SEMIGROUP THEORY

1. The Basic Concept

**Definition 1.1.** A *semigroup* is a pair \((S, \ast)\) where \(S\) is a non-empty set and \(\ast\) is an associative binary operation on \(S\). [i.e. \(\ast\) is a function \(S \times S \to S\) with \((a, b) \mapsto a \ast b\) and for all \(a, b, c \in S\) we have \(a \ast (b \ast c) = (a \ast b) \ast c\).]

<table>
<thead>
<tr>
<th>(n)</th>
<th>Semigroups</th>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>18</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>126</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>1160</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>15973</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>836021</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>1843120128</td>
<td>5</td>
</tr>
<tr>
<td>9</td>
<td>52989400714478</td>
<td>2</td>
</tr>
</tbody>
</table>

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

We abbreviate “\((S, \ast)\)” by “\(S\)” and often omit \(\ast\) in “\(a \ast b\)” and write “\(ab\)”. By induction \(a_1a_2\ldots a_n\) is unambiguous. Thus we write \(a^n\) for \(\underbrace{aa\ldots a}_{n \text{ times}}\).

**Index Laws** For all \(n, m \in \mathbb{N} = \{1, 2, \ldots\}\):

\[
a^n a^m = a^{n+m} \\
(a^n)^m = a^{nm}.
\]

**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 \(n, m \in \mathbb{N}^0 = \{0, 1, 2, \ldots\}\).

**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 \(b \in G\) with \(ab = 1 = ba\).
Example A 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

\[
\begin{array}{c|c}
  e & e \\
  e & e \\
\end{array}
\]

is also called the trivial semigroup or trivial monoid.

Example B A ring is a semigroup under \( \times \). If the ring has an identity then this semigroup is a monoid.

Example C \( \mathbb{N} \) is a monoid under \( \times \).

\( \mathbb{N} \) is a semigroup under \( + \).

\( \mathbb{N}^0 \) is a monoid under \( + \) and \( \times \).

Example D Let \( I, J \) be non-empty sets and set \( T = I \times J \) with the binary operation

\[(i, j)(k, \ell) = (i, \ell).
\]

Note

\[
((i, j)(k, \ell))(m, n) = (i, \ell)(m, n) = (i, n),
\]

\[(i, j)((k, \ell)(m, n)) = (i, j)(k, n) = (i, n),
\]

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, which is \textit{not} a monoid. Find a symbol not in $S$, call it "1". On $S \cup \{1\}$ we define $\ast$ by

\[
a \ast b = ab \quad \text{for all } a, b \in S,
\]
\[
a \ast 1 = a = 1 \ast a \quad \text{for all } a \in S,
\]
\[
1 \ast 1 = 1.
\]

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

For an arbitrary semigroup $S$ the monoid $S^1$ is defined by

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

$S^1$ is “$S$ with a 1 adjoined if necessary”.

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

\[
\begin{array}{c|ccc}
 & 1 & (a, b) & (a, c) \\
\hline
1 & 1 & (a, b) & (a, c) \\
(a, b) & (a, b) & (a, b) & (a, c) \\
(a, c) & (a, c) & (a, b) & (a, c)
\end{array}
\]
Example E: 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.

\[
\max\{a, b\} = \begin{cases} 
a & \text{if } a \geq b, 
b & \text{if } b \geq a.
\end{cases}
\]

We note some further things about $\max$:

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

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 $a, b, c \in \mathbb{Z}$

\[
(*) \quad \begin{align*}
a + \max\{b, c\} &= \max\{a + b, a + c\}, \\
\max\{b, c\} &= a + \max\{b - a, c - a\}.
\end{align*}
\]

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

**Proof.** With $(a, b), (c, d) \in B$ and $t = \max\{b, c\}$ we have $t - b \geq 0$ and $t - c \geq 0$. Thus we have $a - b + t \geq a$ and $d - c + t \geq d$. 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

\[
(0, 0)(a, b) = (0 - 0 + \max\{0, a\}, b - a + \max\{0, a\}) = (0 - 0 + a, b - a + a) = (a, b) = (a, b)(0, 0).
\]

Therefore $(0, 0)$ is the identity of $B$.

We need to verify associativity.

Let $(a, b), (c, d), (e, f) \in B$. Then
\[(a, b)(c, d)(e, f) = (a - b + \max\{b, c\}, d - c + \max\{b, c\})(e, f),\]
\[= (a - b - d + c + \max\{d - c + \max\{b, c\}, e\},\]
\[f - e + \max\{d - c + \max\{b, c\}, e\}).\]

\[(a, b)((c, d)(e, f)) = (a, b)(c - d + \max\{d, e\}, f - e + \max\{d, e\}),\]
\[= (a - b + \max\{b, c - d + \max\{d, e\}\})\]
\[f - e - c + d + \max\{b, c - d + \max\{d, e\}\}).\]

Now we have to show that
\[a - \bar{b} - d + c + \max\{d - c + \max\{b, c\}, e\} = a - \bar{b} + \max\{b, c - d + \max\{d, e\}\},\]
\[f - \bar{c} + \max\{d - c + \max\{b, c\}, e\} = f - \bar{c} - c + d + \max\{b, c - d + \max\{d, e\}\}.

We can see that these equations are the same and so we only need to show
\[c - d + \max\{d - c + \max\{b, c\}, e\} = \max\{b, c - d + \max\{d, e\}\}.

Now, we have from \((*)\) that this is equivalent to
\[\max\{\max\{b, c\}, c - d + e\} = \max\{b, c - d + \max\{d, e\}\}.

The RHS of this equation is
\[\max\{b, c - d + \max\{d, e\}\} = \max\{b, \max\{c - d + d, c - d + e\}\},\]
\[= \max\{b, {c - d + e}\},\]
\[= \max\{b, c - d + \max\{d, e\}\}.

Therefore multiplication is associative and hence \(B\) is a monoid. \(\square\)

\(B\) is called the \textit{Bicyclic Semigroup/Monoid}.

\textbf{Examples} \(\mathcal{T}_X\) is a semigroup. (See Examples class).

\textbf{Definition 1.5.} A semigroup \(S\) is \textit{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 1.6. A semigroup is *cancellative* if

\[ ac = bc \Rightarrow a = b, \quad \text{and} \quad ca = cb \Rightarrow a = b. \]

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 1.7. A zero “0” of a semigroup \( S \) is an element such that, for all \( a \in S \),

\[ 0a = 0 = a0. \]

Adjoining a Zero Let \( S \) be a semigroup, then pick a new symbol “0”. Let \( S^0 = S \cup \{0\} \); define a binary operation \( \cdot \) on \( S^0 \) by

\[ a \cdot b = ab \quad \text{for all} \quad a \in S, \]

\[ 0 \cdot a = 0 = a \cdot 0 \quad \text{for all} \quad a \in S, \]

\[ 0 \cdot 0 = 0. \]

Then \( \cdot \) is associative, so \( S^0 \) is a semigroup with zero 0. We say that “\( S \) is a semigroup with a zero adjoined”.

**Example G** Let \( S \) be any set with a distinguished element \( z \in S \) and define an operation on \( S \) by \( a \cdot b = z \) for every \( a, b \in S \). Then \( (S, \cdot) \) is a semigroup with zero \( z \), and we call it a zero semigroup.

**Example H** Let \( G \) be a group and define a binary operation on \( \mathcal{P}(G) \) (that is, the set of all subsets of \( G \)) by \( A \cdot B = \{ab : a \in A, b \in B\} \). Then \( (\mathcal{P}(G), \cdot) \) is a semigroup. It has both a zero and an identity.

**Example I** Let \( X \) be a nonempty set. A *word* is a finite (possibly empty) sequence of elements of \( X \). The empty word is denoted by \( \epsilon \). We define

\[ X^* = \{w : w \text{ is a word over } X\}. \]

Multiplication on \( X^* \) is just concatenation, for example if \( X = \{a, b, c\} \) then

\[ abac \cdot bac = abacbac. \]

Then \( (X^*, \cdot) \) is a monoid with identity \( \epsilon \).
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 2.1.**
1. $(\mathbb{N}, +)$ is a subsemigroup of $(\mathbb{Z}, +)$.
2. $R = \{c_x \mid x \in X\}$ is a subsemigroup of $T_X$, since $c_xc_y = c_y$ for all $x, y \in X$.

Then $R$ 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

$$(a, a)(b, b) = (a - a + t, b - b + t) \quad \text{where } t = \max\{a, b\},$$

$$= (t, t),$$

$$= (b, b)(a, a).$$

**Definition 2.2.** Let $(A, \cdot), (B, *)$ be semigroups. Then on the cartesian product $A \times B$ we define an operation by

$$(a, b) \cdot (a', b') = (a \cdot a', b * b').$$

Then $(A \times B, \cdot)$ is a semigroup which is called the direct product of $A$ by $B$.

**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 $\theta$ is a monoid (homo)morphism if $\theta$ is a semigroup morphism and $1_S \theta = 1_T$.

