}\}$ is a subsemigroup of $\langle a \rangle$ and for all $s, t \in \mathbb{N}^0$,

$$a^{n+s} = a^{n+t} \Leftrightarrow s \equiv t \ (\mathit{mod}\ r).$$

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. This is case (i).

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 $r \in \mathbb{N}$ – 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 $a^n = a^{n+r}$.
DO NOT CANCEL
Let $s, t \in \mathbb{N}^0$ with

$$s = s' + ur, t = t' + vr$$

with

$$0 \leq s', t' \leq r - 1,\ u, v \in \mathbb{N}^0.$$

Then

$$\begin{aligned}
a^{n+s} &= a^{n+s'+ur} \\
&= a^{s'}a^{n+ur} \text{ in } S^1 \\
&= a^{s'}a^{n+r}a^{(u-1)r} \\
&= a^{s'}a^{n}a^{(u-1)r} \\
&= a^{s'}a^{n+(u-1)r} \\
&\vdots \\
&= a^{s'}a^{n} \\
&= a^{n+s'}.
\end{aligned}$$

Similarly, $a^{n+t} = a^{n+t'}$. Therefore

$$a^{n+s} = a^{n+t} \Leftrightarrow a^{n+s'} = a^{n+t'} \Leftrightarrow s' = t' \Leftrightarrow s \equiv t(\bmod r).$$

Notice that

$$a^{n+ur} = a^n$$

for all u.
We have shown

$$\{a, a^2, \ldots, a^n, a^{n+1}, \ldots, a^{n+r-1}\} = \langle a\rangle$$

and

$$|\langle a\rangle| = n + r - 1.$$

Clearly

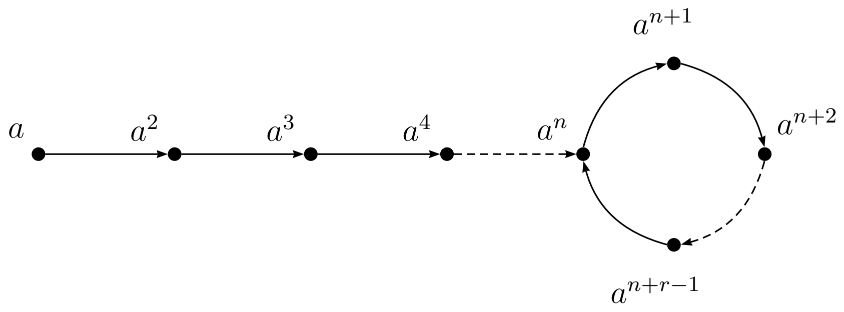
$$\{a^n, a^{n+1}, \ldots, a^{n+r-1}\}$$

is a subsemigroup. In fact

$$a^{n+s}a^{n+t} = a^{n+u}$$

where $u \equiv s + n + t \pmod r$ and $0 \leq u \leq r - 1$. This is case (ii).

We can express this pictorially:



□

Lemma 2.16 (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

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

and so $a^{n+s} \in E(S)$. $\square$

In fact, $\{a^n, a^{n+1}, \dots, a^{n+r-1}\}$ is a cyclic group with identity a^{n+s}.

Corollary 2.17. *Any finite semigroup contains an idempotent.*

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

We know $c_x c_y = c_y$ for all $x, y \in X$ and hence $c_x c_x = c_x$ for all $x \in X$. Therefore $c_x \in E(\mathcal{T}_X)$ for all $x \in X$. But if $|X| > 1$ then there are other idempotents in $\mathcal{T}_X$ as well.

Example 2.18. Let us define an element

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

Then

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix},$$

thus α is an idempotent.

Definition 2.19. Let $\alpha\colon X \to Y$ be a map and let $Z \subseteq X$. Then the *restriction of α to the set Z* is the map

$$\alpha|_Z\colon Z \to Y, z \mapsto z\alpha \text{ for every } z \in Z.$$

NOTE: Sometimes we treat the restriction $\alpha|_Z$ as a map with domain Z and codomain $Z\alpha$.

Example 2.20. Let us define a map with domain $\{a, b, c, d\}$ and codomain $\{1, 2, 3\}$:

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

Then $\alpha|_{\{a,d\}}$ is the following map:

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

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

Let $\alpha \in \mathcal{T}_X$ (i.e. $\alpha\colon X \to X$). Recall that

$$\operatorname{Im} \alpha = \{x\alpha : x \in X\} \subseteq X = X\alpha.$$

Example 2.21. In $\mathcal{T}_3$ we have $\operatorname{Im} c_1 = \{1\}$, $\operatorname{Im} I_3 = \{1,2,3\}$ and

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

The following lemma gives a rather useful characterization of the idempotents of a transformation monoid.

Lemma 2.22 (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. $\varepsilon|_{\operatorname{Im}\varepsilon} = I_{\operatorname{Im}\varepsilon}$ means that for all $y \in \operatorname{Im}\varepsilon$ we have $y\varepsilon = y$.
Note that $\operatorname{Im}\varepsilon = \{x\varepsilon : x \in X\}$.
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 2.23. Let

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

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 2.24. We can similarly create another idempotent in $\mathcal{T}_7$, first we determine its image: let it be the subset $\{1,2,5,7\}$. Our map must fix these elements, but can map the other elements to any of these:

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 1 & 2 & & & 5 & & 7\end{pmatrix} \to \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 1 & 2 & 5 & 7 & 5 & 2 & 7\end{pmatrix} \in E(\mathcal{T}_7).$$

Using Lemma 2.22 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

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

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

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

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

3. Relations

Please see the handout 'Functions and Relations'.

In group theory, homomorphic images of groups are determined by normal subgroups. The situation is more complicated in semigroup theory, namely the homomorphic images of semigroups are determined by special equivalence relations. Furthermore, elements of semigroups can be quite often 'ordered'. For example there is a natural notion of a map being 'bigger' than another one: namely if its image has a bigger cardinality. These examples show that relations play a central role in semigroup theory.

Definition 3.1. A (binary) *relation* ρ on A is a subset of $A \times A$.

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

3.1. **Some special relations**

Properties of the relation $\leqslant$ on $\mathbb{R}$:

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

Thus, the relation $\leqslant$ is a total order on $\mathbb{R}$ (sometimes we say that $\mathbb{R}$ is linearly ordered by $\leqslant$).

Recall that if X is any set, we denote by $\mathcal{P}(X)$ the set of all subsets of X (and call it the *power set of* X. Properties of the relation $\subseteq$ on a power set $\mathcal{P}(X)$ of an arbitrary set X:

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

Notice that if $|X| > 2$ and $x, y \in X$ with $x \neq y$ then $\{x\} \not\subseteq \{y\}$ and $\{y\} \not\subseteq \{x\}$, thus $\subseteq$ is a partial order but not a total order on $\mathcal{P}(X)$.

Recall that

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

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

We denote by ω the UNIVERSAL relation on A: $\omega = A \times A$. So $x \ \omega \ y$ for all $x, y \in A$, and $[x] = A$ for all $x \in A$.

We denote by ι be the EQUALITY relation on A:

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

Thus $x \ \iota \ y \Leftrightarrow x = y$ and so $[x] = \{x\}$ for all $x \in A$.