**Example 2.2.**
1. $\theta : B \to \mathbb{Z}$ given by $(a, b)\theta = a - b$ is a monoid morphism because

$$((a, b)(c, d))\theta = (a - b + t, d - c + t)\theta \quad \text{where } t = \max\{b, c\}$$

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

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

$$= (a, b)\theta + (c, d)\theta.$$
Furthermore \((0,0)\theta = 0 - 0 = 0\).

(2) Let \(T = I \times J\) be the rectangular band then define \(\alpha : T \to T_J\) by \((i,j)\alpha = c_j\). Then we have

\[
(i,j)(k,\ell)\alpha = (i,\ell)\alpha,
\]

\[
= c_{\ell},
\]

\[
= c_jc_{\ell},
\]

\[
= (i,j)\alpha(k,\ell)\alpha.
\]

So, \(\alpha\) is a morphism.

**Definition 2.4.** 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 \(\text{Im} \ \alpha\) is a subsemigroup (submonoid) of \(T\). If \(\alpha\) 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 2.5 (The “Cayley Theorem” – for Semigroups).** Let \(S\) be a semigroup. Then \(S\) is embedded in \(T_{S^1}\).

**Proof.** Let \(S\) be a semigroup and set \(X = S^1\). We need a 1:1 morphism \(S \to T_X\).

For \(s \in S\), we define \(\rho_s \in T_X\) by \(x\rho_s = xs\).

Now define \(\alpha : S \to T_X\) by \(s\alpha = \rho_s\).

\(\alpha\) is 1:1 If \(sa = ta\) 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 \(\alpha\) is 1:1.

\(\alpha\) 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 \(\alpha\) is a morphism. Hence \(\alpha : S \to T_X\) is an embedding. \(\square\)
Theorem 2.6 (The “Cayley Theorem” - for Monoids). Let $S$ be a monoid. Then there exists an embedding $S \hookrightarrow T_S$.

Proof. $S^1 = S$ so $T_S = T_{S^1}$. We know $\alpha$ 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 2.7 (The Cayley Theorem - for Groups). Let $S$ be a group. Then there exists an embedding $S \hookrightarrow S_S$.

Proof. Exercise. □

2.1. Idempotents

$S$ will always denote a semigroup.

Definition 2.8. $e \in S$ 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. $E(S) = \emptyset$ (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

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

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 2.9. If $E(S) = S$, then $S$ is a band.

Definition 2.10. If $E(S) = S$ and $S$ is commutative, then $S$ is a semilattice.

Lemma 2.11. Suppose $ef = fe$ for all $f, e \in E(S)$. Then $E(S) = \emptyset$ or $E(S)$ is a subsemigroup.

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

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

and hence $ef \in E(S)$. □

From Lemma 2.11 if $E(S) \neq \emptyset$ and idempotents in $S$ commute then $E(S)$ is a semilattice.
Example 2.3. (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 $(i, j)(k, \ell) = (k, \ell)(i, j) \iff i = k$ and $j = \ell$.

Definition 2.12. 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 2.13. 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 $s, t \in \mathbb{N}^0$,

$a^{n+s} = a^{n+t} \iff s \equiv t \pmod{r}$.

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 $a^n = a^{n+r}$. Hence

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

We can express this pictorially:

We have $a^n = a^{n+r}$: DO NOT CANCEL

Let $s, t \in \mathbb{N}^0$ with

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

with

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

We have $a^n = a^{n+r}$: DO NOT CANCEL

Let $s, t \in \mathbb{N}^0$ with

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

with

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

We have $a^n = a^{n+r}$: DO NOT CANCEL

Let $s, t \in \mathbb{N}^0$ with

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

with

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

We have $a^n = a^{n+r}$: DO NOT CANCEL

Let $s, t \in \mathbb{N}^0$ with

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

with

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

We have $a^n = a^{n+r}$: DO NOT CANCEL

Let $s, t \in \mathbb{N}^0$ with

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

with

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

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 $a^n = a^{n+r}$. Hence

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

We can express this pictorially:
Then
\[ a^{n+s} = a^{n+s'+ur} = a^{s'}a^{n+ur} \text{ in } S^1 = a^{s'}a^{n+r}(u-1)r = a^{s'}a^{n+(u-1)r} = \ldots = a^{s'}a^n = a^{n+s}. \]

Similarly, \( a^{n+t} = a^{n+t'} \). Therefore
\[ a^{n+s} = a^{n+t} \iff a^{n+s'} = a^{n+t'} \iff s' = t' \iff s \equiv t \pmod{r}. \]

Notice that
\[ a^{n+ur} = a^n \]
for all \( u \).

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).

**Lemma 2.14** (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 \( a^{n+s} \in E(S) \).

In fact, \( \{a^n, a^{n+1}, \ldots, a^{n+r-1}\} \) is a group with identity \( a^{n+s} \).

**Corollary 2.15.** Any finite semigroup contains an idempotent.
2.2. Idempotents in $T_X$

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 $c_x \in E(T_X)$ for all $x \in X$. But if $|X| > 1$ then there are other idempotents in $T_X$ as well.

**Example 2.4.** Let us define an element

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

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 $\alpha$ is an idempotent.

**Definition 2.16.** Let $\alpha: X \to Y$ be a map and let $Z \subseteq X$. Then the *restriction of $\alpha$ to the set $Z$* is the map

$$\alpha|_Z: Z \to Y, z \mapsto z\alpha$$

for every $z \in Z$.

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

**Example 2.5.** 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 $\alpha$ is not one-to-one but $\alpha|_{\{a, d\}}$ is.

Let $\alpha \in T_X$ (i.e. $\alpha: X \to X$). Recall that $\text{Im} \alpha = \{x\alpha : x \in X\} \subseteq X = X\alpha$.

**Example 2.6.** In $T_3$ we have $\text{Im} \ c_1 = \{1\}$, $\text{Im} \ I_3 = \{1, 2, 3\}$ and

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

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

**Lemma 2.17 (The $E(T_X)$ Lemma).** An element $\varepsilon \in T_X$ is idempotent $\iff \varepsilon|_{\text{Im} \varepsilon} = I_{\text{Im} \varepsilon}$.

**Proof.** $\varepsilon|_{\text{Im} \varepsilon} = I_{\text{Im} \varepsilon}$ means that for all $y \in \text{Im} \varepsilon$ we have $y\varepsilon = y$. Of course, for every $x \in X$ we have $x\varepsilon \in \text{Im} \varepsilon$. Then
\( \varepsilon \in E(T_X) \iff \varepsilon^2 = \varepsilon, \)
\( \iff x\varepsilon^2 = x\varepsilon \quad \text{for all } x \in X, \)
\( \iff (x\varepsilon)\varepsilon = x\varepsilon \quad \text{for all } x \in X, \)
\( \iff y\varepsilon = y \quad \text{for all } y \in \text{Im } \varepsilon, \)
\( \iff \varepsilon|_{\text{Im } \varepsilon} = I_{\text{Im } \varepsilon}. \)

**Example 2.7.** Let
\[ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix} \in T_3, \]
this has image \( \text{Im } \alpha = \{2, 3\}. \) Now we can see that \( 2\alpha = 2 \) and \( 3\alpha = 3. \) Hence \( \alpha \in E(T_3). \)

**Example 2.8.** We can similarly create another idempotent in \( T_7, \) 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:
\[ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 5 & 7 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 5 & 7 & 5 & 2 & 7 \end{pmatrix} \in E(T_7). \]

Using Lemma 2.17 we can now list all the idempotents in \( T_3. \) We start with the constant maps, i.e. \( \varepsilon \in E(T_3) \) such that \( |\text{Im } \varepsilon| = 1. \) 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 \( \varepsilon \in E(T_3) \) such that \( |\text{Im } \varepsilon| = 2. \) These are
\[ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 2 \end{pmatrix}. \]

Now there is only one idempotent such that \( |\text{Im } \varepsilon| = 3, \) that is the identity map
\[ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}. \]

### 3. 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 \( \rho \) 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 \( \leq \) on \( \mathbb{R} \):

- \( a \leq a \) for all \( a \in \mathbb{R} \),
- \( a \leq b \) and \( b \leq c \) \( \Rightarrow \) \( a \leq c \) for all \( a, b, c \in \mathbb{R} \),
- \( a \leq b \) and \( b \leq a \) \( \Rightarrow \) \( a = b \) for all \( a, b \in \mathbb{R} \),
- \( a \leq b \) or \( b \leq a \) for all \( a, b \in \mathbb{R} \).

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

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 \( X \):

- \( A \subseteq A \) for all \( A \in \mathcal{P}(X) \),
- \( A \subseteq B \) and \( B \subseteq C \) \( \Rightarrow \) \( A \subseteq C \) for all \( A, B, C \in \mathcal{P}(X) \),
- \( A \subseteq B \) and \( B \subseteq A \) \( \Rightarrow \) \( A = B \) for all \( A, B \in \mathcal{P}(X) \).

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 not a total order on \( \mathcal{P}(X) \).

We denote by \( \omega \) 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 \( \iota \) be the EQUALITY relation on \( A \):

\[
\iota = \{(a, a) \mid a \in A\}.
\]

Thus \( x \iota y \iff x = y \) and so \( \{x\} = \{x\} \) for all \( x \in A \).

### 3.2. Algebra of Relations

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

\[
a (\rho \cap \lambda) b \iff (a, b) \in (\rho \cap \lambda) \\
\iff (a, b) \in \rho \text{ and } (a, b) \in \lambda \\
\iff a \rho b \text{ and } a \lambda b.
\]

We note that \( \rho \subseteq \lambda \) means \( a \rho b \Rightarrow a \lambda b \). Note that \( \iota \subseteq \rho \iff \rho \) is reflexive and so \( \iota \subseteq \rho \) for any equivalence relation \( \rho \). We see that \( \iota \) is the smallest equivalence relation on \( A \) and \( \omega \) is the largest equivalence relation on \( A \). Recall that

\[
[a] = \{b \in A \mid a \rho b\}.
\]
If \( \rho \) is an equivalence relation then \([a]\) is the equivalence-class, or the \(\rho\)-class, of \(a\).

**Lemma 3.2.** If \(\rho, \lambda\) 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 \(\rho, \lambda\) 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 \(\rho\)-class of \(a\) and \([a]_{\lambda}\) the \(\lambda\)-class of \(a\) we have that,

\[
[a]_{\rho \cap \lambda} = \{ b \in A | b (\rho \cap \lambda) a \},
= \{ b \in A | b \rho a \text{ and } b \lambda a \},
= \{ b \in A | b \rho a \} \cap \{ b \in A | b \lambda a \},
= [a]_{\rho} \cap [a]_{\lambda}.
\]

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

\[
3 \equiv 1 \pmod{2},
1 \equiv 4 \pmod{3}.
\]

If \((\equiv (\bmod 2)) \cup (\equiv (\bmod 3))\) were to be transitive then we would have

\[
(3, 1) \in (\equiv (\bmod 2)) \cup (\equiv (\bmod 3)) \implies (3, 4) \in (\equiv (\bmod 2)) \cup (\equiv (\bmod 3)) \implies 3 \equiv 4 \pmod{2} \text{ or } 3 \equiv 4 \pmod{3}
\]

but this is a contradiction!

### 3.3. Kernels

**Definition 3.3.** Let \(\alpha : X \to Y\) be a map. Define a relation \(\ker \alpha\) on \(X\) by the rule

\[a \ker \alpha b \iff a\alpha = b\alpha.\]

We call \(\ker \alpha\) the *kernel of \(\alpha\).*

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

**Example 3.1.** Let \(\alpha : \{1, 2, 3, 4, 5, 6\} \to \{1, 2, 3, 4, 5, 6\}\) 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 $\alpha : A \to B$ is a map then $\alpha$ is one-one if and only if $\ker \alpha = \iota_A$ and $\alpha$ is constant if and only if $\ker \alpha = \omega_A$.

**Definition 3.4.** An equivalence relation $\rho$ on a semigroup $S$ is a **congruence** if

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

**Lemma 3.5** (The Kernel Lemma). Let $\theta : S \to T$ be a semigroup morphism. Then $\ker \theta$ is a congruence on $S$.

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

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

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

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

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

**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:

$\alpha : \mathbb{N} \to \mathbb{Z}$, $n\alpha =$ 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 $\rho$ 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 $\rho$ is $X = \{A, B, C, D\}$. We try do define a map from $X$ to $\mathbb{N}$ by

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

What is the image of $A$ under $\alpha$? 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 ‘$\alpha$ 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

$\beta : X \to \mathbb{N}^0, [n]_{\rho} \beta = \pi$,
where \( \pi \) denotes the remainder of \( n \) on division by 4 (that is, 0, 1, 2 or 3). In this case \( \beta \) 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 \( \rho \) be a congruence on \( S \). Then we define

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

Define a binary operation on \( S/\rho \) 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 \( \rho \) 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

\[
[a](b[c]) = [a][bc],
\]

\[
= [a(bc)],
\]

\[
= [(ab)c],
\]

\[
= [ab][c],
\]

\[
= ([a][b])[c].
\]

If \( S \) is a monoid, then so is \( S/\rho \) because we have

\[
[1][a] = [1a] = [a] = [a1] = [a][1]
\]

for any \( a \in S \). Hence we conclude that \( S/\rho \) is a semigroup and if \( S \) is a monoid, then so is \( S/\rho \).

**Definition 3.6.** We call \( S/\rho \) the factor semigroup (or monoid) of \( S \) by \( \rho \).

Now, define \( \nu_{\rho} : S \to S/\rho \) by

\[
s\nu_{\rho} = [s].
\]

Then we have

\[
s\nu_{\rho}t\nu_{\rho} = [s][t] \quad \text{definition of } \nu_{\rho},
\]

\[
= [st] \quad \text{definition of multiplication in } S/\rho,
\]

\[
= (st)\nu_{\rho} \quad \text{definition of } \nu_{\rho}.
\]
Hence $\nu_\rho$ is a semigroup morphism. We now want to examine the kernel of $\nu_\rho$ and so

\[
\begin{align*}
 s \ker \nu_\rho t & \iff s \nu_\rho = t \nu_\rho \\
 & \iff [s] = [t] \\
 & \iff s \rho t
\end{align*}
\]

definition of $\ker \nu_\rho$, definition of $\nu_\rho$, definition of $\rho$.

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

**Theorem 3.7** (The Fundamental Theorem of Morphisms for Semigroups). Let $\theta : S \to T$ be a semigroup morphism. Then $\ker \theta$ is a congruence on $S$, $\text{Im} \theta$ is a subsemigroup of $T$ and $S / \ker \theta \cong \text{Im} \theta$.

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

\[
\begin{align*}
[a] = [b] & \iff a \theta b \\
 & \iff a \theta = b \theta \\
 & \iff [a] \bar{\theta} = [b] \bar{\theta}.
\end{align*}
\]

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

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

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

Ideals play an important role in semigroup theory, but a bit different role than they do in ring theory. The reason is that in case of rings, ALL homomorphisms are determined by ideals, but in case of semigroups, this is not so.

4.1. Notation

If \( A, B \subseteq S \) then we write

\[
AB = \{ab \mid a \in A, b \in B\},
\]

\[
A^2 = AA = \{ab \mid a, b \in A\}.
\]

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 \( \mathcal{P}(A) \).

Definition 4.1. Let \( \emptyset \neq I \subseteq S \) then \( I \) is a right ideal if \( IS \subseteq I \) (i.e. \( a \in I, s \in S \Rightarrow as \in I \)). We say \( I \) is a left ideal if \( SI \subseteq I \). Finally \( I \) is a (two sided) ideal if \( IS \cup SI \subseteq I \).

Note that any (left/right) ideal is a subsemigroup. If \( S \) is commutative, all 3 concepts coincide.

Example 4.1. Some examples of ideals.

1. Let \( i \in I \) then \( \{i\} \times J \) is a right ideal in a rectangular band \( I \times J \).
2. Let \( m \in \mathbb{N}^0 \) be fixed. Then \( I_m = \{(x, y) \mid x \geq m, y \in \mathbb{N}^0\} \) 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 \( \{\alpha \in \mathcal{T}_X \mid \text{Im} \alpha \subseteq Y\} \) is a left ideal of \( \mathcal{T}_X \).
(4) For any \( n \in \mathbb{N} \) we define

\[ S^n = \{ a_1a_2 \ldots a_n \mid a_i \in S \}. \]

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

\[ s = s \underbrace{1 \ldots 1}_{n-1} \in S^n. \]

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

**Definition 4.2.** 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).

**Example 4.2.** Let \( G \) be a group and \( I \) a left ideal. Let \( g \in G, a \in I \) then we have

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

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

**Exercise:** \( G^0 \) is 0-simple

**Example 4.3.** We have \( (\mathbb{N}, +) \) is a semigroup. Let \( n \in \mathbb{N} \). Now define \( I_n \subseteq (\mathbb{N}, +) \) to be

\[ I_n = \{ n, n + 1, n + 2, \ldots \}, \]

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

**Note.** \( \{2, 4, 6, \ldots \} \) is a subsemigroup but not an ideal.

**Example 4.4.** The bicyclic semigroup \( B \) is simple.

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

\[ (a, b) = (a, b)(0, 0) \in I \]

and hence \( B = I \Rightarrow B \) is simple. \( \square \)
4.2. Principal Ideals

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

\[
S^1 A = \{ sa \mid s \in S^1, a \in A \},
\]

\[
= \{ sa \mid s \in S \cup \{1\}, a \in A \},
\]

\[
= \{ sa \mid s \in S, a \in A \} \cup \{ 1a \mid a \in A \},
\]

\[
= SA \cup A.
\]

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

\[
S^1 a = Sa \iff a \in Sa,
\]

\[
\iff a = ta
\]

for some $t \in S$. We have $S^1 a = Sa$ 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 $1 \not\in 1 + \mathbb{N}$. Dually,

\[
aS^1 = aS \cup \{ a \}
\]

and similarly

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

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

**Claim.** $aS^1$ is the “smallest” right ideal containing $a$.

**Proof.** 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 $aS^1 \subseteq IS^1 = I \cup IS \subseteq I$. \qed

**Definition 4.3.** We call $aS^1$ the principal right ideal generated by $a$. Similarly, $S^1 a$ is the principal left ideal generated by $a$. The ideal $S^1 aS^1$ is the smallest ideal containing $a$ – it is called the principal ideal generated by $a$.