3.2. **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 that $\iota \subseteq \rho \Leftrightarrow \rho$ 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.

Lemma 3.2. *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. $\square$

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 $\big(\equiv \pmod 2\big) \cup \big(\equiv \pmod 3\big)$ were to be transitive then we would have

$$\left.\begin{aligned} (3,1) &\in \big(\equiv \pmod 2\big) \cup \big(\equiv \pmod 3\big) \\ (1,4) &\in \big(\equiv \pmod 2\big) \cup \big(\equiv \pmod 3\big) \end{aligned}\right\}$$

$\Rightarrow (3,4) \in \big(\equiv \pmod 2\big) \cup \big(\equiv \pmod 3\big)$
$\Rightarrow 3 \equiv 4 \pmod 2$ or $3 \equiv 4 \pmod 3$
but this is a contradiction!

3.3. **Kernels**

Definition 3.3. Let $\alpha\colon X \to Y$ be a map. Define a relation $\ker\alpha$ on X by the rule

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

We call $\ker\alpha$ the *kernel of* α.

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 3.4. Let $\alpha\colon \underline{6} \to \underline{4}$ where

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

In this case the different $\ker\alpha$-classes are $\{1,3\}, \{2,4,5\}, \{6\}$.

Note that if $\alpha\colon A \to B$ is a map then α is one-one if and only if $\ker\alpha = \iota_A$ and α is constant if and only if $\ker\alpha = \omega_A$.

Definition 3.5. 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 3.6 (The Kernel Lemma)**.** *Let $\theta\colon S \to T$ 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. □

NOTE. Some remarks on the notion *well-defined*: usually we define a map on a set by simply stating what the image of the individual elements should be, e.g:

$$\alpha\colon \mathbb{N} \to \mathbb{Z},\ n\alpha = \text{the number of 9's less the number of 2's in the decimal form of } n.$$

But very often in mathematics, the set on which we would like to define the map is a set of classes of an equivalence relation (that is, the *factor set of the relation*). In such cases, we usually define the map by using the elements of the equivalence classes (for usually we can use some operations on them). For example let

$$\rho = \{(n, m) | n \equiv m \pmod 4\} \subseteq \mathbb{N} \times \mathbb{N}.$$

Then ρ is an equivalence relation having the following 4 classes:

$$A = \{1, 5, 9, 13, \ldots\}, B = \{2, 6, 10, 14, \ldots\},$$

$$C = \{3, 7, 11, 15, \ldots\}, D = \{4, 8, 12, 16, \ldots\}.$$

Thus, the factor set of ρ is $X = \{A, B, C, D\}$. We try do define a map from X to $\mathbb{N}$ by

$$\alpha\colon X \to \mathbb{N}, [n]_\rho\alpha = 2^n.$$

What is the image of A under α? We choose an element n of A (that is, we *represent* A as $[n]_\rho$): $1 \in A$, thus $A = [1]_\rho$. So $A\alpha = [1]_\rho\alpha = 2$. However, $5 \in A$, too! So we have $A\alpha = [5]_\rho\alpha = 2^5 = 32$. Thus, $A\alpha$ has more than one values. We refer to this situation as 'α being not well-defined'.

Keep in mind that whenever we try to define something (a map, or an operation) on a factor set of an equivalence relation by referring to ELEMENTS of the equivalence classes, it MUST be checked, that the choice of the elements of the equivalence classes does not influence the result.

For example in the above-mentioned example let

$$\beta\colon X \to \mathbb{N}^0, [n]_\rho\beta = \overline{n},$$

where $\overline{n}$ denotes the remainder of n on division by 4 (that is, $0, 1, 2$ or 3). In this case β is well-defined, because all elements in the same class have the same remainder, for example

$$A\beta = [1]_\rho\beta = 1 = [5]_\rho\beta = [9]_\rho\beta = \ldots$$

The following construction and lemmas might be familiar...

Let ρ be a congruence on S. Then we define

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

Define a binary operation on S/ρ by

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

We need to make sure that this is a well-defined operation, that is, that the product $[a][b]$ does not depend on the choice of a and b. 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.

Definition 3.7. 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. Moreover if S is a monoid then $1\nu_\rho = [1]$, so that ν_ρ is a monoid morphism. We now want to examine the kernel of ν_ρ:

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

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

Theorem 3.8. *[The Fundamental Theorem of Morphisms for Semigroups] Let $\theta\colon S \to T$ 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 $\bar{\theta}\colon S/\ker\theta \to \operatorname{Im}\theta$ 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-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 analogue of Theorem 3.8 holds for monoid to give us the **The Fundamental Theorem of Morphisms for Monoids**.

Example 3.9. $\theta : B \to (\mathbb{Z}, +)$ given by $(a, b)\theta = a - b$ is a monoid morphism. Check that θ is onto, so by FTH we have

$$B/\ker\theta \cong \mathbb{Z}.$$

Moreover, $\ker\theta$ is the congruence given by

$$(a, b)\ \ker\theta\, (c, d) \Leftrightarrow a - b = c - d.$$

4. Ideals

Ideals play an important role in Semigroup Theory, but rather different to that they hold in Ring Theory. The reason is that in case of rings, ALL homomorphisms are determined by ideals, but in case of semigroups, only some *are.*

4.1. 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 $\mathcal{P}(S) = \{S \mid A \subseteq S\}$, equipped by the above-defined operation, 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 - think of a right zero semigroup, there $AC = BC = C$ for all $A, B, C \subseteq S$.
(4) A is isomorphic to the subsemigroup $\{\{a\} \mid a \in A\}$ of $\mathcal{P}(A)$.
(5) $S^1S = S = SS^1$.

Definition 4.1. Let $\emptyset \neq I \subseteq S$ then I is
(1) a *left ideal* if $SI \subseteq I$ (i.e. $a \in I, s \in S \Rightarrow sa \in I$);
(2) a *right ideal* if $IS \subseteq I$;
(3) an *(two-sided) ideal* if $IS \cup SI \subseteq I$, that is, I is both a left and a right ideal.

Note that if S is commutative, (1),(2) and (3) above coincide.
If $\emptyset \neq I \subseteq S$ then we have:
I is a left ideal $\Leftrightarrow S^1I \subseteq I$;
I is a right ideal $\Leftrightarrow IS^1 \subseteq I$;
I is an ideal $\Leftrightarrow S^1IS^1 \subseteq I$.

Note that any (left/right) ideal is a subsemigroup.

Example 4.2. (1) Let $i \in I$ then $\{i\} \times J$ is a right ideal in a rectangular band $I \times J$.
(2) Let $m \in \mathbb{N}^0$ be fixed. Then $I_m = \{(x, y) \mid x \geqslant m, y \in \mathbb{N}^0\}$ is a right ideal in the bicyclic semigroup B.
Indeed, let $(x, y) \in I_m$ and let $(a, b) \in B$. Then
$$(x, y)(a, b) = (x - y + t, b - a + t),$$
where $t = \max\{y, a\}$. Now, we know that $x \geq m$ and that $t \geq y$, so $t - y \geq 0$. Adding up these two inequalities, we get that $x - y + t \geq m$, thus the product is indeed in I_m.
(3) If $Y \subseteq X$ 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
$$S^n = \{a_1a_2 \dots a_n \mid a_i \in S\}.$$
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 4.3. Let S be a semigroup.
(1) We say that 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 $S^2 \neq 0$.