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

**Example 4.5.** In a group $G$ we have

\[
aG^1 = G = G^1 a = G^1 aG^1
\]

for all $a \in G$.

**Example 4.6.** In $\mathbb{N}$ under addition we have

\[
n + \mathbb{N}^1 = I_n = \{ n, n + 1, n + 2, \ldots \}
\]
Example 4.7. $B$ is simple, so

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

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

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

**Proof.** We have

$$(m, n)B = \{(m, n)(u, v) \mid (u, v) \in B\} \subseteq \{(x, y) \mid x \geq m, y \in \mathbb{N}^0\}.$$

Let $x \geq m$ then

$$(m, n)(n + (x - m), y) = (m - n + n + (x - m), y),$$

$$= (x, y).$$

Therefore $(x, y) \in (m, n)B \Rightarrow \{(x, y) \mid x \geq m, y \in \mathbb{N}^0\} \subseteq (m, n)B$. Hence we have proved our claim. \[ \square \]

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

**Lemma 4.4** (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 (i) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i) and so we prove (i) $\iff$ (ii).

(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 $S^1a \subseteq S^1b$. \[ \square \]

**Lemma 4.5** (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 $aS \subseteq bS \iff a \in bS \iff a = bt$ for some $t \in S$.

The following relation is crucial in semigroup theory.
**Definition 4.6.** The relation $L$ on a semigroup $S$ is defined by the rule

$$a \ L \ b \iff S^1a = S^1b$$

for any $a, b \in S$.

**Definition 4.7.** If $\alpha$ is a relation on a semigroup $S$ then we say that $\alpha$ is **left compatible** if for every $a, b, c \in S$, if $a \alpha b$ then $ca \alpha cb$. Similarly we define right compatible relations. A left (right) compatible equivalence relation is a **left (right) congruence**.

**Note.**

1. $L$ is an equivalence.
2. If $a \ L \ b$ and $c \in S$ then $S^1a = S^1b$, so $S^1 ac = S^1bc$ and hence $ac \ L \ bc$, that is, $L$ is a right compatible equivalence, so it is a right congruence.

**Corollary 4.8.** We have that

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

**Proof.** We start with $a \ L \ b$

$$a \ L \ b \iff S^1a = S^1b$$

$$\iff S^1a \subseteq S^1b \text{ and } S^1b \subseteq S^1a$$

$$\iff \exists s, t \in S^1 \text{ with } a = sb, b = ta$$

by the Principal Left Ideal Lemma. We note that this statement about $L$ can be used as a definition of $L$. \qed

**Remark.**

1. $a \ L \ b \iff a = b$ or there exist $s, t \in S$ with $a = sb, b = ta$.
2. If $Sa = S^1a$ and $Sb = S^1b$, then $a \ L \ b \iff \exists s, t \in S$ with $a = sb, b = ta$.

Dually, the relation $R$ is defined on $S$ by

$$a \ R \ b \iff aS^1 = bS^1,$$

$$\iff \exists s, t \in S^1 \text{ with } a = bs \text{ and } b = at,$$

$$\iff a = b \text{ or } \exists s, t \in S \text{ with } a = bs \text{ and } b = at.$$  

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

**Definition 4.9.** We define the relation $H = L \cap R$ and note that $H$ is an equivalence.

The relations $L, R, H$ are in fact three of the so-called **Greens’ relations**.
Example 4.8. If $S$ is commutative, $\mathcal{L} = \mathcal{R} = \mathcal{H}$. In a group $G$,

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

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

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

\[
a + \mathbb{N}^1 = \{a, a + 1, \ldots\}
\]

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

Example 4.10. In $B$ we know

\[
(m, n)B^1 = \{(x, y) \mid x \geq m, y \in \mathbb{N}^0\}
\]

and so we have

\[
(m, n)B^1 = (p, q)B^1 \iff m = p.
\]

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

\[
(m, n) \mathcal{L} (p, q) \iff n = q.
\]

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

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

Claim. $\alpha\mathcal{T}_X \subseteq \beta\mathcal{T}_X \iff \ker \beta \subseteq \ker \alpha$. [Recall $\ker \alpha = \{(x, y) \in X \times X \mid x\alpha = y\alpha\}$].

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 $\gamma: X \to X$ by $z\gamma = z$ if $z \notin \text{Im} \beta$. Otherwise $z = x\beta$ for some $x \in X$, so let

\[
z\gamma = (x\beta)\gamma = x\alpha
\]
If \( z = x\beta = y\beta \), then \( (x, y) \in \ker \beta \subseteq \ker \alpha \) so \( x\alpha = y\alpha \). Hence \( \gamma \) 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, \( \alpha\mathcal{T}_X \subseteq \beta\mathcal{T}_X \). \( \square \)

**Corollary 4.10** (\( \mathcal{R} - \mathcal{T}_X \)-Lemma). \( \alpha \mathcal{R} \beta \iff \ker \alpha = \ker \beta \).

**Proof.** We have

\[
\alpha \mathcal{R} \beta \iff \alpha\mathcal{T}_X = \beta\mathcal{T}_X \\
\iff \alpha\mathcal{T}_X \subseteq \beta\mathcal{T}_X \quad \text{and} \quad \beta\mathcal{T}_X \subseteq \alpha\mathcal{T}_X \\
\iff \ker \beta \subseteq \ker \alpha \quad \text{and} \quad \ker \alpha \subseteq \ker \beta \\
\iff \ker \alpha = \ker \beta.
\]

\( \square \)

**FACT:** \( \mathcal{T}_X \alpha \subseteq \mathcal{T}_X \beta \iff \text{Im} \alpha \subseteq \text{Im} \beta \) (Exercise 4).

**Corollary 4.11** (\( \mathcal{L} - \mathcal{T}_X \)-Lemma). \( \alpha \mathcal{L} \beta \iff \text{Im} \alpha = \text{Im} \beta \).

Consequently \( \alpha \mathcal{H} \beta \iff \ker \alpha = \ker \beta \) and \( \text{Im} \alpha = \text{Im} \beta \).

**Example 4.11.** Let us define

\[
\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix} \in E(T_3)
\]

Now we have \( \text{Im} \varepsilon = \{2, 3\} \). We can see that \( \ker \varepsilon \) has classes \( \{1, 2\}, \{3\} \). So

\[
\alpha \mathcal{H} \varepsilon \iff \text{Im} \alpha = \text{Im} \varepsilon \quad \text{and} \quad \ker \alpha = \ker \varepsilon \\
\iff \text{Im} \alpha = \{2, 3\} \quad \text{and} \quad \ker \alpha \text{ has classes } \{1, 2\}, \{3\}.
\]

So we have

\[
\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 2 \end{pmatrix} \quad \text{or} \quad \alpha = \varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix}
\]

\[
\begin{array}{ccc}
\varepsilon & \alpha \\
\varepsilon & \varepsilon & \alpha \\
\alpha & \alpha & \varepsilon
\end{array}
\]

which is the table of a 2-element group. Thus the \( \mathcal{H} \)-class of \( \varepsilon \) is a group.
4.4. 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 $H$.

\[ e \]

**Figure 2.** $e$ is the only idempotent in $H$.

3. If $e \in E(S)$, then $\{e\}$ is a trivial subgroup.
4. $S_X$ is a subgroup of $T_X$; $\{\varepsilon, \alpha\}$ (as above) is a subgroup of $T_3$. Notice

\[ \alpha \mathcal{H} I_X \Leftrightarrow \text{Im } \alpha = \text{Im } I_X \text{ and } \ker \alpha = \ker I_X, \]
\[ \Leftrightarrow \text{Im } \alpha = X \text{ and } \ker \alpha = \iota, \]
\[ \Leftrightarrow \alpha \text{ is onto and } \alpha \text{ is one-one}, \]
\[ \Leftrightarrow \alpha \in S_X. \]

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

**Definition 4.12.** 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 $L_{(2,3)} = \{(x, 3) \mid x \in \mathbb{N}_0\}$.

4.5. Maximal Subgroup Theorem

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.

**Lemma 4.13** (Principal Ideal for Idempotents). Let $a \in S$, $e \in E(S)$. Then
Figure 3. Existence of a Maximal Subgroup.

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

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

\[ ae = (te)e = t(ee) = te = a. \]

\[ \square \]

Corollary 4.14. Let \( e \in E(S) \). Then we have

\[ a R e \Rightarrow ea = a, \]
\[ a L e \Rightarrow ae = a, \]
\[ a H e \Rightarrow a = ae = ea. \]

Thus, idempotents are left/right/two-sided identities for their \( R/L/H \)-classes.

Lemma 4.15. Let \( G \) be a subgroup with idempotent \( e \). Then \( G \subseteq H_e \), thus, the elements of \( G \) are all \( H \)-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

\[ \begin{align*}
    ea &= a \\
    aa^{-1} &= e
\end{align*} \]

\[ \Rightarrow a R e \]

\[ \begin{align*}
    ae &= a \\
    a^{-1}a &= e
\end{align*} \]

\[ \Rightarrow a L e \]

\[ \Rightarrow a H e. \]

Therefore \( a H e \) for all \( a \in G \), so \( G \subseteq H_e \). \[ \square \]
Theorem 4.16 (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 \( b \not\sim e \), so \( b \not\sim ae \) (\( \sim \) is left compatible) so \( ab \not\sim ae = a \not\sim e \). Also, \( a \not\sim eb = b \not\sim e \) hence \( ab \not\sim H_e \) so \( ab \not\in H_e \). 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 \( H_e = \mathcal{R} \cap \mathcal{L} \), there exist \( s, t \in S^1 \) with

\[
\begin{align*}
  at & = e = sa, \\
  e \cdot ee & = eee = a(ete) = (ese)a.
\end{align*}
\]

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

\[
\begin{align*}
  eb & = b \not\sim e, \\
  ba & = e \not\sim b, \\
  be & = b \not\sim ab = e
\end{align*}
\]

so \( b \not\sim H_e \), thus \( b \not\in H_e \). Hence \( H_e \) is indeed a subgroup. \( \Box \)

Let’s take 2 distinct idempotents \( e, f \in E(S) \) 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 4.17 (Green’s Theorem). If \( a \in S \), then \( a \) lies in a subgroup iff \( a \not\sim a^2 \).

Proof. See later. \( \Box \)

Corollary 4.18. Let \( a \in S \). Then the following are equivalent:

(i) \( a \) lies in a subgroup,
(ii) \( a \not\sim e \), for some \( e \in E(S) \),
(iii) \( H_a \) is a subgroup,
(iv) \( a \not\sim a^2 \).

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 \( a \not\sim H_e \).

(ii) \( \Rightarrow \) (iii): If \( a \not\sim e \), 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 \( a \not\sim a^2 \). \( \Box \)
Subgroups of $T_n$

We use Green’s Theorem to show the following.

**Claim.** Let $\alpha \in T_n$. Then $\alpha$ lies in a subgroup of $T_n \iff$ the map diagram has no tails of length $\geq 2$.

**Proof.** We have that $\alpha$ lies in a subgroup $\iff \alpha H \alpha^2 \iff \alpha L \alpha^2 \iff \alpha R \alpha^2 \iff \text{Im} \alpha = \text{Im} \alpha^2$, $\ker \alpha = \ker \alpha^2$. We know $\text{Im} \alpha^2 \subseteq \text{Im} \alpha$ (as $T_n \alpha^2 \subseteq T_n \alpha$). Let $\rho$ be an equivalence on a set $X$. Let $X = \{1, 2, \ldots, n\} = \mathbb{Z}$. Put

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

We have seen that

$$|X/\ker \alpha| = |\text{Im} \alpha|.$$

**Claim.** For $\alpha \in T_n$, $\text{Im} \alpha = \text{Im} \alpha^2 \Rightarrow \ker \alpha = \ker \alpha^2$.

**Proof.** We know that $\ker \alpha \subseteq \ker \alpha^2$ ($\alpha T_n \subseteq \alpha^2 T_n$), which means that the $\ker \alpha^2$-classes are just unions of $\ker \alpha$-classes:

![Figure 4. The classes of $\ker \alpha$ and $\ker \alpha^2$.](image)

Suppose now that $\text{Im} \alpha = \text{Im} \alpha^2$. Then

$$|\text{Im} \alpha^2| = \left|\frac{n}{\ker \alpha^2}\right| \leq \left|\frac{n}{\ker \alpha}\right| = |\text{Im} \alpha|,$$

thus $\ker \alpha$ and $\ker \alpha^2$ have the same number of classes. Hence $\ker \alpha = \ker \alpha^2$. $\square$

As a consequence we have that $\alpha$ lies in a subgroup $\iff \text{Im} \alpha = \text{Im} \alpha^2$. Note that elements of $\text{Im} \alpha \setminus \text{Im} \alpha^2$ are exactly those second vertices of tails in the map diagram of $\alpha$ which are not members of a cycle. Thus, $\text{Im} \alpha^2 = \text{Im} \alpha$ 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 $T_n$ looks like:

\[ \alpha \rightarrow \alpha \]

\[ \in \text{Im } \alpha \setminus \text{Im } \alpha^2 \]

Example 4.12.

(1) We take an element of $T_5$ to be

\[ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 3 & 1 \end{pmatrix} \in T_5. \]

This has map diagram

Now $\alpha$ has a tail with length $\geq 2$ and therefore $\alpha$ doesn’t lie in any subgroup.

(2) Let us take the constant element $c_1 \in T_5$

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

This has the following map diagram

Now $\alpha$ has no tails of length $\geq 2$, therefore $\alpha$ lies in a subgroup and hence $\alpha$ lies in $H_\alpha$. Note that actually $\alpha^2 = \alpha$. 
Now for any \( \beta \),

\[
\beta \in H_\alpha \iff \beta \mathcal{H}_\alpha, \quad
\iff \beta \mathcal{R} \alpha \text{ and } \beta \mathcal{L} \alpha, \\
\iff \ker \beta = \ker \alpha \text{ and } \Im \beta = \Im \alpha, \\
\iff \ker \beta \text{ has classes } \{1, 2, 3, 4, 5\} \text{ and } \Im \beta = \{1\}, \\
\iff \beta = \alpha.
\]

Therefore the maximal subgroup containing \( \alpha \) is \( \mathcal{H}_\alpha = \{\alpha\} \).

(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 \( \geq 2 \). Therefore \( \alpha \) lies in a subgroup. Hence \( \alpha \) lies in a maximal subgroup. Hence the maximal subgroup containing \( \alpha \) is \( \mathcal{H}_\alpha \). For any \( \beta \) \n
\[
\beta \in H_\alpha \iff \beta \mathcal{H}_\alpha, \quad
\iff \beta \mathcal{R} \alpha \text{ and } \beta \mathcal{L} \alpha, \\
\iff \ker \beta = \ker \alpha \text{ and } \Im \beta = \Im \alpha, \\
\iff \Im \beta = \{2, 3, 5\} \text{ and } \ker \beta \text{ has classes } \{1, 3\}, \{2, 4\}, \{5\}.
\]

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

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

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):
These are all 6 elements.
Check $\mathcal{H}_\alpha \cong S_3$. 
4.6. \( \mathcal{D} \) and \( \mathcal{J} \)

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

**Definition:** We say that \( a \ J \ b \) if and only if

\[
S^1aS^1 = S^1bS^1
\]

\[
\Leftrightarrow \exists s, t, u, v \in S^1 \text{ with } a = sbt \quad b = uav
\]

**Note.** If \( a \ L \ b \), then \( S^1a = S^1b \) so

\[
S^1aS^1 = S^1bS^1
\]

and so \( a \ J \ b \), 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

\[
S^1aS^1 = S = S^1bS^1 \quad \text{so } a \ J \ b
\]

and \( \mathcal{J} = \omega \) (the universal relation). Conversely if \( \mathcal{J} = \omega \) and \( I \prec S \), 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. Thus we have that \( S \) is simple \( \Leftrightarrow \mathcal{J} = \omega \).

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

The relation \( \mathcal{J} \) allows us to introduce a quasiorder on any semigroup \( S \), namely let \( s, t \in S \).

Then \( s \leq \mathcal{J} t \Leftrightarrow S_1sS_1 \subseteq S_1tS_1 \).

Note that \( \leq \mathcal{J} \) is a reflexive and transitive relation, but it is not anti-symmetric: we have that \( a \leq \mathcal{J} b \) and \( b \leq \mathcal{J} a \) if and only if \( a \ J \ b \).

However, \( \leq \mathcal{J} \) helps in understanding (though very roughly) how semigroups work: if \( a, b \in S \) then \( ab \leq \mathcal{J} a, b \). Thus the product always lies ‘below’ its factors with respect to \( \leq \mathcal{J} \).

4.7. Composition of Relations

**Definition:** If \( \rho \) and \( \lambda \) are relations on \( A \) we define

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

**Claim.** If \( \rho, \lambda \) are equivalence relations and if \( \rho \circ \lambda = \lambda \circ \rho \) then \( \rho \circ \lambda \) is an equivalence relation. Also, it’s the smallest equivalence relation containing \( \rho \cup \lambda \).