Note that S^2 is always an ideal, so the condition $S^2 \neq 0$ is only required to exclude the 2-element null semigroup. A null semigroup is a semigroup with zero such that every product equals 0 - notice that every subset containing 0 is an ideal.

Example 4.4. 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 4.5. We have $(\mathbb{N}, +)$ is a semigroup. Let $n \in \mathbb{N}$. 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 4.6. 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. □

4.2. **Principal 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

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

Claim. aS^1 (S^1a, S^1aS^1) is the "smallest" right (left, two-sided ideal) containing a.

Proof. (for aS^1).
We have $a = a1 \in aS^1$ 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 $aS^1 \subseteq IS^1 = I \cup IS \subseteq I$. □

Definition 4.7. We call aS^1 (S^1a, S^1aS^1) the *principal right (left, two-sided) ideal generated by a.*

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

Example 4.8. In a group G we have

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

for all $a \in G$.

Example 4.9. In $\mathbb{N}$ under addition we have

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

Example 4.10. B is simple, so

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

for all $(m,n) \in B$. However:

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 4.11 (Principal 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 (ii), (iii) and (iv) are equivalent.

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

(ii) $\Rightarrow$ (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 4.12 (Principal 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 $t \in S$.

The following relation is crucial in semigroup theory.

DEFINITION 4.13. The relation $\mathcal{L}$ on a semigroup S is defined by the rule

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

for any $a, b \in S$.

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

Corollary 4.14. *We have that*

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

Proof.

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

by the Principal Left Ideal Lemma. □

We note that this statement about $\mathcal{L}$ **can be used as a definition of $\mathcal{L}$.**

REMARK.
(1) $a \mathrel{\mathcal{L}} b \Leftrightarrow a = b$ or there exist $s, t \in S$ 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

$$a \mathcal{R} b \Leftrightarrow aS^1 = bS^1$$

and

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

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 4.15. 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 the so-called *Greens' relations.*

Example 4.16. (1) If S is commutative, $\mathcal{L} = \mathcal{R} = \mathcal{H}$.

(2) 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 have $\mathcal{H} = \omega$.

Example 4.17. 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 4.18. In B we know

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

and so we have

$$(m,n)B^1 = (p,q)B^1 \Leftrightarrow m = p.$$

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 $\mathcal{H} = \iota$.

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

CLAIM. $\alpha\mathcal{T}_X \subseteq \beta\mathcal{T}_X \Leftrightarrow \ker\beta \subseteq \ker\alpha$.
(Recall $\ker\alpha = \big\{(x,y) \in X \times X \mid x\alpha = y\alpha\big\}$).

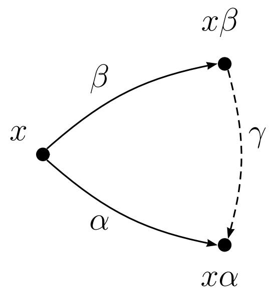
Proof. ($\Rightarrow$) Suppose $\alpha\mathcal{T}_X \subseteq \beta\mathcal{T}_X$. Then $\alpha = \beta\gamma$ for some $\gamma \in \mathcal{T}_X$. Let $(x,y) \in \ker\beta$. Then

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

Hence $(x,y) \in \ker\alpha$ and so $\ker\beta \subseteq \ker\alpha$.

($\Leftarrow$) Suppose $\ker\beta \subseteq \ker\alpha$. Define $\gamma\colon X \to X$ by

$$z\gamma = \begin{cases} z & z \notin \operatorname{Im}\beta \\ x\alpha & z = x\beta \end{cases}$$



If $z = x\beta = y\beta$, then $(x,y) \in \ker\beta \subseteq \ker\alpha$ 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 Principal Ideal Lemma, $\alpha\mathcal{T}_X \subseteq \beta\mathcal{T}_X$. □

Corollary 4.19 ($\mathcal{R}$–$\mathcal{T}_X$-Lemma)**.** *$\alpha\ \mathcal{R}\ \beta \Leftrightarrow \ker\alpha = \ker\beta$.*

Proof. We have

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

□

FACT: $\mathcal{T}_X\alpha \subseteq \mathcal{T}_X\beta \Leftrightarrow \operatorname{Im}\alpha \subseteq \operatorname{Im}\beta$ (See Exercises).

Corollary 4.20 ($\mathcal{L} - \mathcal{T}_X$-Lemma)**.** *$\alpha\ \mathcal{L}\ \beta \Leftrightarrow \operatorname{Im}\alpha = \operatorname{Im}\beta$.*

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

EXAMPLE 4.21. 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 $\ker\varepsilon$ has classes $\{1,2\},\{3\}$. So

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

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. Subgroups of Semigroups

Let S be a semigroup and let $H \subseteq S$. 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.

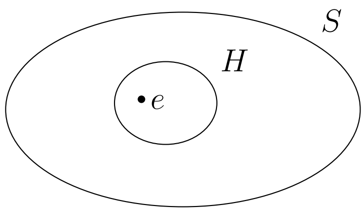


Figure 2. e is the only idempotent in H.

(3) If $e \in E(S)$, then $\{e\}$ is a trivial subgroup.
(4) With $\alpha = \begin{pmatrix}1 & 2 & 3\\ 3 & 3 & 2\end{pmatrix}$ and $\epsilon = \begin{pmatrix}1 & 2 & 3\\ 2 & 2 & 3\end{pmatrix}$ we have the $\mathcal{H}$-class $\{\epsilon, \alpha\}$ is a subgroup of $\mathcal{T}_3$.

(5) $\mathcal{S}_X$ is a subgroup of $\mathcal{T}_X$. Notice

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

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

Definition 5.1. In the sequel, we are going to denote by L_a the $\mathcal{L}$-class of a; by R_a the $\mathcal{R}$-class of a and by H_a the $\mathcal{H}$-class of a.

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

We are going to show that the maximal subgroups of semigroups are just the $\mathcal{H}$-classes of idempotents. As a consequence, we will see that whenever two subgroups are not disjoint, then they are both contained within a subgroup, as the following figure shows.

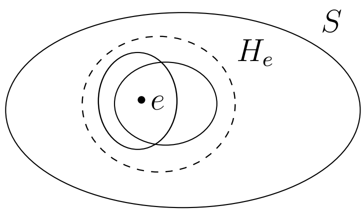


Figure 3. Existence of a Maximal Subgroup.

Lemma 5.2 (Principal Ideal for Idempotents). *Let $a \in S$, $e \in E(S)$. Then*

(i) $S^1a \subseteq S^1e \Leftrightarrow ae = a$

(ii) $aS^1 \subseteq eS^1 \Leftrightarrow ea = a$.

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 Principal Ideal Lemma. Conversely, if $S^1a \subseteq S^1e$ then by the Principal Ideal Lemma we have $a = te$ for some $t \in S^1$. Then

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

□

Corollary 5.3. *Let $e \in E(S)$. Then we have*

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

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

Lemma 5.4. *Let G be a subgroup with idempotent e. Then $G \subseteq H_e$, thus, the elements of G are all $\mathcal{H}$-related.*

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 $a \,\mathcal{H}\, e$ for all $a \in G$, so $G \subseteq H_e$. □

Theorem 5.5 (Maximal Subgroup Theorem)**.** *Let $e \in E(S)$. Then H_e is the maximal subgroup of S with identity e.*

Proof. We have shown that if G is a subgroup with identity e, then $G \subseteq H_e$.
We show now that H_e itself is a subgroup with identity e.
We know that e is an identity for H_e. Suppose $a, b \in H_e$. 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 $ab \in H_e$. It remains to show that for all $a \in H_e$ there exists $b \in H_e$ with $ab = e = ba$.

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

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

We have

$$a(ete) = (ae)te = ate = ee = e = \cdots = (ese)a.$$

Let $x = ete$, $y = ese$ so $x, y \in S$ and $ex = xe = x$, $ey = ye = y$. Also $e = ax = ya$. Now

$$x = ex = (ya)x = y(ax) = ye = y.$$

So let $b = x = y$. Then

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

so $b \,\mathcal{H}\, e$, thus $b \in H_e$. Hence H_e is indeed a subgroup. □

Let $e, f \in E(S)$ with $e \neq f$. Since H_e and H_f are subgroups containing the idempotents e and f, respectively, $H_e \neq H_f$. This implies that $H_e \cap H_f = \emptyset$.

Theorem 5.6. *[Green's Theorem] If $a \in S$, then a lies in a subgroup iff $a \,\mathcal{H}\, a^2$.*

Proof. See later. □

Corollary 5.7. *Let $a \in S$. Then the following are equivalent:*

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

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

(ii) $\Rightarrow$ (iii): If $a \,\mathcal{H}\, e$, then $H_a = H_e$ and by the MST, H_e is a subgroup.

(iii) $\Rightarrow$ (i): Straightforward, for $a \in H_a$.

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

(iv) $\Rightarrow$ (i) This follows from Greeen's Theorem (Theorem 5.6).

□

Subgroups of $\mathcal{T}_n$

We use Green's Theorem to show the following.

Lemma 5.8. *Let $\alpha \in \mathcal{T}_n$. Then α lies in a subgroup of $\mathcal{T}_n \Leftrightarrow$ the map diagram has no tails of length $\geqslant 2$.*

Proof. We have that

$$\begin{aligned} \alpha \text{ lies in a subgroup} &\Leftrightarrow \alpha \,\mathcal{H}\, \alpha^2 \\ &\Leftrightarrow \alpha \,\mathcal{L}\, \alpha^2, \alpha \,\mathcal{R}\, \alpha^2 \\ &\Leftrightarrow \operatorname{Im}\alpha = \operatorname{Im}\alpha^2, \ker\alpha = \ker\alpha^2. \end{aligned}$$

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. Recall

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

We have seen that

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

We know that $\ker\alpha \subseteq \ker\alpha^2$ ($\alpha^2\mathcal{T}_n \subseteq \alpha\mathcal{T}_n$), which means that the $\ker\alpha^2$-classes are just unions of $\ker\alpha$-classes:

Claim. For $\alpha \in \mathcal{T}_n$, $\operatorname{Im}\alpha = \operatorname{Im}\alpha^2 \Leftrightarrow \ker\alpha = \ker\alpha^2$.

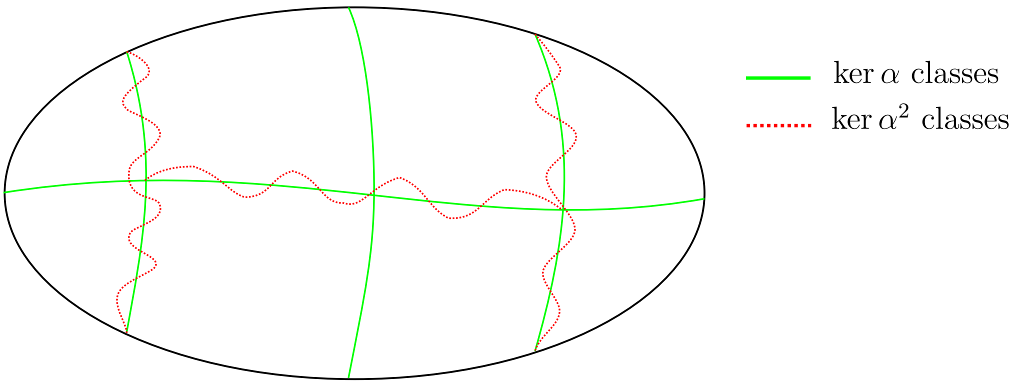


FIGURE 4. The classes of $\ker\alpha$ and $\ker\alpha^2$.

Proof.

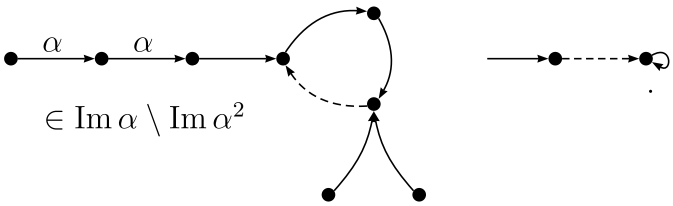
$$\left|\underline{n}/\ker\alpha^2\right| = |\operatorname{Im}\alpha^2| \leq |\operatorname{Im}\alpha| = |\underline{n}/\ker\alpha|\,.$$

Thus $\ker\alpha$ and $\ker\alpha^2$ have the same number of classes if and only if $|\operatorname{Im}\alpha| = |\operatorname{Im}\alpha^2|$. It follows that $\ker\alpha = \ker\alpha^2$ if and only if $\operatorname{Im}\alpha = \operatorname{Im}\alpha^2$. □

We now continue with the proof of Lemma 5.8:

We have that α lies in a subgroup $\Leftrightarrow \operatorname{Im}\alpha = \operatorname{Im}\alpha^2$. Note that elements of $\operatorname{Im}\alpha \setminus \operatorname{Im}\alpha^2$ are exactly those second vertices of tails in the map diagram of α which are not members of a cycle. Thus, $\operatorname{Im}\alpha^2 = \operatorname{Im}\alpha$ if and only if no such vertices exist, thus if and only if all tails have length smaller than or equal to 1. □

An arbitrary element of $\mathcal{T}_n$ looks like:

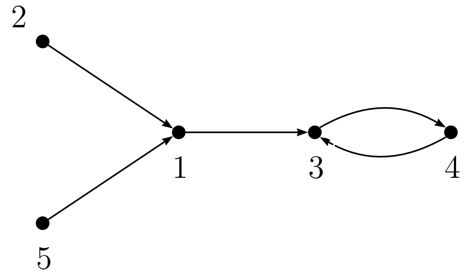


EXAMPLE 5.9.

(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

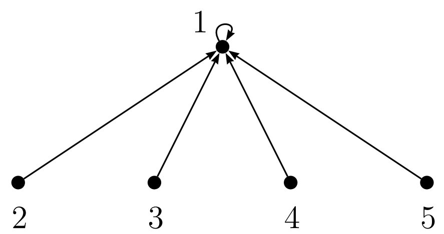


Now α has a tail with length $\geqslant 2$ and therefore α doesn't lie in any subgroup.