**Proof.** Put \( \nu = \rho \circ \lambda = \lambda \circ \rho \)

- for any \( a \in A \), \( apa \lambda a \) so \( a \nu a \) and \( \nu \) is reflexive.
- Symmetric - an exercise.
Suppose that \( a \nu b \nu c \) then there exists \( x, y \in A \) with
\[
a \rho x \lambda y \rho c.
\]
(Note that first we use that \( \nu = \rho \circ \lambda \), and next we use that \( \nu = \lambda \circ \rho \).)
From \( x \lambda y \) we have \( x \lambda y \), so
\[
a \rho x \lambda y \rho c.
\]
Therefore \( x \nu c \) hence there exists \( z \in A \) such that \( a \rho x \rho z \lambda c \) and hence \( a \nu c \). Therefore \( \nu \) is transitive.

We have shown that \( \nu \) 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 \( \tau \) 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 \( \tau \) is transitive. Therefore \( \nu \subseteq \tau \). \( \square \)

**Definition:** \( D = \mathcal{R} \circ \mathcal{L} \), i.e. \( a \mathcal{D} b \iff \exists c \in S \) with \( a \mathcal{R} c \mathcal{L} b \).

**Lemma 4.19** (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 \( a \mathcal{R} \mathcal{L} b \). Then there exists \( c \in S \) with

\[
a \mathcal{R} c \mathcal{L} b
\]

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

\[
a = cu \quad (1) \quad c = av \quad (2) \quad c = sb \quad (3) \quad b = tc.
\]

Put \( d = bu \) then we have

\[
a = cu = sbu = sd, \tag{1}
\]
\[
d = bu = tcu = ta. \tag{4}
\]

Therefore \( a \mathcal{L} d \). Also

\[
b = tc = tav = tcuv = buv = dv. \tag{4}
\]

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

Hence \( \mathcal{D} \) is an equivalence relation – \( \mathcal{D} = \mathcal{L} \lor \mathcal{R} \). Now by definition

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

As \( \mathcal{J} \) is an equivalence relation and \( \mathcal{L} \cup \mathcal{R} \subseteq \mathcal{J} \) we must have \( \mathcal{D} \subseteq \mathcal{J} \). This has Hasse Diagram
Notation: $D_a$ is the $D$ class of $a \in S$ and $J_a$ is the $J$-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 $D$-class. Let $u, v \in D$ then $u D v$. This implies that there exists $h \in S$ with $u R h L v$, 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 $D$ is an equivalence, $S$ is the union of such “egg-boxes”: the rows represent the $R$-classes, and the columns represent the $L$-classes.

<table>
<thead>
<tr>
<th></th>
<th>$u$</th>
<th>$h$</th>
<th>$v$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.8. Structure of $D$-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 4.20** (Green’s Lemma). Let $a, b \in S$ be such that $a R b$ and let $s, s' \in S$ be such that

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

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

**Proof.** If $c \in L_a$ then

$$c \rho_s = cs L as = b,$$

because $L$ is a right congruence. So $c \rho_s L b$ 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

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

Again, let $c \in L_a$. Then

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

Therefore $c \mathcal{R} cs = cp_s$. \hfill \Box

**Lemma 4.21** (Continuing Green’s Lemma). For any $c \in L_a$ we have $\rho_s : H_c \to H_{cs}$ is a bijection with inverse $\rho_{s'} : H_{cs} \to H_c$. In particular – put $c = a$ then

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

are mutually inverse bijections.

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

**Lemma 4.22** (Dual of Green’s Lemma). Let $a, b \in S$ be such that $a \mathcal{L} b$ and let $t, t' \in S$ be such that $ta = b$ and $t'b = a$. Then $\lambda_t : R_a \to R_b$ 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 4.23.** If $a \mathcal{D} b$ then there exists a bijection $H_a \to H_b$.

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

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 4.24** (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, $aH = H$.

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’s a subgroup. \hfill \Box

**Corollary 4.25.**

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

**Proof.**

(i) We know \( H_a \) is a subgroup \( \Rightarrow a, a^2 \in H_a \) so \( aH_a^2 \). If \( aH_a^2 \), 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. \( \Box \)

### 5. Rees Matrix Semigroups

Just as the main building blocks of groups are the simple groups, the main building blocks of semigroups are the 0-simple semigroups. In general, the structure of 0-simple semigroups is very complicated, however, in the finite case they are much more simple: they can be described by a group and a matrix.

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

**Definition:** \( \mathcal{M}^0 = \mathcal{M}^0(G; I, \Lambda; P) \) 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

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

Then \( \mathcal{M}^0 \) is a semigroup with zero 0 – a Rees Matrix Semigroup over \( G \).

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

\[
a = axa.
\]

\( S \) is **regular** if every \( a \in S \) is regular.

If \( S \) is regular then \( a \mathcal{R} b \iff aS = bS \iff \) there exists \( s, t \in S \) with \( a = bs \) and \( b = at \), etc.
5.1. Rees Matrix Facts

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

1. $(i, a, \lambda)$ is idempotent $\iff p_{\lambda i} \neq 0$ and $a = p_{\lambda i}^{-1}$.
2. $\mathcal{M}^0$ is regular.
3. $(i, a, \lambda) \mathcal{R} (j, b, \mu) \iff i = j$.
4. $(i, a, \lambda) \mathcal{L} (j, b, \mu) \iff \lambda = \mu$.
5. $(i, a, \lambda) \mathcal{H} (j, b, \mu) \iff i = j$ and $\lambda = \mu$.
6. The $D = J$-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:
   \[
   \begin{align*}
   xy \mathcal{D} x & \Leftrightarrow xy \mathcal{R} x \\
   xy \mathcal{D} y & \Leftrightarrow xy \mathcal{L} y
   \end{align*}
   \forall x, y \in \mathcal{M}^0
   \]
9. Put $H_{i\lambda} = \{(i, a, \lambda) \mid a \in G\}$ by (5) we have $H_{i\lambda}$ is an $H$-class ($H_{i\lambda} = H_{(i,e,\lambda)}$). If $\rho_{\lambda i} \neq 0$ we know $(i, \rho_{\lambda i}^{-1}, \lambda)$ is an idempotent $\Rightarrow H_{i\lambda}$ is a group, by the Maximal Subgroup Theorem. The identity is $(i, \rho_{\lambda i}^{-1}, \lambda)$ and $(i, a, \lambda)$ is $\rho_{\lambda i}^{-1} = (i, \rho_{\lambda i}^{-1}a^{-1}, \rho_{\lambda i}^{-1}, \lambda)$.
10. If $\rho_{\lambda i} \neq 0$ and $\rho_{\mu j} \neq 0$ then (exercise) $H_{i\lambda} \simeq H_{j\mu}$ (the bijection is $(i, a, \lambda) \mapsto (j, a, \mu)$). The morphism is a bit more sophisticated.

Proof.

1. We have that
   \[
   (i, a, \lambda) \in E(\mathcal{M}^0) \Leftrightarrow (i, a, \lambda) = (i, a, \lambda)(i, a, \lambda),
   \]
   \[
   \Leftrightarrow (i, a, \lambda) = (i, ap_{\lambda i}a, \lambda),
   \]
   \[
   \Leftrightarrow a = ap_{\lambda i}a,
   \]
   \[
   \Leftrightarrow p_{\lambda i} \neq 0 \text{ and } p_{\lambda i} = a^{-1}.
   \]
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
   \[
   (i, a, \lambda) = (j, b, \mu)(k, c, \nu) = (j, bp_{\nu k}c, \nu)
   \]
   and so $i = j$. Conversely, if $i = j$, pick $k$ with $p_{\mu k} \neq 0$. Then
   \[
   (i, a, \lambda) = (j, b, \mu)(k, p_{\nu k}^{-1}b^{-1}a, \lambda)
   \]
   and consequently $(i, a, \lambda) \mathcal{R} (j, b, \mu)$
4. Dual.
5. This comes from (3) and (4) above.
(6) \(\{0\}\) is a \(\mathcal{D}\)-class and a \(\mathcal{J}\)-class. If \((i, a, \lambda), (j, b, \mu) \in \mathcal{M}^0\) 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 \(p_\lambda \neq 0\) 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

\[x = (i, a, \lambda) \quad y = (j, b, \mu)\]

Then \(xy = (i, a\rho_j b, \mu)\), so \(xy \mathcal{R} x\). The result for \(\mathcal{L}\) is dual. □

A finitary property is a property that captures finite nature.

**Chain conditions**

**Definition:** A semigroup \(S\) has \(M_L\) if there are no infinite chains

\[S^1 a_1 \supset S^1 a_2 \supset S^1 a_3 \supset \ldots\]

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

**Claim (The Chain Claim).** The semigroup \(S\) has \(M_L\) if and only if any chain

\[S^1 a_1 \supseteq S^1 a_2 \supseteq \ldots\]

terminates (stabilizes) with

\[S^1 a_n = S^1 a_{n+1} = \ldots\]

**Proof.** If every chain with \(\supseteq\) terminates, then clearly we cannot have an infinite strict chain

\[S^1 a_1 \supset S^1 a_2 \supset \ldots\]

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

\[S^1 a_1 \supseteq S^1 a_2 \supseteq \ldots\]

The strict inclusions are at the \(j_i\)th steps

\[S^1 a_1 = S^1 a_2 = \cdots = S^1 a_{j_1} \supset S^1 a_{j_1+1} = S^1 a_{j_1+2} = \cdots = S^1 a_{j_2} \supset S^1 a_{j_2+1} = \cdots\]

Then \(S^1 a_{j_1} \supset S^1 a_{j_2} \supset \ldots\). As \(S\) has \(M_L\), this chain is finite with length \(n\) say. Then
\[ S^1 a_{jn + 1} = S^1 a_{jn + 2} = \ldots \]

and our sequence has stabilised. \(\square\)

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

**Example 5.1.** Every finite semigroup has \(M_L, M_R, M^L, M^R\). For, if

\[ S^1 a_1 \supset S^1 a_2 \supset S^1 a_3 \supset \ldots , \]

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 5.2.** The Bicyclic semigroup \(B\) has \(M^L\) and \(M^R\). We know \(B(x, y) = \{(p, q) \mid q \geq y\}\) and so \(B(x, y) \subseteq B(u, v) \iff y \geq v\), inclusion is strict if and only if \(y > v\). If we had an infinite chain

\[ B(x_1, y_1) \subset B(x_2, y_2) \subset B(x_3, y_3) \subset \ldots \]

then we would have

\[ y_1 > y_2 > y_3 > \ldots , \]

which is impossible in \(\mathbb{N}\).

Hence \(M^L\) holds, dually \(M^R\) holds. However, since \(0 < 1 < 2 < \ldots\) we have

\[ B(0, 0) \supset B(1, 1) \supset B(2, 2) \supset \ldots \]

so there exists infinite descending chains. Hence \(B\) doesn’t have \(M_L\) or \(M_R\). \(\square\)

**Example 5.3.** Let \(M^0 = M^0(G; I; \Lambda; P)\) be a Rees Matrix Semigroup over a group \(G\). Then \(M^0\) has \(M_L, M_R, M^L\) and \(M^R\).

**Proof.** We show that the length of the strict chains is at most 2. Suppose \(\alpha M^0 \subseteq \beta M^0\).

We could have \(\alpha = 0\). If \(\alpha \neq 0\) then \(\alpha M^0 \neq \{0\}\) so \(\beta \neq 0\) and we have \(\alpha = (i, g, \lambda)\), \(\beta = (j, h, \mu)\) and \(\alpha = \beta \gamma\) for some \(\gamma = (\ell, k, \nu)\) so that

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

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

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

By above, any Rees Matrix Semigroup over a group is completely 0-simple. Our aim is to show that every completely 0-simple semigroup is isomorphic to a Rees Matrix Semigroup over a group.
Theorem 5.1 (The $\mathcal{D} = \mathcal{J}$ Theorem). Suppose

\[
\begin{aligned}
&\forall a \in S, \exists n \in \mathbb{N} \text{ with } a^n \mathcal{L} a^{n+1}, \\
&\forall a \in S, \exists m \in \mathbb{N} \text{ with } a^m \mathcal{R} a^{m+1}.
\end{aligned}
\]

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

Example 5.4.

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

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

\[
b = xay, \ a = ubv.
\]

Then

\[
b = xay = (xu)b(vy) = (xu)(xubvy)(vy) = (xu)^2b(vy)^2 = \cdots = (xu)^n b(vy)^n
\]

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

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

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

\[
S^1b = S^1xub \subseteq S^1ub \subseteq S^1b.
\]

So $S^1b = S^1ab$, 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, $\mathcal{D} = \mathcal{J}$.

Let $S$ be a semigroup having $M_L$ and let $a \in S$. Then

\[
S^1a \supseteq S^1a^2 \supseteq S^1a^3 \supseteq \ldots.
\]

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 $a^n \mathcal{L} a^{n+1}$. Similarly, if $S$ has $M_R$, then for every $a \in S$ there exists $m \in \mathbb{N}$ such that $a^m \mathcal{R} a^{m+1}$. As a consequence we have the following:

Corollary 5.2. If a semigroup $S$ has $M_L$ and $M_R$, then it satisfies $(\star)$ and thus $\mathcal{D} = \mathcal{J}$.

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

(i) $a \mathcal{J} ab \iff a \mathcal{D} ab \iff a \mathcal{R} ab$,

(ii) $b \mathcal{J} ab \iff b \mathcal{D} ab \iff b \mathcal{L} ab$.

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

\[
a \mathcal{J} ab \iff a \mathcal{D} ab
\]

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

\[
a = xaby = xa(by) = x^n a(by)^n
\]
for all \( n \). Pick \( n \) with \((by)^n \mathcal{R} (by)^{n+1}\). Then

\[
a = x^n a(by)^n \mathcal{R} x^n a(by)^{n+1} = x^n a(by)^n b y = aby
\]

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

**Lemma 5.3** (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 \( J \)-classes are \( \{0\} \) and \( S \setminus \{0\} \).

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

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

\[
S = SaS \subseteq S^1 a S^1 \subseteq S
\]

and therefore \( S = S^1 a S^1 \).

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

\[
S^1 a S^1 = S = S^1 b S^1
\]

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

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

\[
S^3 = SS^2 = S^2 = S \neq 0.
\]

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

\[
0 \subseteq SxsS \subseteq SxS = 0.
\]

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

\[
S^3 = SIS, = \bigcup_{x \in I} SxS, = 0.
\]

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 5.4. 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,

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

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 $t \geq 0$. Similarly $u^m \mathcal{L} u^{m+t}$ for all $t \geq 0$. 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 4.18, $u^s$ lies in a subgroup. Therefore $u^s \mathcal{H} e$ for some idempotent $e$. As $u^s \neq 0$ and $H_0 = \{0\}$, we have $e \neq 0$. □

Theorem 5.5 (Rees’ Theorem - 1941). Let $S$ be a semigroup with zero. Then $S$ is completely 0-simple $\iff$ $S$ 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 Rees Matrix facts), 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 $(\ast)$). As $S$ is 0-simple, the $\mathcal{D} = \mathcal{J}$-classes are $\{0\}$ and $S \setminus \{0\}$. Let $D = S \setminus \{0\}$. By the Corollary to the 0-simple Lemma, $D$ contains 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 $\Lambda$ 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 $\Lambda$ 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

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

Thus, by Green’s Lemma,

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

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

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

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 \( \rho_{q\lambda} \) and \( \lambda r_i \), 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 \( q\lambda r_i \mathcal{D} q\lambda \).

By the rectangular property \( q\lambda r_i \mathcal{R} q\lambda \mathcal{R} e \).

\[
\begin{array}{c|c|c}
 & L_1 & L_\lambda \\
\hline
R_1 & a & q\lambda \\
\hline
R_i & r_i & r_i a q\lambda \\
\end{array}
\]

Also by the rectangular property, if \( q\lambda r_i \neq 0 \) then as \( q\lambda r_i \mathcal{D} r_i \) we have

\[ q\lambda r_i \mathcal{L} r_i \mathcal{L} e. \]

Therefore \( q\lambda r_i = 0 \) or \( q\lambda r_i \in G \). So, \( P = (p_{\lambda i}) = (q\lambda r_i) \) is a \( \Lambda \times I \) matrix over \( G \cup \{0\} \).

For any \( i \in I \), by the 0-simple Lemma we have \( Sr_i S = S \). So, \( ur_i v \neq 0 \) for some \( u, v \in S \). Say, \( u = r_kbq\lambda \) for some \( k, \lambda \) and \( b \). Then

\[ p_{\lambda i} = q\lambda r_i \neq 0 \]
as \( r_kbq\lambda r_i v \neq 0 \). 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

\[ (0x)\theta = 0\theta = 0 = (x\theta) = 0\theta x\theta. \]

Also, \( (x0)\theta = x\theta0\theta \). For \( (i, a, \lambda), (k, b, \mu) \in \mathcal{M}^0 \) we have
\[(i, a, \lambda)(k, b, \mu)\theta = \begin{cases} 0\theta & \text{if } p_{\lambda k} = 0, \\ (i, a p_{\lambda k} b, \mu)\theta & \text{if } p_{\lambda k} \neq 0, \end{cases} \]

\[= \begin{cases} 0 & \text{if } p_{\lambda k} = 0, \\ r_{i} a p_{\lambda k} b q_{\mu} & \text{if } p_{\lambda k} \neq 0, \end{cases} \]

\[= r_{i} a q_{\lambda} r_{k} b q_{\mu}, \]

\[= (i, a, \lambda)\theta(k, b, \mu)\theta. \]

Therefore \(\theta\) is a morphism, and since it is bijective, it is an isomorphism. \(\square\)

### 6. Regular Semigroups

**Definition 6.1.** 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. Of non-regular semigroups: \((\mathbb{N}, +)\), \((\mathbb{Z}, \ast)\), nontrivial null (or zero) semigroups. Note that \((\mathbb{N}, +)\) does not even contain a single regular element.