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

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

This has the following map diagram



Now c_1 has no tails of length $\geqslant 2$, therefore c_1 lies in a subgroup and hence c_1 lies in a subgroup. Note that actually $c_1^2 = c_1$.

Now for any β,

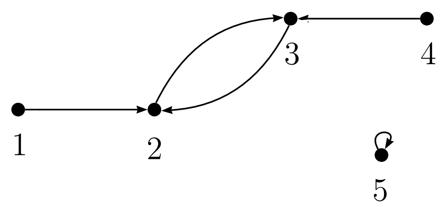
$$\begin{aligned} \beta \in H_{c_1} &\Leftrightarrow \beta \ \mathcal{H} \ c_1, \\ &\Leftrightarrow \beta \ \mathcal{R} \ c_1 \text{ and } \beta \ \mathcal{L} \ c_1, \\ &\Leftrightarrow \ker \beta = \ker c_1 \text{ and } \operatorname{Im} \beta = \operatorname{Im} c_1, \\ &\Leftrightarrow \ker \beta \text{ has classes } \{1,2,3,4,5\} \text{ and } \operatorname{Im} \beta = \{1\}, \\ &\Leftrightarrow \beta = c_1. \end{aligned}$$

Therefore the maximal subgroup containing c_1 is $H_{c_1} = \{c_1\}$.

(3) Take the element

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

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

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

We now figure out what the elements of $\mathcal{H}_\alpha$ are. 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 (note that 1 and 3 must have the same images, just as 2 and 4):

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

These are all 6 elements.

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

6. $\mathcal{D}, \mathcal{J}$ and Green's Lemmas

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

Definition 6.1. We say that $a \mathcal{J} b$ if and only if

$$a \mathcal{J} b \Leftrightarrow S^1aS^1 = S^1bS^1$$

Check:

$$a \mathcal{J} b \Leftrightarrow \exists\, s, t, u, v \in S^1 \text{ with } a = sbt \quad b = uav.$$

Note. If $a \mathcal{L} b$, then $S^1a = S^1b$ so $S^1aS^1 = S^1bS^1$ 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 I is an ideal of S, 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.

We have shown that that

$$S \text{ is simple } \Leftrightarrow \mathcal{J} = \omega.$$

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.

6.1. **Composition of Relations**

Definition 6.2. If ρ and λ are relations on A we define

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

Lemma 6.3. *If ρ, λ are equivalence relations and if $\rho \circ \lambda = \lambda \circ \rho$ then $\rho \circ \lambda$ is an equivalence relation. Also, it is 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

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

  (Note that first we use that $\nu = \rho \circ \lambda$, and next we use that $\nu = \lambda \circ \rho$.)
  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 $x\ \rho\ z\ \lambda\ c$, 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 $\nu \subseteq \tau$. □

The smallest equivalence relation containing any ρ and λ is denoted by $\rho \vee \lambda$; we have shown that if ρ and λ commute, then $\rho \vee \lambda = \rho \circ \lambda$.

Definition 6.4. $\mathcal{D} = \mathcal{R} \circ \mathcal{L}$, i.e. $a\ \mathcal{D}\ b \Leftrightarrow \exists c \in S$ with $a\ \mathcal{R}\ c\ \mathcal{L}\ b$.

Lemma 6.5 (The $\mathcal{D}$ Lemma)**.** $\mathcal{R} \circ \mathcal{L} = \mathcal{L} \circ \mathcal{R}$

Proof. We prove that $\mathcal{R} \circ \mathcal{L} \subseteq \mathcal{L} \circ \mathcal{R}$, the proof of the other direction 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

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

Put $d = bu$ then we have

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

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

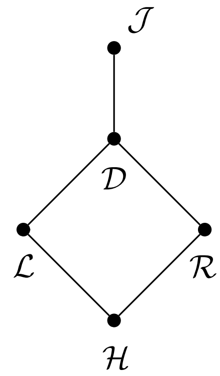
$$b \underset{(4)}{=} tc \underset{(2)}{=} tav \underset{(1)}{=} tcuv \underset{(4)}{=} buv = dv.$$

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

Hence $\mathcal{D}$ is an equivalence relation and $\mathcal{D} = \mathcal{L} \vee \mathcal{R}$.
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. Then for any $a \in D$ we have $R_a \subseteq D = D_a$, and $L_a \subseteq D$. We denote the $\mathcal{R}$-classes as rows and the $\mathcal{L}$-classes as columns. The cells (if non-empty) will be $\mathcal{H}$-classes - we show they are all non-empty!
Let $u, v \in D$ then $u \mathrel{\mathcal{D}} v$. This implies that there exists $h \in S$ with $u \mathrel{\mathcal{R}} h \mathrel{\mathcal{L}} v$, so $R_u \cap L_v \neq \emptyset$, that is, **no cell is empty**. Moreover

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

As $\mathcal{D}$ is an equivalence, S is the union of such "egg-boxes": the rows represent the $\mathcal{R}$-classes, and the columns represent the $\mathcal{L}$-classes.

	u	h	
		v	

6.2. 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 6.6 (Green's Lemma). *Let $a, b \in S$ be such that $a \mathrel{\mathcal{R}} b$ and let $s, s' \in S$ be such that*

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

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 $c \mathrel{\mathcal{R}} c\rho_s$ and if $d \in L_b$ then $d \mathrel{\mathcal{R}} d\rho_{s'}$).

Proof. If $c \in L_a$ then

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

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

Let $c \in L_a$. 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

$$\begin{aligned} cs &= c \cdot s, \\ c &= cs \cdot s'. \end{aligned}$$

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

Continuing Lemma 6.6. 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.

Let $s \in S^1$. Then we define $\lambda_s : S \to S$ by $a\lambda_s = sa$.

Lemma 6.7 (Dual of Green's Lemma)**.** *Let $a, b \in S$ be such that $a \mathrel{\mathcal{L}} b$ and let $t, t' \in S$ be such that $ta = b$ and $t'b = a$. Then $\lambda_t : R_a \to R_b$ and $\lambda_{t'} : R_b \to R_a$ 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 6.8. *If $a \mathrel{\mathcal{D}} b$ then there exists a bijection $H_a \to H_b$.*

Proof. If $a \mathrel{\mathcal{D}} b$ then there exists $h \in S$ with $a \mathrel{\mathcal{R}} h \mathrel{\mathcal{L}} b$. 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 (just like any two $\mathcal{R}$- and $\mathcal{L}$-classes).

Theorem 6.9 (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. We prove that if $H^2 \cap H \neq \emptyset$, then H is a subgroup. This is exactly the statement of the theorem.
So suppose $H^2 \cap H \neq \emptyset$. Then there exists $a, b, c \in H$ such that $ab = c$. 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, $aH = H$.
Let $u, v \in H$. Then $av \in H$ so that as above, $Hv = H$. But then $uv \in H$ and H is a subsemigroup. Further, $vH = H$ so that by a standard argument (see Exercises 1), H is a subgroup of S.