**Definition 6.2.** An element \(a' \in S\) is an inverse of \(a\) if \(a = aa'a\) and \(a' = a'aa'\). We denote by \(V(a)\) the set of inverses of \(a\).

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

\[(i, j)(k, \ell)(i, j) = (i, j) \]

\[(k, \ell)(i, j)(k, \ell) = (k, \ell) \]

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

**Lemma 6.3.** If \(a \in S\), then \(a\) is regular \(\iff V(a) \neq \emptyset\).

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

\[aa'a = a(xax)a = (axa)xa = axa = a,\]

\[a'aa' = (xax)a(xax) = x(axa)(xax) = xa(xax) = x(axa)x = xax = a'.\]

So \(a' \in V(a)\). \(\square\)
Note. If \( a = axa \) then

\[
(ax)^2 = (ax)(ax) = (axa)x = ax
\]

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

\[
a = axa \quad ax = ax \Rightarrow a \mathcal{R} ax,
\]

\[
a = axa \quad xa = xa \Rightarrow a \mathcal{L} xa.
\]

**Figure 5.** The egg box diagram of \( D_a \).

**Definition 6.4.** \( S \) is inverse if \( |V(a)| = 1 \) for all \( a \in S \), i.e. every element has a unique inverse.

**Example 6.1.**

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

**Theorem 6.5** (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 6.3. Suppose \( x, y \in V(a) \). Then

\[
\begin{align*}
a &= axa & x &= xax & a &= aya & y &= yay, \\
(1) & & (2) & & (3) & & (4)
\end{align*}
\]

so \( ax, xa, ay, ya \in E(S) \). This gives us that
So \( |V(a)| = 1 \) and \( S \) is inverse.

Conversely suppose \( S \) is inverse. 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 \( x = (ef)' \). Consider the element \( fxe \). Then

\[
(fxe)^2 = (fxe)(fxe) = f(xef)e = fxe
\]
as \( x = (ef)' \). So \( fxe \in E(S) \) and therefore \( fxe = (fxe)' \). We want to show that \( fxe \) and \( ef \) are mutually inverse, i.e.

\[
ef(fxe)ef = ef^{2}xe^{2}f = efxef = ef,
\]
\[
(fxe)ef(fxe) = fxe^{2}f^{2}xe = fxefxe = fxe.
\]

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

\[
ef(fe)ef = ef^{2}e^{2}f = efef = ef,
\]
\[
fe(ef)fe = fe
\]
similarly. Therefore we have \( ef = (fe)' = fe \).

\[\square\]

**Example 6.2.**

1. \( E(B) = \{(a, a) \mid a \in \mathbb{N}^0\} \), 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. \( T_X \) – we know \( T_X \) is regular. For \( |X| \geq 2 \) let \( x, y \in X \) with \( x \neq y \) we have \( c_x, c_y \in E(T_X) \). Then \( c_xc_y \neq c_yc_x \) so \( T_X \) is not inverse.

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

\[
S \text{ is inverse} \iff ef = fe \text{ for all } e, f \in E(S),
\]
\[
\iff ef = fe \text{ for all } e, f \in S,
\]
\[
\iff S \text{ is a semilattice.}
\]

**Definition 6.6.** Let \( S \) be an inverse semigroup (monoid), and let \( A \subseteq S \) be nonempty. We say that \( A \) is an inverse subsemigroup (submonoid) of \( S \) if \( A \) is a subsemigroup (submonoid) of \( S \), and for every \( a \in A \) we have that \( a' \in A \) as well.
Example 6.3. For example, let $A = \{(0, x) : x \in \mathbb{N}^0\}$ be a subset of $B$. Then for every $(0, x), (0, y) \in A$, we have that $(0, x)(0, y) = (0, x + y) \in A$, and also, $(0, 0) \in A$. So $A$ is a submonoid of $B$. However, $(0, 1) = (1, 0) \notin A$, so $A$ is not an inverse submonoid of $B$. 
6.1. 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 \( e \not\sim f \) then \( |H_e| = |H_f| \) (by the Corollary to Green’s Lemmas). We will show that \( H_e \cong H_f \).

**Lemma 6.7.** We have that

1. If \( a = axa \) then \( ax, xa \in E(S) \) and \( ax \mathrel{\text{R}} a \mathrel{\text{L}} xa \),
2. If \( b \mathrel{\text{R}} f \in E(S) \), then \( b \) is regular,
3. If \( b \mathrel{\text{L}} f \in E(S) \), then \( b \) is regular.

**Proof.**

(i) we know this.

(ii) If \( b \mathrel{\text{R}} f \) then \( fb = b \). Also, \( f = bs \) for some \( s \in S^1 \). Therefore \( b = fb = bsb \) and so \( b \) is regular.

(iii) this is dual to (ii).

\( \square \)

**Lemma 6.8** (Regular \( \mathcal{D} \)-class Lemma). If \( a \not\sim b \) then if \( a \) is regular, so is \( b \).

**Proof.** Let \( a \) be regular with \( a \not\sim b \). Then \( a \mathrel{\text{R}} c \mathrel{\text{L}} b \) for some \( c \in S \).

\[
\begin{array}{ccc}
  a & e & c \\
  & f & \\
  & & b \\
\end{array}
\]

**Figure 6.** The egg box diagram of \( \mathcal{D} \).

There exists \( e = e^2 \) with \( e \mathrel{\text{R}} a \mathrel{\text{R}} c \) by (ii) above. By (ii), \( c \) is regular. By (i), \( c \mathrel{\text{L}} f = f^2 \).

By (iii), \( b \) is regular.

\( \square \)

**Corollary 6.9.** Since idempotents are regular, as a direct consequence we have that an element \( a \in S \) is regular if and only if it is \( \mathrel{\text{R}} \)-related to an idempotent and \( \mathrel{\text{L}} \)-related to an idempotent as well.

**Corollary 6.10** (Corollary to Green’s Lemmas). Let \( e, f \in E(S) \) with \( e \not\sim f \). 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

$$xax = fx = ffsa = fse = x.$$

So we have the diagram

\[
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
 e \quad a \\
 \rho_a \\
 x \\
 f
\end{array}
\end{array}
\end{array}
\]

We have $ea = a$ therefore $\rho_a : H_e \to H_a$ is a bijection. From $a \mathcal{L} f$ and $xa = f$ we have $\lambda_x : H_a \to H_f$ is a bijection. Hence $\rho_a \lambda_x : H_e \to H_f$ is a bijection. Let $h, k \in H_e$. 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 $H_e \cong H_f$. □
It worth noting that the previous proof also allows us to locate the inverses of a regular element.

**Lemma 6.11.** If \( a \in S \) is regular, and \( x \in V(a) \), then there exist idempotents \( e \) and \( f \) such that

\[
a \mathcal{R} e \mathcal{L} x, \ a \mathcal{L} f \mathcal{R} x.
\]

And 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

\[
e \mathcal{L} x, \ f \mathcal{R} x.
\]

Furthermore, \( ax = e \) and \( xa = f \) in this case.

<table>
<thead>
<tr>
<th>( a )</th>
<th>( e = ax )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( f = xa )</td>
<td>( x )</td>
</tr>
</tbody>
</table>

**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.

For the second part, just look at the proof of the previous corollary: it starts by the assumption that \( e \mathcal{R} a \mathcal{L} f \), and concludes that there exists an \( x \) satisfying \( a = axa \) and \( x = xax \) such that \( ax = e \) and \( xa = f \), which proves the lemma. \( \square \)

**Example 6.4.**

1. If \( \mathcal{M}^0 = \mathcal{M}^0(G; I; \Lambda; P) \) then \( \mathcal{M}^0 \setminus \{0\} \) is a \( \mathcal{D} \)-class. We have \( H_{i\lambda} = \{(i, g, \lambda) \mid g \in G\} \).

   If \( p_{\lambda_1} \neq 0 \), \( H_{i\lambda} \) is a group \( \mathcal{H} \)-class. If \( p_{\lambda_1}, p_{\mu_1} \neq 0 \) then \( H_{i\lambda} \cong H_{j\mu} \) (seen directly).

2. \( B \) (the Bicyclic Monoid). \( B \) is bisimple. \( E(B) = \{(a, a) \mid a \in \mathbb{N}^0\} \). Then \( H_{(a,a)} = \{(a, a)\} \). Clearly \( H_{(a,a)} \cong H_{(b,b)} \).

3. In \( T_n \), then \( \alpha \mathcal{D} \beta \iff \rho(\alpha) = \rho(\beta) \) where \( \rho(\alpha) = \lvert \text{Im}(\alpha) \rvert \). By the Corollary, if \( \varepsilon, \mu \in E(T_n) \) and \( \rho(\varepsilon) = \rho(\mu) = m \) say, then \( H_{\varepsilon} \cong H_{\mu} \). In fact \( H_{\varepsilon} \cong H_{\mu} \cong S_m \).