Alternatively 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 $d = bs = dbs = d^2$. Hence H contains an idempotent, so (by the Maximal Subgroup Theorem) it is a subgroup. □

Corollary 6.10. *$a \mathcal{H} a^2 \Leftrightarrow H_a$ is a subgroup.*

Proof. We know H_a is a subgroup $\Rightarrow a, a^2 \in H_a$ so $a \mathcal{H} a^2$.
Conversely, 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's Lemma, H_a is a subgroup. □

7. Rees Matrix Semigroups

Just as the main building blocks of groups are simple groups, the main building blocks of semigroups are 0-simple semigroups.
In general, the structure of 0-simple semigroups is very complicated. In the finite case and, more generally, in case certain *chain conditions* hold, their structure is transparent - they can be described by a group and a matrix.

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

$\mathcal{M}^0 = \mathcal{M}^0(G; I, \Lambda; P)$ is the set

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

with binary operation given by $0n = 0 = n0$ for all $n \in \mathcal{M}^0$ and

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

Check that $\mathcal{M}^0(G; I, \Lambda; P)$ is a semigroup with zero 0.

Definition 7.1. $\mathcal{M}^0 = \mathcal{M}^0(G; I, \Lambda; P)$ is called a *Rees Matrix Semigroup over G*.

Definition 7.2. $a \in S$ 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.

Proposition 7.3. Rees matrix facts *Let $\mathcal{M}^0 = \mathcal{M}^0(G; I, \Lambda; P)$ be a Rees Matrix Semigroup over a group G.*

1. *(i, a, λ) is idempotent $\Leftrightarrow p_{\lambda i} \neq 0$ and $a = p_{\lambda i}^{-1}$.*
2. *$\mathcal{M}^0$ 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 $\mathcal{M}^0 \setminus \{0\}$ (so 0 and $\mathcal{M}^0$ are the only ideals).*
7. *$\mathcal{M}^0$ is 0-simple.*
8. *The so-called rectangular property:*

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

Proof. (1) We have that

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

(2) $0 = 000$ so 0 is regular. Let $(i, a, \lambda) \in \mathcal{M}^0 \setminus \{0\}$ 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 $\mathcal{M}^0$ is regular.

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

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

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 together with the dual we have $(i, a, \lambda) \,\mathcal{R}\, (j, b, \mu)$

(4) Dual.

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

(6) $\{0\}$ is a $\mathcal{D}$-class and a $\mathcal{J}$-class. If $(i,a,\lambda),(j,b,\mu)\in\mathcal{M}^0$ 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 $\mathcal{M}^0\setminus\{0\}$ are the only classes.

(7) We have already shown that the only $\mathcal{J}$-classes are $\{0\}$ and $\mathcal{M}^0\setminus\{0\}$. Let $i\in I$, then there exists $\lambda\in\Lambda$ with $p_{\lambda i}\neq 0$ so $(i,1,\lambda)^2\neq 0$. Therefore $(\mathcal{M}^0)^2\neq 0$ and so $\mathcal{M}^0$ is 0-simple.

(8) If $xy\ \mathcal{R}\ x$, then clearly $xy\ \mathcal{D}\ x$, because $\mathcal{R}\subseteq\mathcal{D}$. For the other direction, suppose that $xy\ \mathcal{D}\ x$. Notice that the two $\mathcal{D}$-classes are zero and everything else. If $xy=0$, then necessarily $x=0$, because $D_0=\{0\}$. If $xy\neq 0$, then necessarily $x,y\neq 0$, so we have that

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

Then $xy=(i,ap_{\lambda j}b,\mu)$, so $xy\ \mathcal{R}\ x$. The result for $\mathcal{L}$ is dual. $\square$

Some more facts!

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

(10) If $p_{\lambda i}\neq 0$ and $p_{\mu j}\neq 0$ then $H_{i\lambda}\simeq H_{j\mu}$. It is clear that $(i,a,\lambda)\mapsto(j,a,\mu)$ is a bijection, but this is not in general a morphism. *Exercise: find a morphism!*

Chain conditions

A finitary property is a property held by all finite semigroups: chain conditions are one kind of finitary property.

Definition 7.4. A semigroup S has M_L if there are no infinite chains

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

of principal left ideals. M_L is the *descending chain condition* (d.c.c.) on principal left ideals.
The left/right dual is M_R.

Lemma 7.5 (The Chain Lemma). *The semigroup S has M_L if and only if any chain*

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

terminates (stabilizes) i.e. there exists $n\in\mathbb{N}$ with

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

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

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

Let the strict inclusions be at the j_ith steps:

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

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 7.6. 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 Lemma holds for M^L and (M^R).

Example 7.7. Every finite semigroup has M_L, M_R, M^L, M^R. For example, if

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

then in every step, the cardinality of the sets must decrease at least by one, so the length of a strict sequence cannot be greater than $|S|$.

Example 7.8. The Bicyclic semigroup B has M^L and M^R. We know

$$B(x,y) = \big\{(p,q) \mid q \geqslant y\big\}$$

and so

$$B(x,y) \subseteq B(u,v) \Leftrightarrow y \geqslant v,$$

and inclusion is strict if and only if $y > v$. If we had an infinite chain

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

then we would have

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

which is impossible in $\mathbb{N}$.
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 infinite descending chains. Hence B **does not have** M_L or M_R.

Example 7.9. Let $\mathcal{M}^0 = \mathcal{M}^0(G; I; \Lambda; P)$ be a Rees Matrix Semigroup over a group G. Then $\mathcal{M}^0$ 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 $\alpha\mathcal{M}^0 \subseteq \beta\mathcal{M}^0$. We could have $\alpha = 0$. If $\alpha \neq 0$ then $\alpha\mathcal{M}^0 \neq \{0\}$ so $\beta \neq 0$ and we have $\alpha = (i, g, \lambda)$, $\beta = (j, h, \mu)$ and $\alpha = \beta\gamma$ for some $\gamma = (\ell, k, \nu)$. Then

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

This gives us that $i = j$ and so $\alpha \mathrel{\mathcal{R}} \beta$ and $\alpha\mathcal{M}^0 = \beta\mathcal{M}^0$.
Summarising, $0\mathcal{M}^0 \subset \alpha\mathcal{M}^0$ for all non-zero α. But if $\alpha \neq 0$ and $\alpha\mathcal{M}^0 \subseteq \beta\mathcal{M}^0$, then $\alpha\mathcal{M}^0 = \beta\mathcal{M}^0$. Hence $\mathcal{M}^0$ has M_R and M^R; dually $\mathcal{M}^0$ has M_L and M^L. □

Definition 7.10. 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 7.11 (The $\mathcal{D} = \mathcal{J}$ Theorem)**.** *Suppose*

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

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

Example 7.12.

1. If S is a band, $a = a^2$ for all $a \in S$ and so $(\star)$ holds.
2. Let S be a semigroup having M_L and let $a \in S$. Then
$$S^1a \supseteq S^1a^2 \supseteq S^1a^3 \supseteq \dots.$$
Since S has M_L, we have that this sequence stabilizes, so there exists $n \in \mathbb{N}$ such that $S^1a^n = S^1a^{n+1}$ which means that $a^n \mathrel{\mathcal{L}} a^{n+1}$. Similarly, if S has M_R, then for every $a \in S$ there exists $m \in \mathbb{N}$ such that $a^m \mathrel{\mathcal{R}} a^{m+1}$.

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

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

Then

$$b = xay = x(ubv)y = (xu)b(vy) = (xu)^2b(vy)^2 = \dots = (xu)^nb(vy)^n$$

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

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

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

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

So $S^1 b = S^1 ub$, which means that $b \mathcal{L} ub$. 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, $\mathcal{D} = \mathcal{J}$. □

As a consequence we have the following:

Corollary 7.13. *If a semigroup S has M_L and M_R, then it satisfies $(\star)$ and thus $\mathcal{D} = \mathcal{J}$.*

In the same vein we have:

Lemma 7.14. 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 $\mathcal{D} = \mathcal{J}$. Clearly if $a \mathcal{R} ab$ then $a \mathcal{D} ab$; as $\mathcal{R} \subseteq \mathcal{D}$.
Conversely, If $a \mathcal{J} ab$ then there exists $x, y \in S^1$ with

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

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

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

Now

$$aS^1 = abyS^1 \subseteq abS^1 \subseteq aS^1.$$

Hence $aS^1 = abS^1$ and $a \mathcal{R} ab$. □

7.1. Completely 0-simple semigroups

Let S have a 0. Recall that S is *0-simple* if and only if 0 (properly, $\{0\}$) and S are the only ideals and $S^2 \neq 0$. If in addition S has M_R and M_L, then S is *completely 0-simple*.

Lemma 7.15. *[0-Simple Lemma] Let S have a 0 and $S^2 \neq 0$. Then the following are equivalent:*

(i) *S is 0-simple,*
(ii) *$SaS = S$ for all $a \in S \setminus \{0\}$,*
(iii) *$S^1 a S^1 = S$ for all $a \in S \setminus \{0\}$,*

(iv) *the $\mathcal{J}$-classes are* $\{0\}$ *and* $S \setminus \{0\}$.

Proof. (i) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (iv) is a standard exercise.

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

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

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

(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 $SaS = S$. $\square$

Corollary 7.16. *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 by Corollary 5.7, 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 $e \neq 0$. $\square$

Theorem 7.17 (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 $S \cong \mathcal{M}^0(G; I; \Lambda; P)$ where G is a group, we know $\mathcal{M}^0$ is completely 0-simple (by Proposition 7.3, Rees Matrix facts and Example 7.9), hence S is completely 0-simple.

Conversely, suppose that 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 Corollary 7.16, D contains an idempotent $e = e^2$.

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 indexes 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 we can assume that both I and Λ contain a special symbol 1, and we can also assume that $e \in H_{11}$. Put $G = H_{11}$, which is a group.

For each $\lambda \in \Lambda$ let us choose and fix an arbitrary $q_\lambda \in H_{1\lambda}$ (take $q_1 = e$).
Similarly, for each $i \in I$ let $r_i \in H_{i1}$ (take $r_1 = e$).
Notice that

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

Thus, by Green's Lemma,

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

is a bijection. Now,

$$e = e^2, e \mathrel{\mathcal{L}} r_i \Rightarrow r_i e = r_i.$$

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. By the definition of ρ_{q_λ} and λ_{r_i}, we have that

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

for every $a \in G, i \in I$ and $\lambda \in \Lambda$.

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 $q_\lambda r_i \mathrel{\mathcal{D}} q_\lambda \mathrel{\mathcal{D}} r_i$. By the rectangular property

$$e \mathrel{\mathcal{R}} q_\lambda \mathrel{\mathcal{R}} q_\lambda r_i \mathrel{\mathcal{L}} r_i \mathrel{\mathcal{L}} e$$

so that $q_\lambda r_i \in G$.

$$\begin{array}{c|c|c|c|c|}
\multicolumn{1}{c}{} & \multicolumn{1}{c}{L_1} & \multicolumn{1}{c}{} & \multicolumn{1}{c}{L_\lambda} & \multicolumn{1}{c}{} \\ \cline{2-5}
R_1 & a & & q_\lambda & \\ \cline{2-5}
 & & & & \\ \cline{2-5}
R_i & r_i & & r_i a q_\lambda & \\ \cline{2-5}
 & & & & \\ \cline{2-5}
\end{array}$$

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 (Lemma 7.15) we have $Sr_iS = S$. So, $ur_iv \neq 0$ for some $u, v \in S$. Say, $u = r_kbq_\lambda$ for some k, λ and b. Then

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

as $r_kbq_\lambda r_iv \neq 0$. Therefore every column of P has a non-zero entry. Dually for rows. Therefore

$$\mathcal{M}^0 = \mathcal{M}^0(G; I; \Lambda; P)$$

is a Rees Matrix Semigroup over a group G. For any $x \in \mathcal{M}^0$ ($x = 0$ or x is 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), $(k, b, \mu) \in \mathcal{M}^0$ we have

$$\begin{aligned}
\big((i,a,\lambda)(k,b,\mu)\big)\theta &= \begin{cases} 0\theta & \text{if } p_{\lambda k} = 0, \\ (i, ap_{\lambda k}b, \mu)\theta & \text{if } p_{\lambda k} \neq 0, \end{cases} \\
&= \begin{cases} 0 & \text{if } p_{\lambda k} = 0, \\ r_iap_{\lambda k}bq_\mu & \text{if } p_{\lambda k} \neq 0, \end{cases} \\
&= r_iap_{\lambda k}bq_\mu, \\
&= r_iaq_\lambda r_kbq_\mu, \\
&= (i,a,\lambda)\theta(k,b,\mu)\theta.
\end{aligned}$$

Therefore θ is a morphism, and since it is bijective, it is an isomorphism. □

8. Regular Semigroups

Definition 8.1. We say that $a \in S$ is *regular* if $a = axa$ for some $x \in S$. The semigroup S is *regular* if every $a \in S$ is regular.

Examples of regular semigroups: any band, Rees matrix semigroups, groups.
Examples of non-regular semigroups: $(\mathbb{N}, +), (\mathbb{Z}, *)$
Nontrivial null (or zero) semigroups i.e. $S = X \cup \{0\}$ with $X \neq \emptyset$ and all products are 0.
Note that $(\mathbb{N}, +)$ has *no* regular element.

Definition 8.2. An element $a' \in S$ is an *inverse* of a if

$$a = aa'a \text{ and } a' = a'aa'.$$

We denote by $V(a)$ the set of inverses of a.

If G is a group then $V(a) = \{a^{-1}\}$ for all $a \in G$.

Caution: Inverses need not be unique. For example, in a rectangular band $T = I \times \Lambda$,

$$\begin{aligned}(i,j)(k,\ell)(i,j) &= (i,j)\\ (k,\ell)(i,j)(k,\ell) &= (k,\ell)\end{aligned}$$

for any (i,j) and (k,ℓ). So every element is an inverse of every other element.

Lemma 8.3. *If $a \in S$, then 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

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

and

$$\begin{aligned}a'aa' &= (xax)a(xax) = x(axa)(xax)\\ &= xa(xax) = x(axa)x = xax = a'.\end{aligned}$$

So $a' \in V(a)$. $\square$

Note. If $a = axa$ then

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

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

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

Definition 8.4. S is *inverse* if $|V(a)| = 1$ for all $a \in S$, i.e. every element has a unique inverse.

Example 8.5.

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).

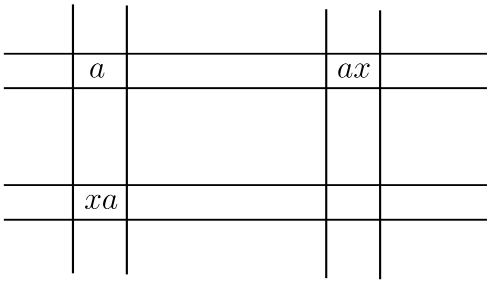


FIGURE 5. The egg box diagram of D_a.

(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 $(a,b) \in B$. Furthermore, B is inverse - see later.
(5) $\mathcal{M}^0$ is regular (see "Proposition 7.3, 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 8.6. *[Inverse Semigroup Theorem] A semigroup S is inverse iff S is regular and $E(S)$ is a semilattice (i.e. $ef = fe$ for all $e, f \in E(S)$).*

Proof. $(\Leftarrow)$ Let $a \in S$. As S is regular, a has an inverse by Lemma 8.3. 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. Let a' denote the *unique* inverse of $a \in S$.
Certainly S is regular. Let $e \in E(S)$. Then e is an inverse of e, because $e = eee$ and $e = eee$, so the inverse of any idempotent e is just itself: $e' = e$.

Let $e, f \in E(S)$. Let $x = (ef)'$. Consider the element 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:

$$\begin{aligned} ef(fxe)ef &= ef^2xe^2f = efxef = ef, \\ (fxe)ef(fxe) &= fxe^2f^2xe = f(xefx)e = fxe. \end{aligned}$$

Therefore we have $ef = (fxe)' = fxe \in E(S)$, so the product of any two idempotents is an idempotent. Therefore $E(S)$ is a band. Let $e, f \in E(S)$. Then

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

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

Example 8.7.

(1) Let B be the Bicyclic Semigroup. Then

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

and

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

where $t = \max\{a, b\}$. So $E(B)$ is commutative, and since B is regular, we have that it is inverse. Note that $(a, b)' = (b, a)$.

(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) If S is a band, then S is regular. Furthermore we have

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

(4) Let $\mathcal{M}^0 = \mathcal{M}^0(G; I, \Lambda; P)$. If $p_{\lambda i}, p_{\mu i}$ are both non-zero, then

$$(i, p_{\lambda i}^{-1}, \lambda), (i, p_{\mu i}^{-1}, \mu) \in E(\mathcal{M}^0)$$

and

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

if and only if $\lambda = \mu$. So for $\mathcal{M}^0$ to be inverse, for every $i \in I$ there must be *exactly* one $\lambda \in \Lambda$ with $p_{\lambda i} \neq 0$; dually for each $\kappa \in \Lambda$ there exists exactly one $j \in I$ with $p_{\kappa j} \neq 0$.

It is an *Exercise* to check that, conversely, if the above condition holds then $\mathcal{M}^0$ is inverse and isomorphic to a *Brandt* semigroup.

8.1. 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 8.8. *We have that*

(i) *If $a = axa$ then $ax, xa \in E(S)$ and $ax \, \mathcal{R} \, a \, \mathcal{L} \, xa$,*
(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 have already proven this.
(ii) If $b \, \mathcal{R} \, f$ then $fb = b$. Also, $f = bs$ for some $s \in S^1$. Therefore $b = fb = bsb$ and it follows that b is regular.
(iii) Dual to (ii).

□

From Lemma 8.8 an element $a \in S$ is regular if and only if it is $\mathcal{R}$-related to an idempotent. Dually, $a \in S$ is regular if and only if it is $\mathcal{L}$-related to an idempotent.

Lemma 8.9 (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 $c \in S$.

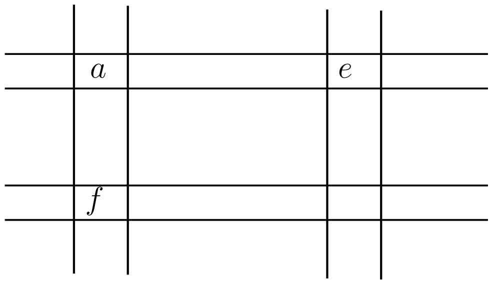
a		e		c	
				f	
				b	

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

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

Corollary 8.10. *[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

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

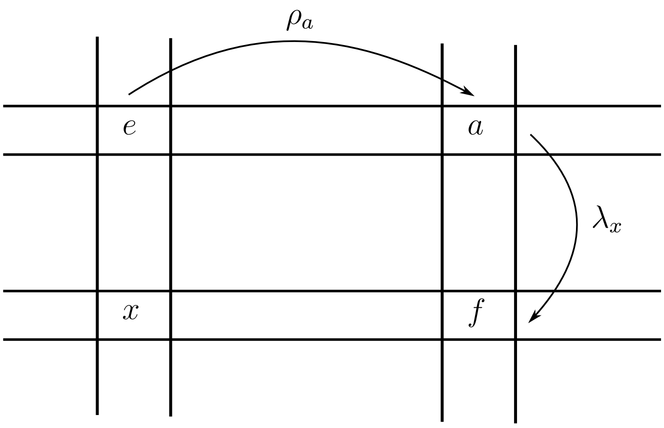
Also

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

So we have

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

We have $e \mathcal{R} a$ and $ea = a$ 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.
So we have the diagram



Let $h, k \in H_e$. 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 $H_e \cong H_f$. $\square$

It is worth noting that the previous proof also allows us to locate the inverses of a regular element.

Lemma 8.11. *If $a \in S$ is regular, and $x \in V(a)$, then there exist idempotents $e = ax$ and $f = xa$ such that*

$$a \,\mathcal{R}\, e \,\mathcal{L}\, x, \;\; a \,\mathcal{L}\, f \,\mathcal{R}\, x.$$

Conversely, if $a \in S$ and e, f are idempotents such that

$$a \,\mathcal{R}\, e, \;\; a \,\mathcal{L}\, f,$$

then there exists $x \in V(a)$ such that $ax = e$ and $xa = f$ (and then

$$e \,\mathcal{L}\, x, \;\; f \,\mathcal{R}\, x.)$$

a		$e = ax$
$f = xa$		x

Proof. For the first part, one just has to define $e = ax$ and $f = xa$. As we have seen, e and f are idempotents satisfying the required properties.
The converse follows directly from the proof of Corollary 8.10 (Corollary to Green's Lemmas). □

Example 8.12.

(1) For $\mathcal{M}^0 = \mathcal{M}^0(G; I; \Lambda; P)$ we know that $\mathcal{M}^0 \setminus \{0\}$ 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 $H_{i\lambda} \cong H_{j\mu}$ (already seen directly).

(2) The Bicyclic Monoid B is bisimple with $E(B) = \big\{(a, a) \mid a \in \mathbb{N}^0\big\}$ and $H_{(a,a)} = \big\{(a, a)\big\}$. 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 Corollary 8.10 , if $\varepsilon, \mu \in E(\mathcal{T}_n)$ and $\rho(\varepsilon) = \rho(\mu) = m$ say, then $H_\varepsilon \cong H_\mu$. In fact $H_\varepsilon \cong H_\mu \cong \mathcal{S}_m$.